La manifattura delle frodi: dalla tecnologia all'artigianato

Banche e Sicurezza

Milano – 27 Maggio 2014

CENTRO ANTIFRODE BANCOMAT

... ci siamo lasciati così ...

2012

1.344 casi segnalati

75 % *cash trapping*

2013

1.053 casi segnalati

55 % *cash trapping*

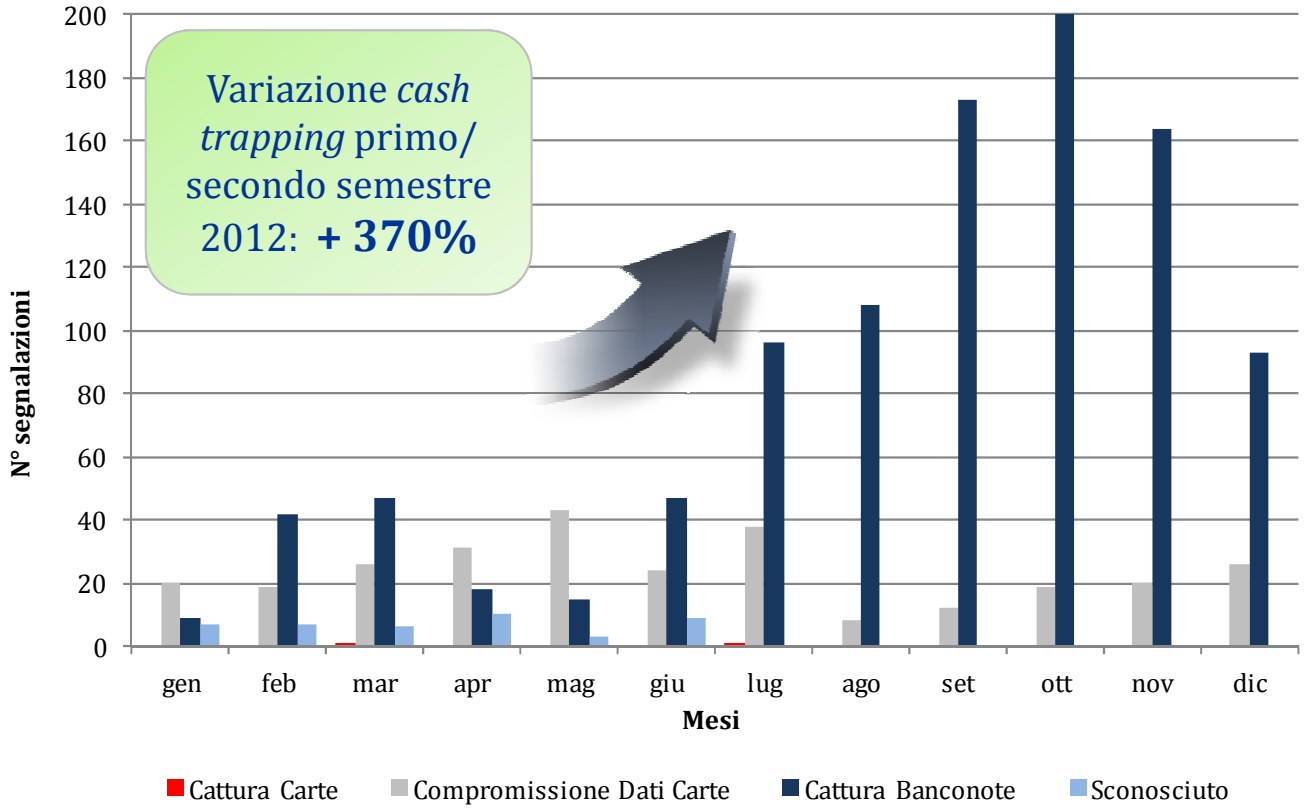
2012 – *War on cash … trapping* (1/2)

Negli ultimi anni, i Circuiti BANCOMAT e PagoBANCOMAT sono stati interessati da due categorie di fenomeni, attacchi **fisici** e attacchi **logici**.

		REMEDIATION
ATTACCHI LOGICI	**Compromissione dati carta (o *skimming*)**	**Remediation:** migrazione della tecnologia delle carte verso lo standard microcircuito
	Cattura del PIN	**Remediation**: irrobustimento del protocollo (il PIN consente di effettuare operazioni se non con la carta originale)
	Colloquio di tratta	**Remediation**: protocollo PagoBANCOMAT CB2; mutua autenticazione
ATTACCHI FISICI	**Cattura carta (o tasca libanese)**	**Remediation**: migrazione della tecnologia delle carte verso lo standard microcircuito
	Cattura banconote (o *cash trapping*)	**Remediation**

2012 – *War on cash ... trapping* (2/2)

Nel secondo semestre del 2012, i Consorziati hanno segnalato sulla piattaforma web del Consorzio un significativo incremento degli episodi di ***cash trapping*** su terminali ATM.



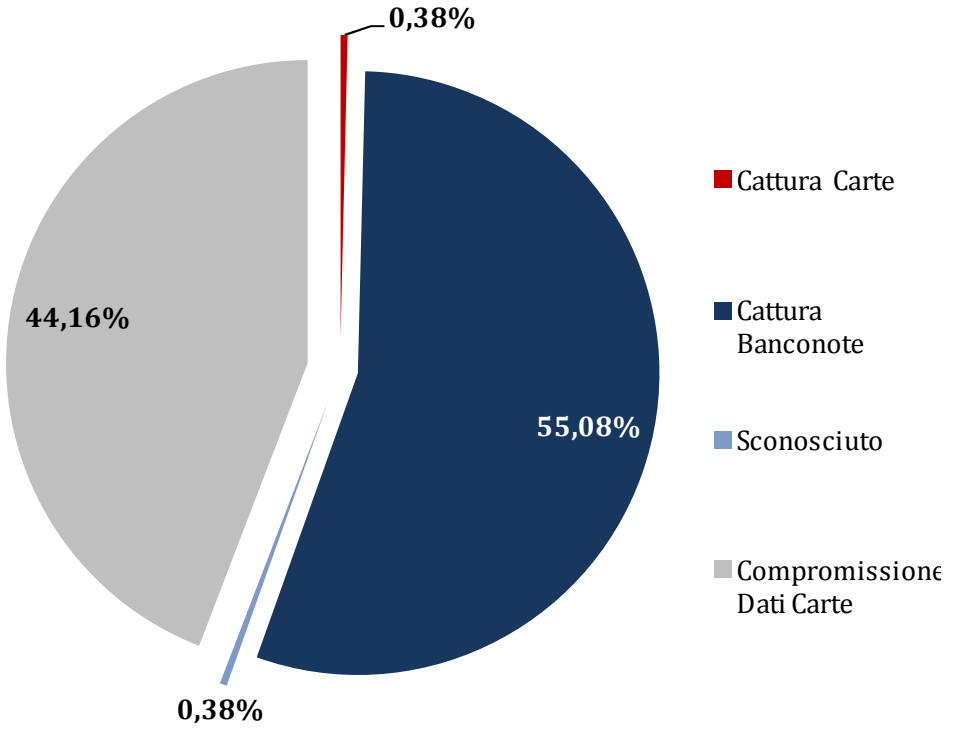
La messa in campo e il coordinamento di *task force* dedicate ha portato all'individuazione di **soluzioni modulari di tipo hardware e software** ampiamente adottate dal Sistema.

Il 2013 in pillole

- **63%** quota di mercato rappresentata dagli enti segnalanti
- **725** ATM manomessi segnalati
- **185** Issuer emittenti carte oggetto degli attacchi
- Circa **15.000** alert inviati
- **17.444** carte transate su terminali manomessi e quindi potenzialmente a rischio preventivamente intercettate

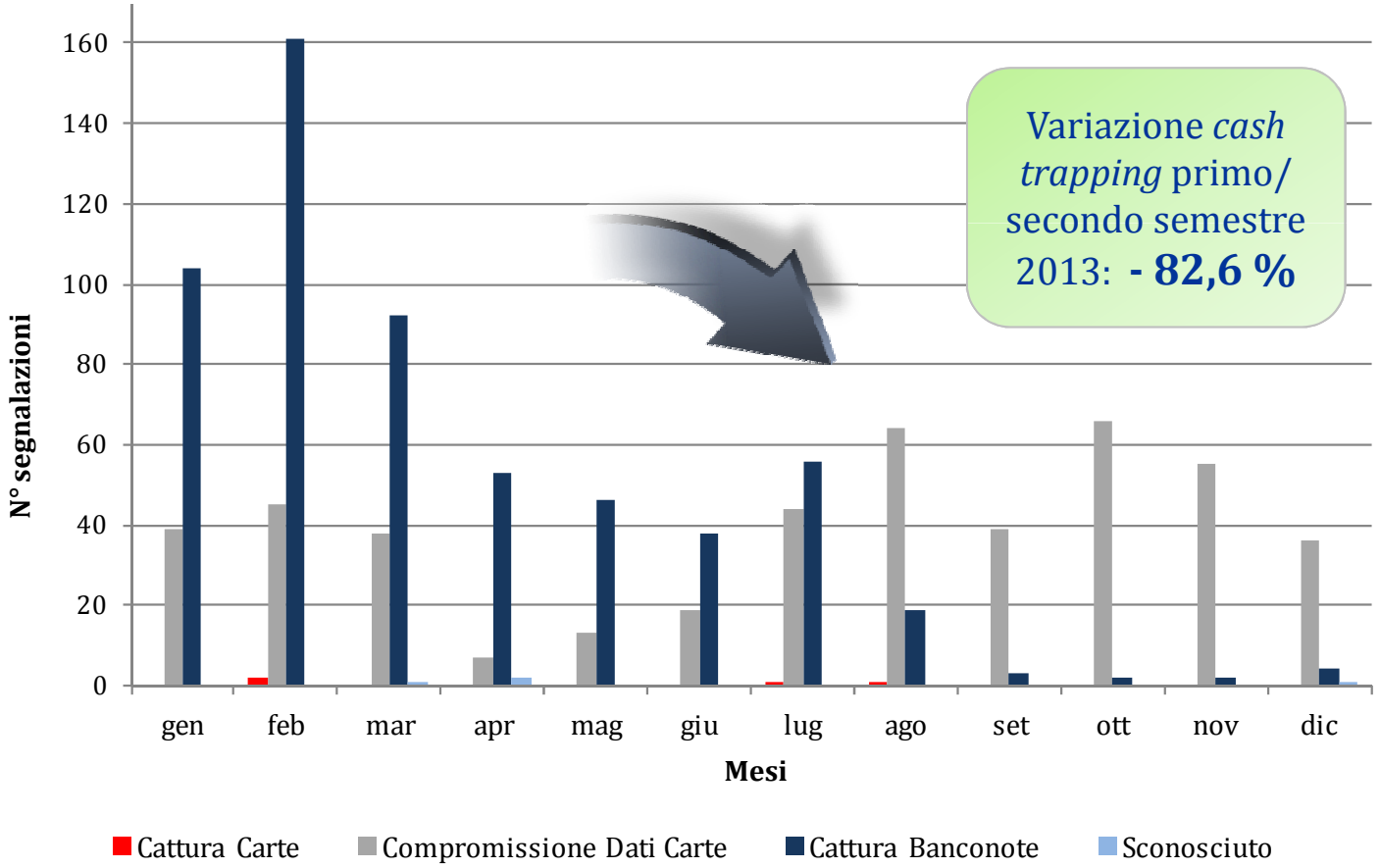
1.053 episodi segnalati sul Presidio del Centro Antifrode, suddivise per tipologia di attacco:

- ✓ Cattura carte
- ✓ Cattura banconote (*cash trapping*)
- ✓ Compromissione dati carte (*skimming*)



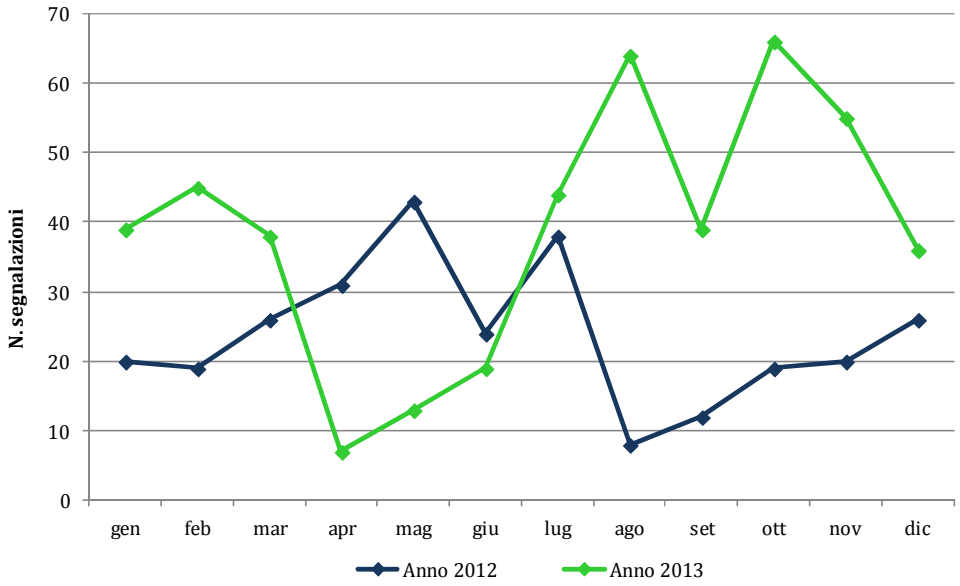
2013 – Distribuzione mensile delle segnalazioni

Quanto fatto nel 2012 ha portato nel 2013 a un abbattimento generale del numero di episodi segnalati (**-22%** rispetto all'anno precedente) e, più in dettaglio, a una forte diminuzione del fenomeno del *cash trapping*.



Confronto anni 2012/ 2013

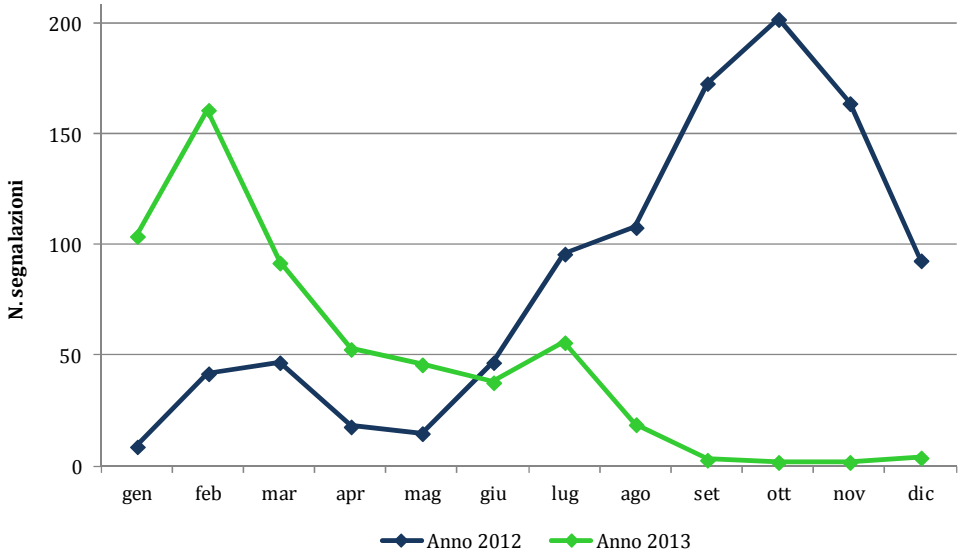
Skimming e *cash trapping*



Gli ultimi due anni, pertanto, sono stati caratterizzati da tendenze opposte.

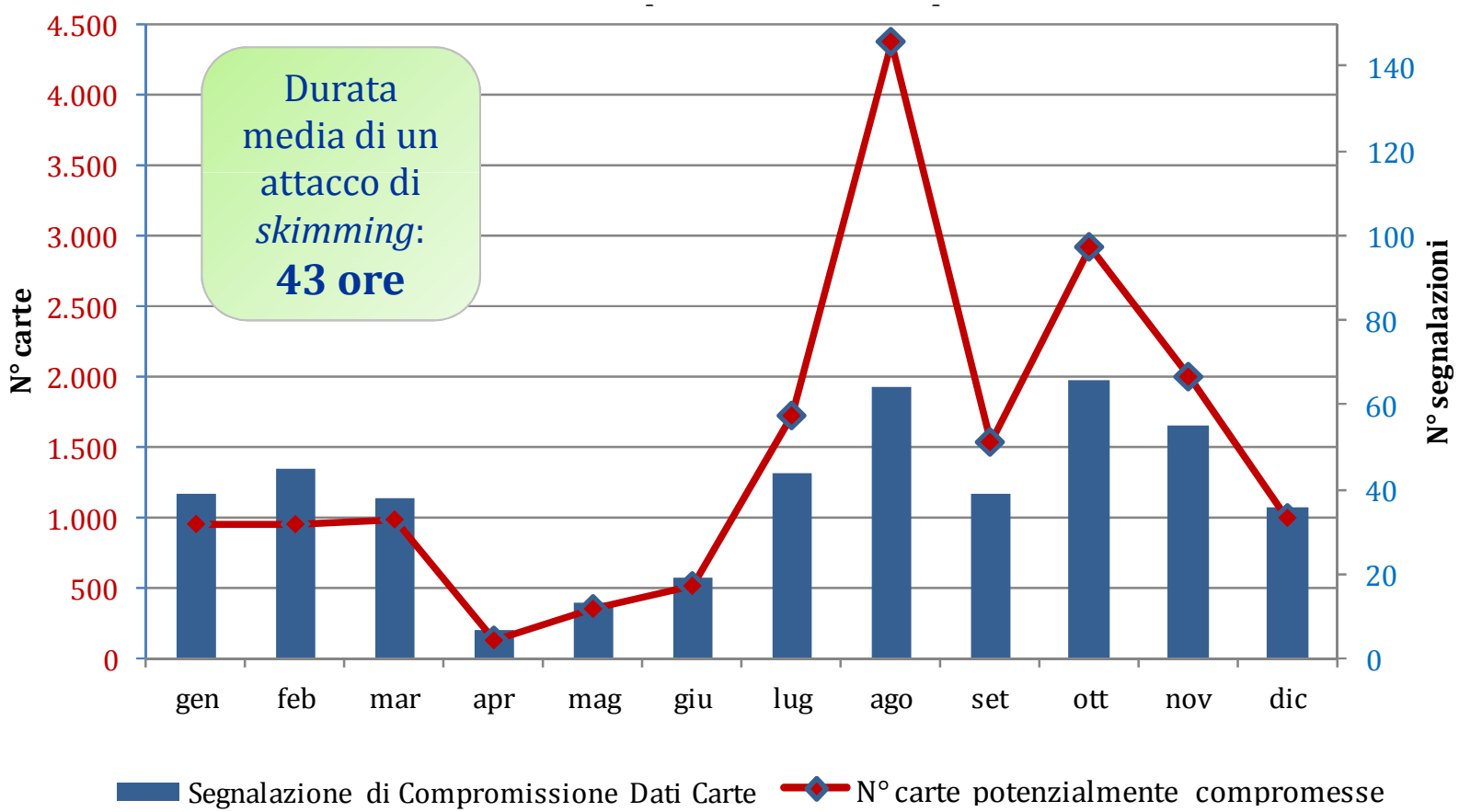
Rispetto al 2012, nel corso del 2013 le segnalazioni di ***Compromissione dati carte*** sono aumentate del **63%**, passando da una media di **24** episodi al mese ad una media di **39** casi al mese.

Rispetto al 2012, nel corso del 2013 le segnalazioni di ***Cattura banconote*** hanno subito una riduzione del **43%**, passando da una media di **85** episodi al mese ad una media di **48** casi al mese.

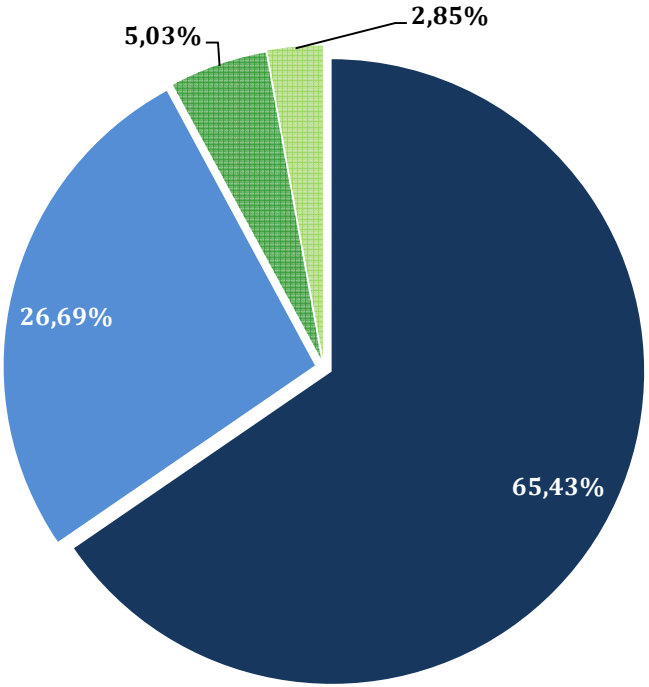


Carte potenzialmente compromesse

Nel corso del 2013 le banche Acquirer hanno segnalato sul Presidio circa 450 episodi di *skimming* ad ognuno dei quali, mediamente, sono state associate **38 carte potenzialmente compromesse**, in quanto transate sui terminali manomessi.

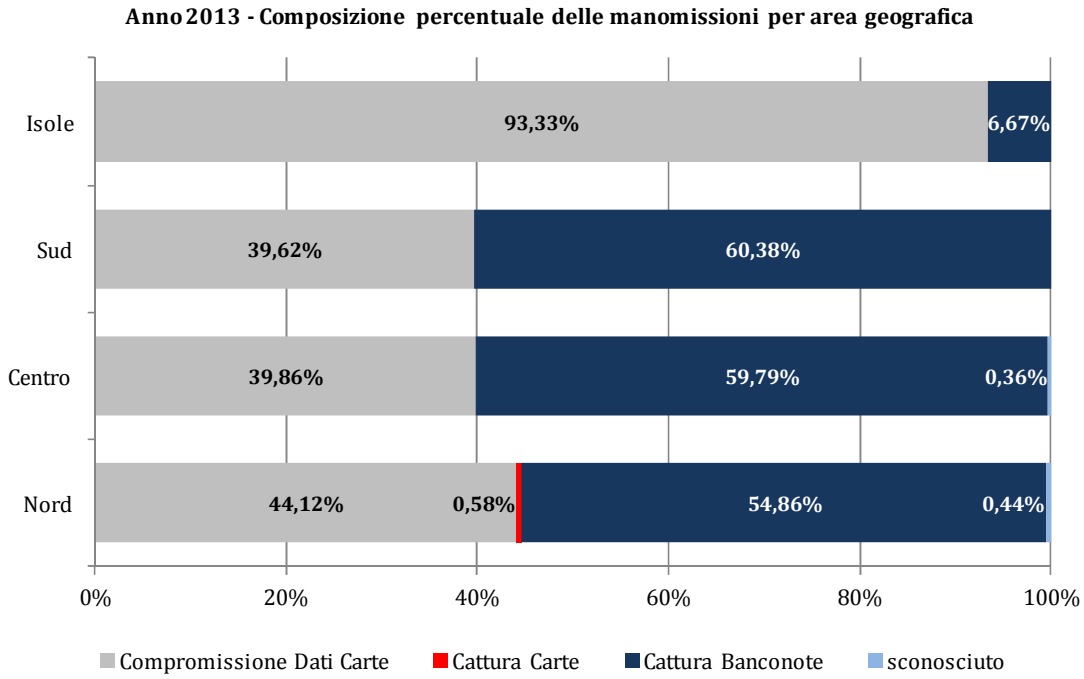


2013 – Distribuzione geografica delle manomissioni (1/2)

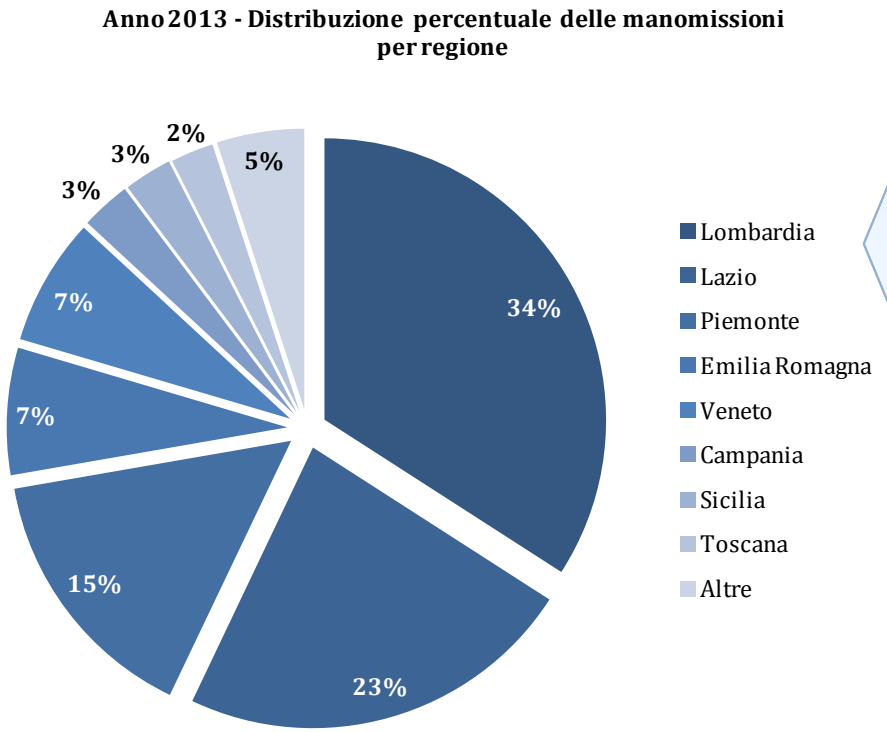


Ogni area geografica è caratterizzata da una diversa composizione delle manomissioni che – eccezion fatta per le Isole – si suddividono in modo abbastanza simile tra *Compromissione dei dati delle carte* e *Cattura banconote*.

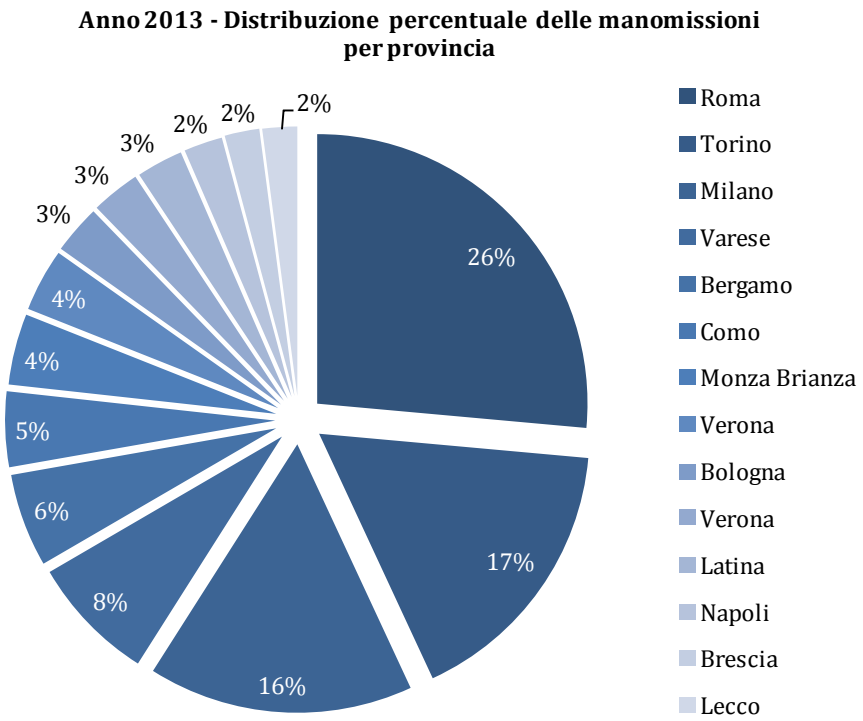
La maggior parte delle manomissioni (**65,43%**) sono state realizzata nell'area Nord del Paese.



2013 – Distribuzione geografica delle manomissioni (2/2)



Le regioni più colpite dagli attacchi agli ATM risultano essere la Lombardia (**34%**), il Lazio (**23%**) e il Piemonte (**15%**).
Le prime due sono maggiormente interessate dal fenomeno di *Cattura delle banconote*; il Piemonte, invece, registra una prevalenza di segnalazioni di *Compromissione dati carte* (58%).



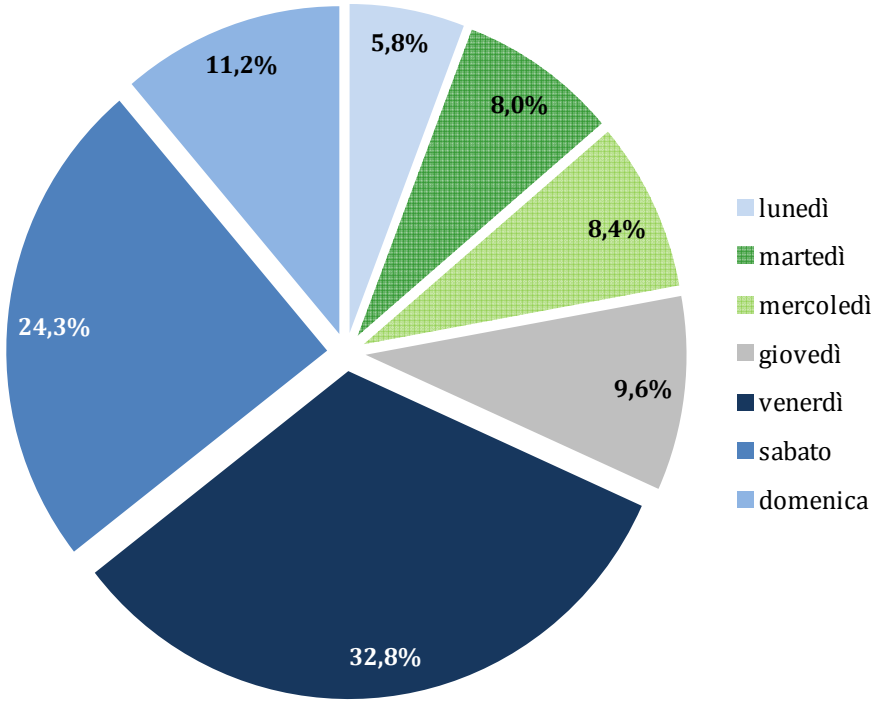
Le province più colpite dagli attacchi agli ATM sono Roma (**26%**), Torino (**17%**) e Milano (**16%**).
Mentre la prima è maggiormente interessata dal fenomeno di *Cattura delle banconote* (67%), le altre due registrano una prevalenza di segnalazioni di *Compromissione dati carte* (62% e 60%).

2013 – Giorni della settimana e fasce orarie più colpite

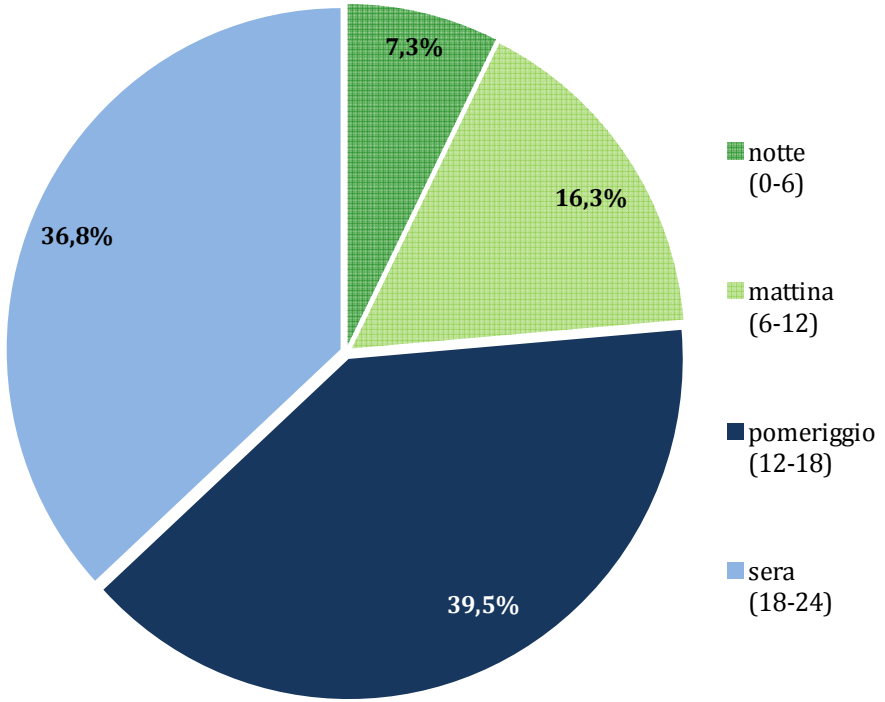
La maggior parte delle manomissioni segnalate hanno avuto inizio nelle giornate di **venerdì** (32,8%) e **sabato** (24,3%).

Le fasce orarie più colpite sono il **pomeriggio** – tra le 16.00 e le 20.00 (44,6%) – e la **sera** – tra le 20.00 e le 24.00 (21,4%).

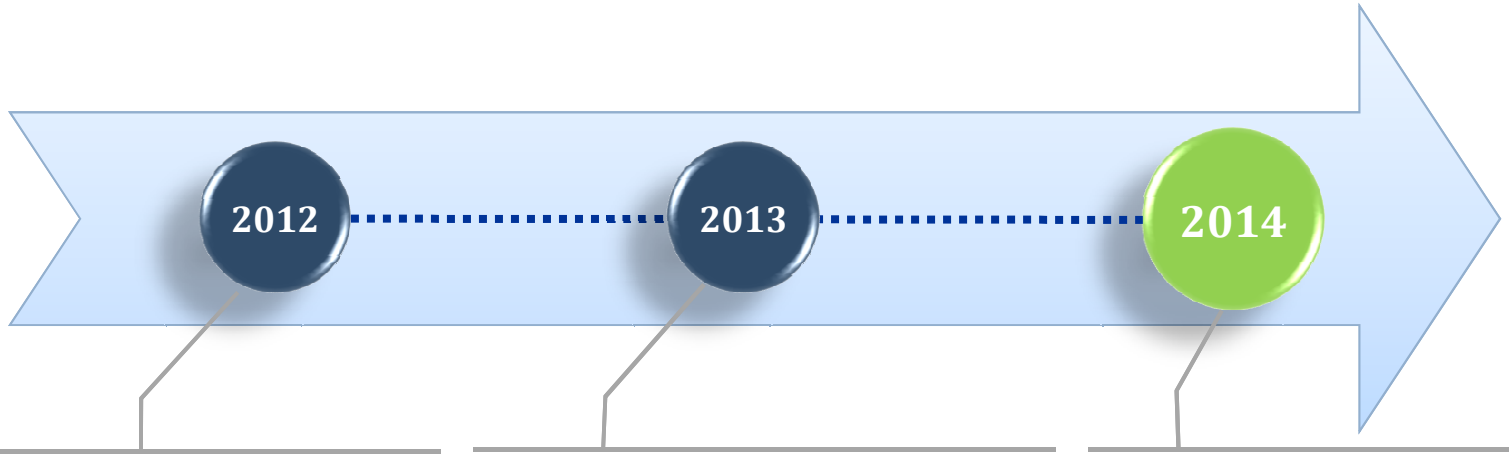
Anno 2013 - Giorni della settimana più colpiti



Anno 2013 - Fasce orarie più colpite



2014 – Nuove tendenze



Anno 2012

Diffusione del *cash trapping*

- ✓ Coordinamento di *task force* finalizzate all'individuazione di strategie di difesa
- ✓ Messa in campo di soluzioni modulari di tipo hardware e software.

Anno 2013

Prevalenza dello *skimming*

- ✓ Irrobustimento del protocollo autorizzativo
- ✓ Analisi transazionali volte a valutare la genuinità delle richieste autorizzative

... e oggi?

Dalle prime rilevazioni emerge il riaccentuarsi di una tendenza nota, ossia una sorta di **regressione tecnologica** delle frodi che perdono quel grado di sofisticatezza che le ha caratterizzate nei periodi precedenti a favore di metodologie più semplici e rudimentali.

2014 – Raggiri con destrezza

Modalità di realizzazione

Negli ultimi mesi, il Centro Antifrode ha ricevuto numerose segnalazioni circa una nuova modalità di frode presso gli ATM che si presenta come un raggiro nei confronti del *card holder* volto a carpire il PIN e a sottrarre la carta originale.

1. Un piccolo gruppo di malviventi sceglie un terminale all'interno di una lobby multipla e, una volta individuata la vittima ideale, un paio entrano nell'ambiente in cui opera l'ATM mentre uno solitamente resta di guardia
2. Una volta all'interno, uno dei frodatori carpisce il PIN mentre viene digitato dal titolare e un altro, un attimo prima che la carta sia rilasciata dal terminale, lascia cadere una banconota in terra (in genere un pezzo da 50€) chiedendo alla vittima se sia la sua
3. In questo modo, i frodatori creano un diversivo che distrae il titolare, facendogli perdere di vista la carta
4. I frodatori sostituiscono rapidamente la carta genuina con una sua imitazione e successivamente la spendono utilizzando il PIN precedentemente intercettato

2014 – Raggiri con destrezza

Caratteristiche dell'attacco

- ✓ **Target specifico delle vittime**: persone anziane o donne con bambini
- ✓ **Caratteristiche strutturali dell'ambiente ATM:** lobby multiple o terminali *indoor* filiale
- ✓ **Vulnerabilità sfruttate:** il raggiro fa leva sulla distrazione del *card holder*, e non sulle caratteristiche tecnico-operative dello strumento di pagamento o del punto di accettazione

- **Assenza di sofisticazioni tecnologiche** – basso costo di realizzazione
- **Alta probabilità di successo** – le operazioni fraudolente sono realizzate con carta originale e corretta digitazione del PIN
- **Difficoltà nell'intercettazione "*real time*"** – è difficile scongiurare gli attacchi se non sensibilizzando la clientela
- **Alta redditività dell'attacco –** perdite economiche e danno di immagine per le Banche

Il raggiro con destrezza è comunque realizzabile solo in determinate condizioni ambientali, soprattutto in caso di terminali *unattended*

2014 – Attacchi fisici agli AFD

Automated Fuel Dispenser

Anche sui terminali POS è evidente la medesima tendenza di "regressione", ma solo nel caso di terminali OPT (*Outdoor Payment Terminal)* quali – ad esempio – gli AFD (*Automated Fuel Dispenser*), in quanto presentano una serie di caratteristiche che li rendono più "appetibili" per i frodatori.

- Alta **redditività** per singolo attacco (soprattutto per i terminali "*cash in cash out*")
- Localizzazione decentrata che determina un **minore controllo** sull'Apparecchiatura
- **Operatività** continuativa dei *self service* h24

Pur nella medesima condizione di strumentazione e localizzazione del terminale, la frode del raggiro non è stata significativamente segnalata in tale ambito.

Nel settore *petrol* si manifestano prevalentemente frodi di tipo *cash trapping* sottoforma di "*brute attack*" alla cassaforte.

Conclusioni

Il Sistema BANCOMAT/ PagoBANCOMAT da tempo lavora all'irrobustimento delle difese di carattere tecnologico degli strumenti e dei processi autorizzativi, tanto che non risulta più appetibile il tentativo di violare le sue difese.

Una vulnerabilità residua è identificabile nella **mancata consapevolezza delle potenzialità** dello strumento che si ha tra le mani.

Per colmare queste lacune e aumentare la fiducia nei confronti del Circuito è necessario che il Sistema continui ad adoperarsi al fine di informare ed educare i *card holder* a un **corretto utilizzo degli strumenti di pagamento**.

Grazie