Centro Antifrode Consorzio BANCOMAT

War on cash … trapping

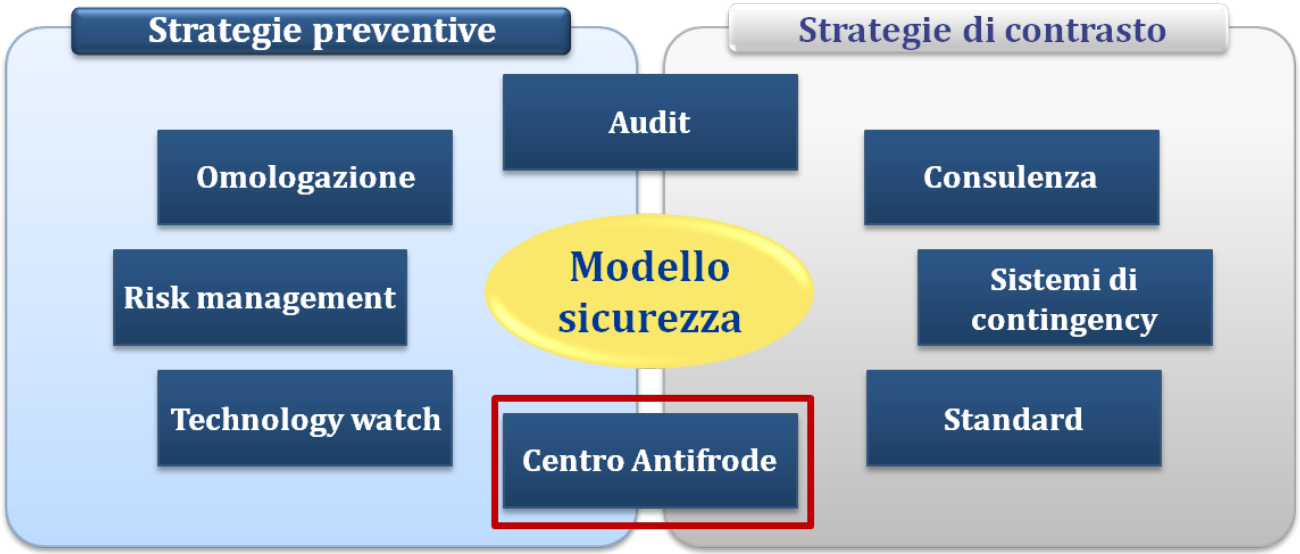
Veronica Borgogna

Consorzio BANCOMAT - Modello di sicurezza

Il Consorzio BANCOMAT è il proprietario dei Marchi "BANCOMAT" e "PagoBANCOMAT" e gestore dei relativi Circuiti.

Nel 2010 ha sviluppato un **Modello di Sicurezza** per il monitoraggio dei fenomeni fraudolenti basato su due tipi di strategie e finalizzato a:

- Efficientare i processi di gestione della sicurezza (interni ed esterni)
- Mitigare gli effetti degli eventuali danni subiti
- Prevenire i possibili attacchi fraudolenti
- Gestire al meglio la vulnerabilità dell'intero Sistema



Le attività del Centro Antifrode

Il Centro Antifrode identifica e contrasta i fenomeni fraudolenti legati al sistema di accettazione delle carte BANCOMAT e PagoBANCOMAT avvalendosi di molteplici strumenti.

ATTIVITÀ

PREVENZIONE

- Raccolta/divulgazione di informazioni sulle frodi
- Diffusione di *best practice* di settore
- Analisi dei livelli di rischio dei terminali/ processi/ sistemi
- Attività di formazione
- Convocazione/coordinamento di tavoli di lavoro con gli *Stakeholder*

CONTRASTO

- Analisi degli *incident* e dei fenomeni fraudolenti
- Diffusione dei dati sulle frodi gestiti dal Consorzio nel sistema di *Knowledge Database*
- Pianificazione di interventi correttivi
- Elaborazione di piani di contenimento perdite
- Diffusione di metodologie di risoluzione degli *incident*

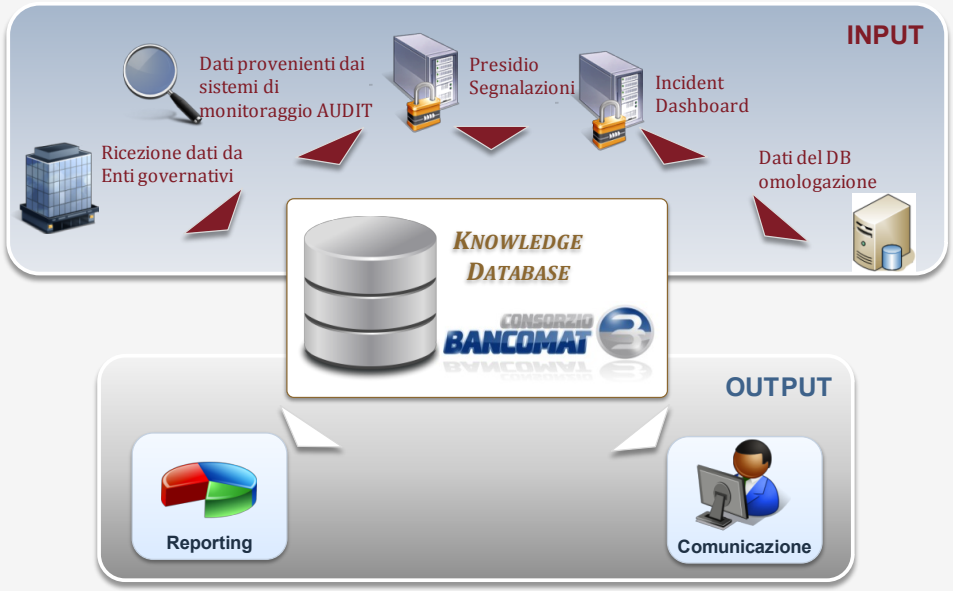
OBIETTIVI

Diminuzione delle probabilità di accadimento delle frodi

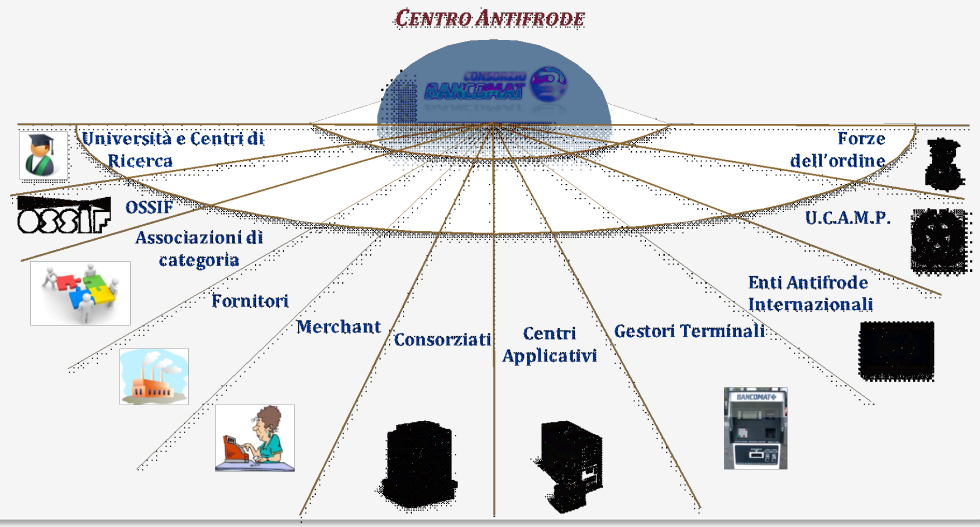
Mitigazione dei danni subiti e individuazione di soluzioni di contrasto

Rapporti e iniziative del Consorzio

STRUTTURA



PARTNER



INIZIATIVE

- Interazione attraverso *community* tra gli attori di Sistema per la raccolta, analisi e gestione centralizzata e condivisa degli *incident* e delle problematiche relative ai Circuiti domestici
- Rubrica interattiva quale strumento di *contact center* per i Fraud Manager
- Presidi Formativi per sensibilizzare gli *stakeholder* sulle tematiche relative alle frodi e alla sicurezza delle Apparecchiature
- Audit di sicurezza sui *Vendor*, *Service* e *Provider*
- Pubblicazione di opuscoli formativi

Tipologie di frodi

Negli ultimi anni i Circuiti BANCOMAT e PagoBANCOMAT sono stati investiti da due categorie di frodi, attacchi logici e attacchi fisici.

ATTACCHI LOGICI	**Compromissione dati carta**	Prevede l'installazione di strumenti capaci di leggere i dati delle carte operanti con tecnologia a banda (es.: skimmer) e di memorizzarli o di inviare gli stessi, tramite strumenti wifi, a supporti esterni.	**Remediation:** Avvio della migrazione della tecnologia delle carte allo standard microcircuito
	Cattura PIN	Prevede l'utilizzo di strumenti o comportamenti volti a ottenere il PIN della carta compromessa o catturata (ad es. micro-telecamera, apposizione tastierino, sostanze chimiche sulla tastiera e rilevazione del calore).	**Remediation**: Irrobustimento del protocollo (il PIN da solo non consente di effettuare operazioni se non che con la carta originale)
	Colloquio di tratta	Comprende tutte le tecniche di accesso non autorizzato e di intercettazione dei dati nell'ambito delle infrastrutture tra terminale, Gestore terminale e Centro Autorizzativo (ad es. l'attacco "*man in the middle*").	**Remediation**: Evoluzione del protocollo PagoBANCOMAT CB2 e introduzione della mutua autenticazione
ATTACCHI FISICI	**Cattura carta (o tasca libanese)**	Prevede la cattura della carta mediante l'inserimento di un elemento all'interno della feritoia dell'ATM. Tale frode è associata generalmente a tecniche di manomissione volte anche all'identificazione del PIN.	**Remediation**: Le risoluzioni adottate per lo *skimming* si sono rivelate efficaci anche per il contrasto a questo tipo di frode
	Cattura banconote (o *cash trapping*)	Prevede l'inserimento di elementi artigianali nello *shutter* volti a compromettere l'erogazione delle banconote.	 ***FOCUS REMEDIATION***

Tipologie di *cash trapping*

Nel corso del 2012 il Consorzio ha registrato un incremento degli episodi di *cash trapping* su terminali ATM finalizzati alla cattura delle banconote.

Le manomissioni di questo tipo possono realizzarsi con diverse modalità.

Frode a "tappo"

MODALITÀ

- Apposizione di un frontalino con pellicola biadesiva per la cattura delle banconote che sono in fase di erogazione.

CARATTERISTICHE

- Non c'è garanzia di riuscita in quanto spesso le banconote cadono, si staccano o si strappano al momento del recupero.

Frode a "forchetta"

MODALITÀ

- Inserimento di un artefatto (es. forchetta metallica) che impedisce l'erogazione delle banconote apposto durante un prelievo effettuato con una carta civetta (*).

CARATTERISTICHE

- Si attua principalmente su alcune famiglie di terminali maggiormente vulnerabili a causa del materiale in lega leggera dello *shutter*.

Frode "*reversal*"

MODALITÀ

- Esecuzione di una prima operazione di prelievo per l'inserimento di una "forchetta" metallica seguita da una seconda operazione di prelievo senza addebito sulla carta.

CARATTERISTICHE

- Si attua principalmente su alcune famiglie di terminali maggiormente vulnerabili.

(*) Con questa terminologia si indicano carte prepagate o al portatore appartenenti prevalentemente a Circuiti internazionali ed emesse anche da Issuer stranieri che, per le loro caratteristiche, sono frequentemente utilizzate per realizzare frodi di tipo *cash trapping*.

Cash trapping "a forchetta"
Modalità di realizzazione

- Il frodatore utilizza una carta civetta per effettuare un prelievo - solitamente di basso importo - e ottenere così accesso allo *shutter* aperto, che permette l'inserimento della forchetta.
- Un ignaro *card holder* avvia un'operazione di prelievo su un terminale così manomesso ma, al momento dell'erogazione delle banconote, queste rimangono incastrate nella forchetta .
- Il *card holder* viene addebitato dell'importo ma, non vedendo fuoriuscire il denaro e credendo in un malfunzionamento della macchina, si allontana dall'ATM permettendo al frodatore di appropriarsi delle banconote.
- La frode a forchetta è di tipo *one shot* (estraendo le banconote incastrate lo *shutter* si danneggia mandando l'ATM fuori uso), pertanto l'ammontare rubato potrebbe anche risultare di basso importo.

Gli ATM più colpiti sono quelli che presentano *shutter* più vulnerabili

Una variante alla frode a forchetta"tradizionale" è quella che utilizza la cosiddetta "**forchetta lunga**". In questo caso, la forma dello strumento consente l'esecuzione di più prelievi e la cattura di un ammontare maggiore di denaro.

Cash trapping "a forchetta"
Possibili risoluzioni hardware

Il Centro Antifrode ha intrapreso confronti diretti con i *vendor* maggiormente colpiti individuando alcune possibili risoluzioni di tipo *hardware*.

1. Modifica della bocchetta di uscita delle banconote per rendere più difficile l'introduzione della forchetta le cui dimensioni sono necessariamente standard (pari alle dimensioni delle cinghie di trasporto delle banconote).
2. Installazione di un telaio di rinforzo allo *shutter* realizzato in lega robusta (più difficile da violare).
3. Introduzione di una componente di ostruzione interna all'ATM e installazione di sensoristica.

BENEFICI DELLE SOLUZIONI

- → Una soluzione di tipo *hardware,* oltre ad essere efficace nel contrasto alla frode, funge anche da deterrente per il frodatore.
- → Le componenti possono essere installate anche separatamente;
- → Pur trattandosi di una soluzione meccanica, ha un costo piuttosto contenuto.

Queste soluzioni sono state ampiamente adottate dai Consorziati spingendo i frodatori a identificare rapidamente nuove modalità di attacco.

Ad oggi, su un totale di circa 48.000 ATM sono stati individuati oltre 13.000 sportelli maggiormente vulnerabili a questa tipologia di frode. Di questi, circa 2.100 sono stati dotati della *remediation* presentata.

Reversal cash trapping
Modalità di realizzazione

- Il frodatore inserisce nell'ATM una "carta civetta" ed effettua un primo prelievo (generalmente di importo esiguo)
- Il frodatore approfitta dell'apertura dello *shutter* per inserire la forchetta e ritira le banconote
- Contestualmente all'apertura dello *shutter*, il frodatore inserisce un elemento che non consente la completa chiusura dello stesso
- Il frodatore inserisce nuovamente una carta nell'ATM e avvia un secondo prelievo per l'importo massimo disponibile
- La seconda carta riceve dall'*Issuer* un'autorizzazione positiva al prelievo e l'ATM prepara le banconote per l'erogazione
- Sull'ATM si innescano una serie di anomalie (es: errore lettura scrittura *badge*, *timeout* ritiro carta, errore dispensatore banconote) generate probabilmente anche dal trattenimento dall'esterno della carta
- L'ATM invia al posto dei messaggi di notifica le anomalie registrate e spesso, a seguire, viene avviato il *reset* dell'Apparecchiatura
- La transazione si conclude senza notifica contabile e pertanto l'importo non viene addebitato sulla carta
- Il contante rimasto bloccato nella forchetta viene recuperato dal frodatore

In molti casi non è stato rilevato alcun danno allo *shutter* per il recupero delle banconote grazie al dispositivo inserito per bloccarne la chiusura.

Reversal cash trapping
Caratteristiche

Il *reversal cash trapping* consente di ottenere nell'immediato maggiori benefici rispetto alla tradizionale frode a "forchetta".

- *Non danneggiare lo shutter in modo da poter ripetere l'operazione più volte sul medesimo terminale a breve distanza di tempo*
- *Poter agire in modo autonomo, senza la necessità di un'operazione da parte di un titolare carta*
- *Minimizzare il rischio di essere individuati e bloccati dalle Forze dell'Ordine*
- *Riuscire ad ottenere importi molto più elevati superando i controlli autorizzativi da parte delle Banche Issuer*

Il Centro Antifrode ha individuato alcune possibili risoluzioni

SOLUZIONI HARDWARE

- Adozione di sensori che inibiscono il prelievo nel momento in cui rilevino elementi estranei sul *presenter* o sulle cinghie di trascinamento.

SOLUZIONI SOFTWARE

- Soluzioni *patch* per ritardare il posizionamento delle banconote sulla cinghia del dispensatore rispetto al *timeout* di espulsione della carta;
- Notifiche all'*host* GT in presenza di sequenze di anomalie registrate dall'ATM per forzare la notifica contabile.

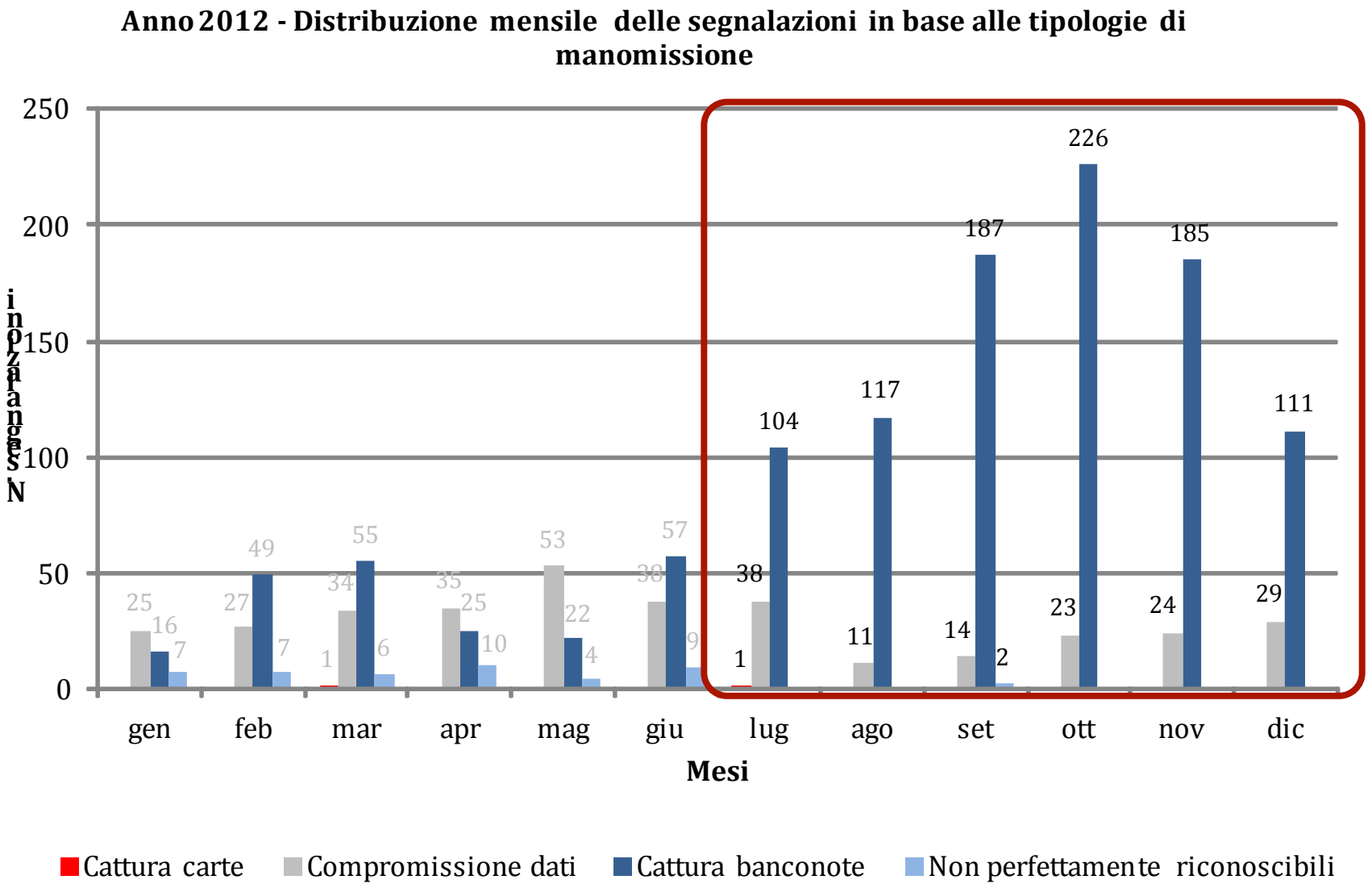
Evoluzioni del reversal cash trapping
Caratteristiche

Il Consorzio ha identificato all'inizio del 2013 un'ulteriore tipologia di *reversal*, denominata ***instant reversal cash trapping***, che si differenzia dalla prima in quanto caratterizzata dalla realizzazione di un'unica operazione in cui avvengono contestualmente sia l'inserimento della forchetta nello *shutter* che il prelievo senza addebito sulla carta.

- Il frodatore riesce ad inserire nell'ATM una forchetta metallica e un elemento che non consente la completa chiusura dello *shutter* ed effettua un prelievo per il massimo importo disponibile
- La carta riceve dall'*Issuer* un'autorizzazione positiva al prelievo e l'ATM prepara le banconote per l'erogazione
- Sull'ATM sono innescate una serie di anomalie (es: errore lettura scrittura *badge*, *timeout* ritiro carta, errore dispensatore banconote) generate probabilmente anche dal trattenimento dall'esterno della carta
- L'ATM invia al posto dei messaggi di notifica le anomalie registrate e spesso, a seguire, viene avviato il *reset* dell'Apparecchiatura
- La transazione si conclude senza notifica contabile e pertanto l'importo non viene addebitato sulla carta
- Il contante rimasto bloccato nella forchetta viene recuperato dal frodatore

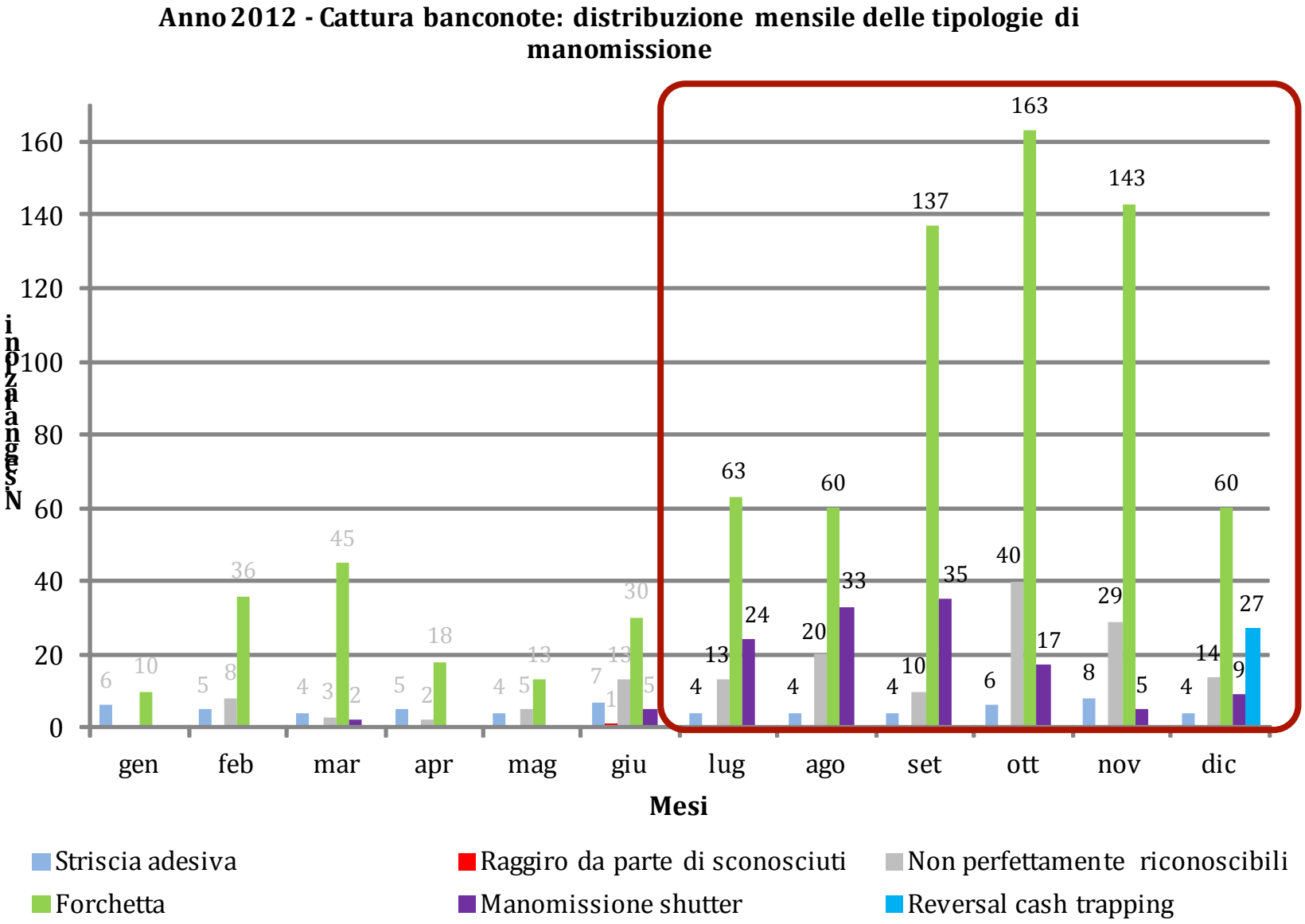
STATISTICHE FRODI ATM - 2012

Distribuzione mensile delle segnalazioni



STATISTICHE FRODI ATM - 2012

Cattura banconote



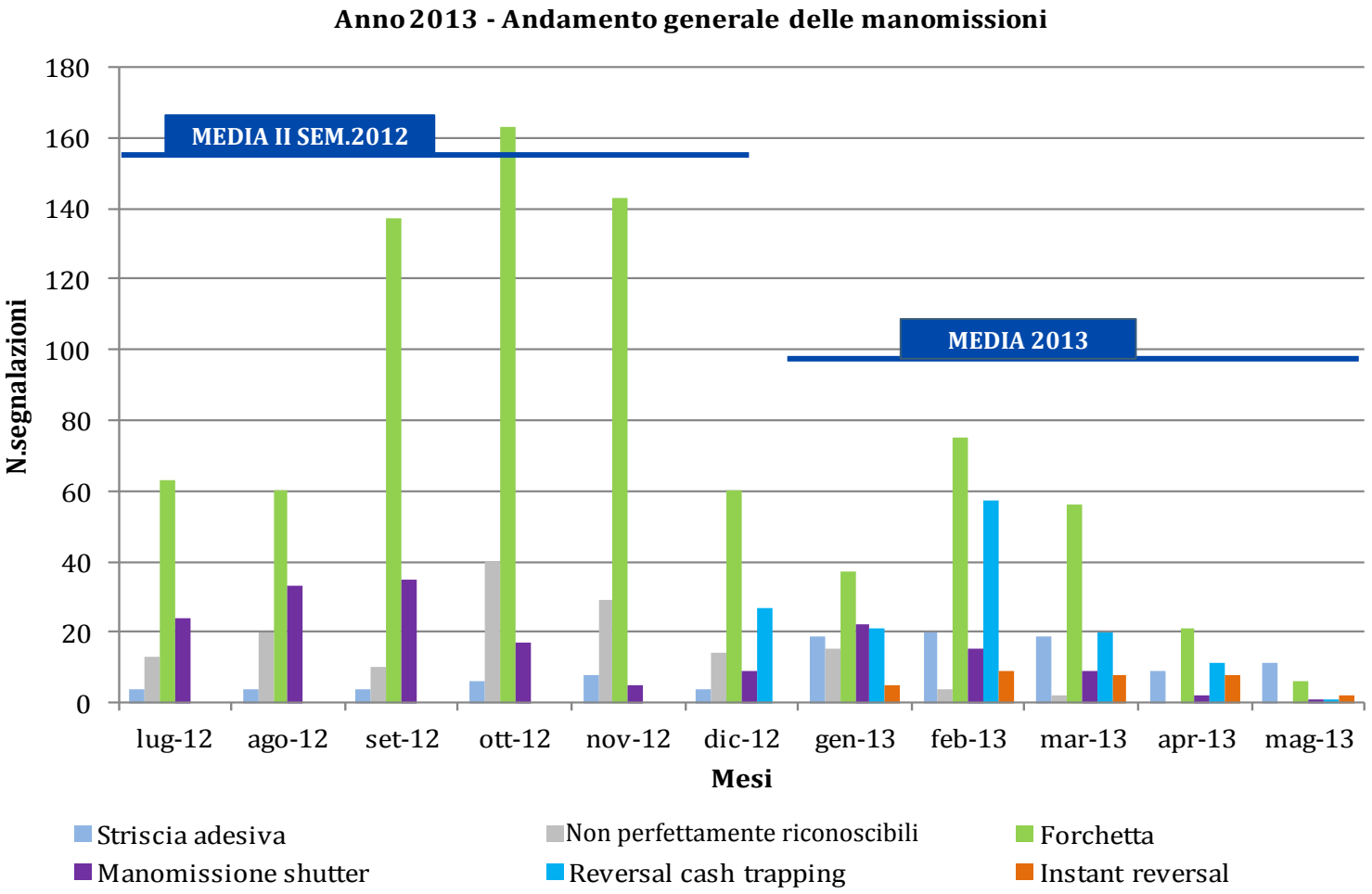
STATISTICHE FRODI ATM - 2013

Cattura banconote

Grazie alle attività di monitoraggio condotte, il Centro Antifrode ha rilevato nei primi mesi del 2013 due fenomeni:

1. Dall'inizio dell'anno la media mensile delle segnalazioni è diminuita rispetto a quella riferita al secondo semestre del 2012 (**-38%**);

2. A dimostrazione dell'efficacia delle **strategie di remediation** messe in atto dalle banche, si è assistito a un *turnover* sempre più rapido di nuove varianti di manomissione.



War on cash

CENNI STORICI

A partire dal 2007 l'ABI e la Convenzione Per la Gestione del Marchio BANCOMAT (CO.GE.BAN) hanno condiviso la politica di "guerra al contante" (*war on cash*) al fine di abbattere, tra l'altro, i costi di gestione del contante, tra i quali una delle voci più significative era e continua ad essere quella relativa alle frodi.

AREE DI RISCHIO

I rischi maggiori si concentrano sui dispostivi di pagamento *unattended* dotati di cassaforte, come ad esempio:

- Totem carburanti
- *Self service*
- *Vending machine*

OGGI

In uno scenario di instabilità economica, politica e sociale, nuovi metodi e tecniche artigianali per la realizzazione di frodi si stanno diffondendo maggiormente rispetto a modalità di manomissione caratterizzate da un alto contenuto tecnologico.

Device unattended

Fra i più appetibili *device* della categoria *unattended* quelli attestati nel settore Petrol risultano oggi essere i più attaccati

MAGGIORE REDDITIVITÀ

PER SINGOLO ATTACCO

E' stato rilevato un incremento del capitolo di spesa legato ai furti con scasso **pari al doppio rispetto all'anno precedente** (la media si assesta su un episodio al mese di furto con scasso e l'area più colpita è il sud Italia).*

* Fonte dati unione Petrolifera

Il ruolo del Circuito

La migrazione dal pagamento *cash* al pagamento con carta è stata rallentata anche da una non completa fiducia nella sicurezza negli strumenti di pagamento elettronici.
Il Consorzio BANCOMAT, nell'ambito della promozione degli strumenti alternativi al contante, profonde il proprio impegno nell'irrobustimento del Circuito anche con l'evoluzione di un ***framework* di sicurezza** complesso che combina più strategie.

Fraud Risk Assessment

- Analisi e monitoraggio del livello di rischio residuo relativo alla gestione delle frodi
- Rilevazione qualitativa delle probabilità di accadimento delle singole tipologie di frodi

Vulnerability Assessment

- Verifica della vulnerabilità di tecnologie, dispositivi e soluzioni hardware/software su terminali ATM e POS
- Valutazione del rischio frodi a cui risulta esposta la rete di accettazione

Definizione standard sicurezza

- Emanazione/ aggiornamento di nuovi presidi normativi per la rete di accettazione/ emissione
- Emanazione di nuovi standard tecnici di sicurezza per la rete di accettazione/ emissione
- Definizione di nuovi processi di omologazione (omologazione di 2° livello)

Più fiducia per noi…

…maggiore sicurezza per te!

Grazie