CERTFin

DENARO E SICUREZZA NELL'ERA DIGITALE

24 novembre 2023

Mario Trinchera
Technical Coordinator

TLP: GREEN

Report Sicurezza e Frodi 2023
…in Sintesi

Nel retail aumenta il controvalore delle frodi tentate

+35% *Rispetto allo scorso anno*

Si riduce la quota di Frodi Effettive sul totale transazioni anomale

6%

…e, significativamente, anche il loro controvalore

-50% *Rispetto allo scorso anno*

La transazioni fraudolente effettive sono spesso avviate dal cliente

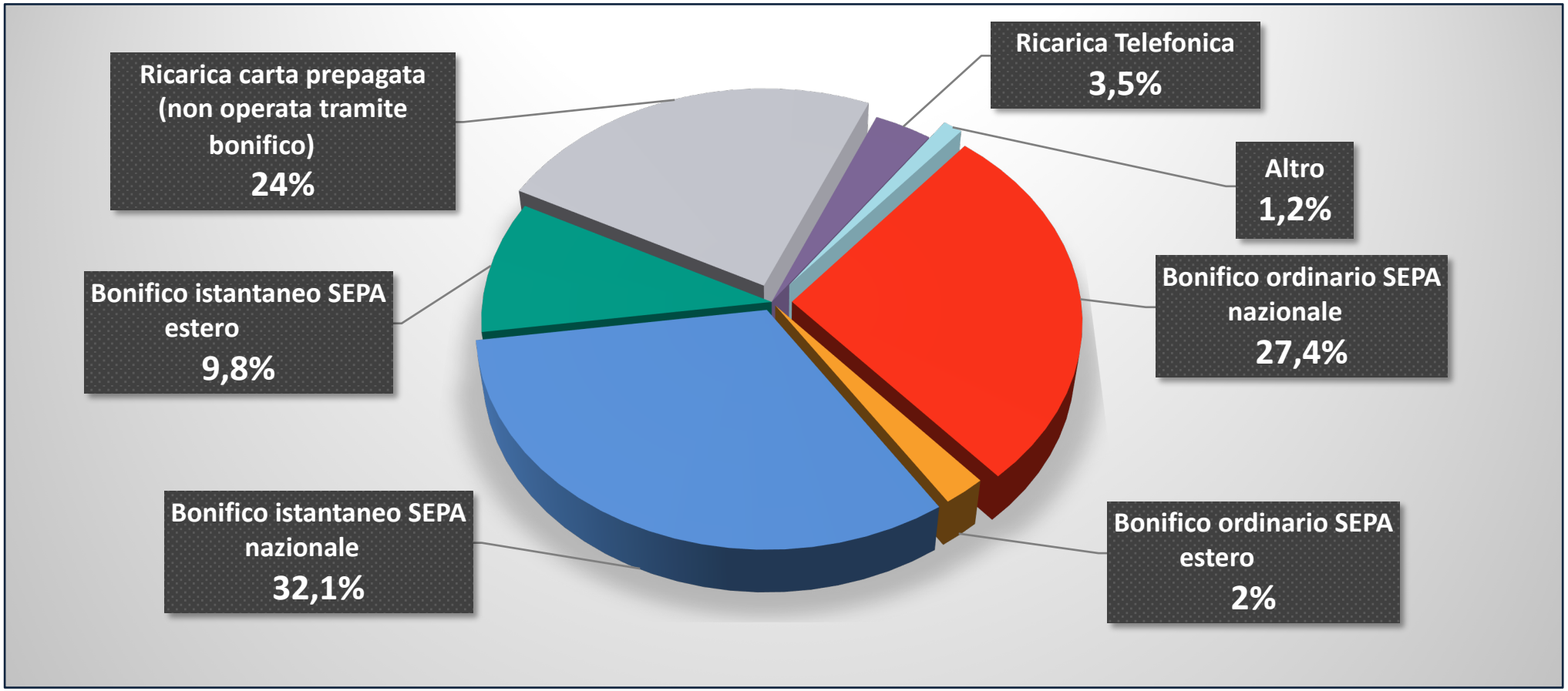
65%

Ancora molto elevato l'importo delle frodi «recuperate»

≈14 *Milioni di euro*

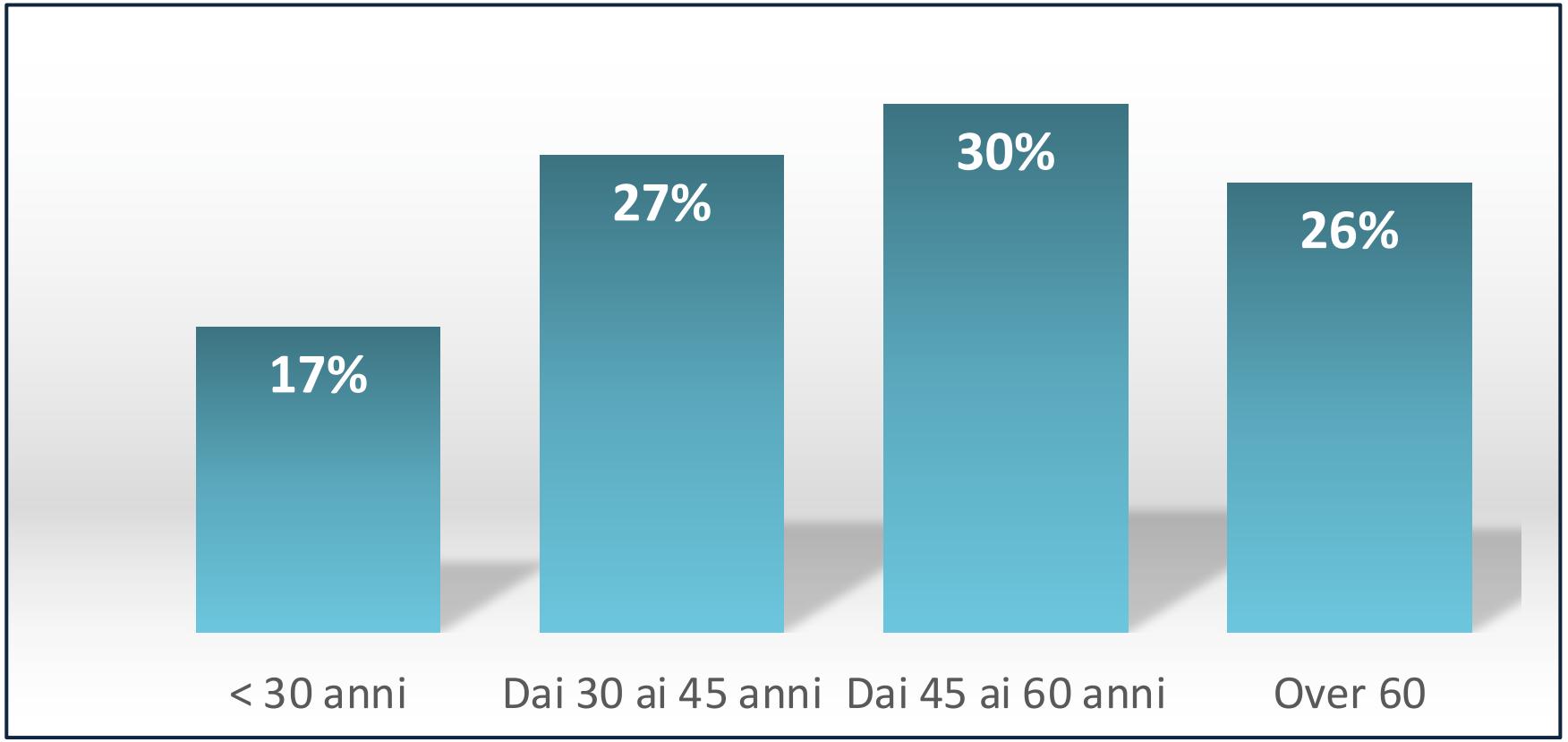
Transazioni Fraudolente Effettive

Ripartizione percentuale per tipologia – analisi sul numero di accadimenti
(segmento Retail)



Età delle vittime

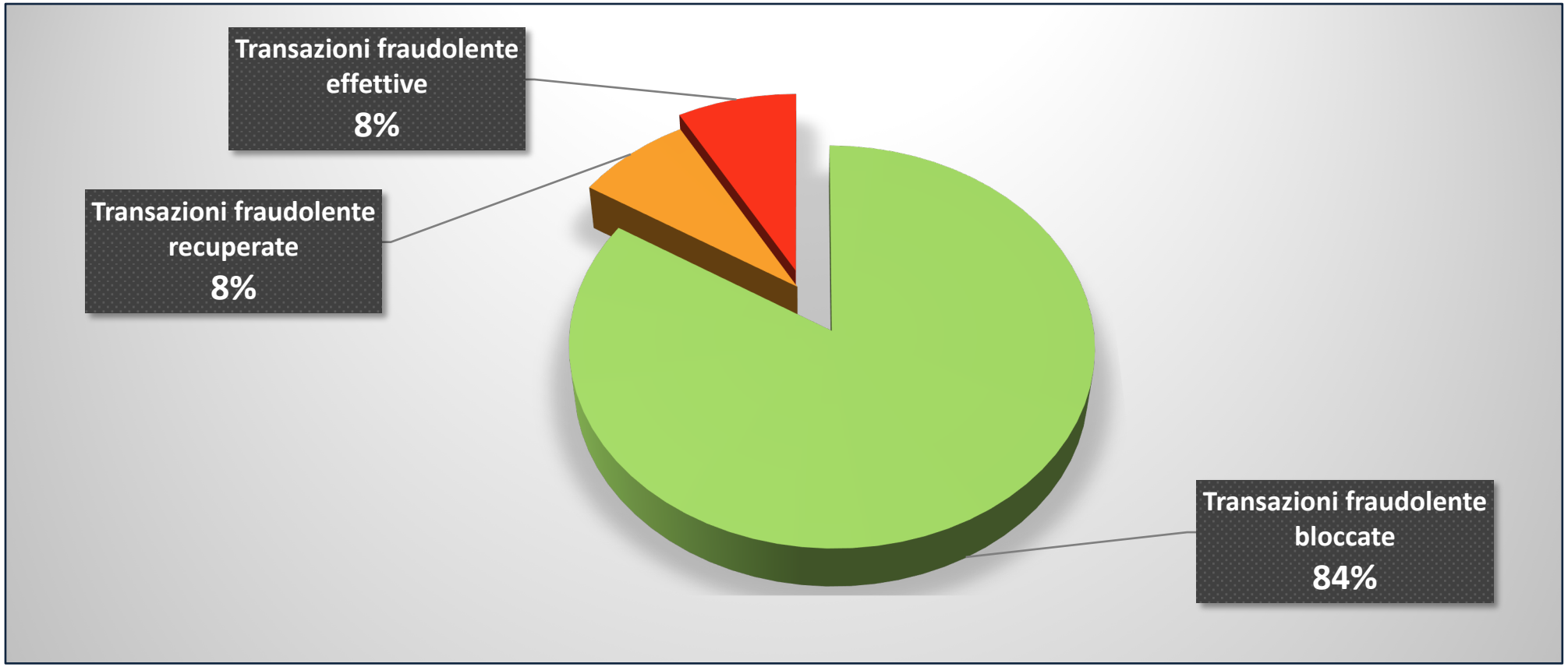
Ripartizione percentuale per fascia d'età – analisi sul numero di accadimenti
(segmento Retail)



Transazioni Anomale

Ripartizione percentuale – analisi sul controvalore in euro

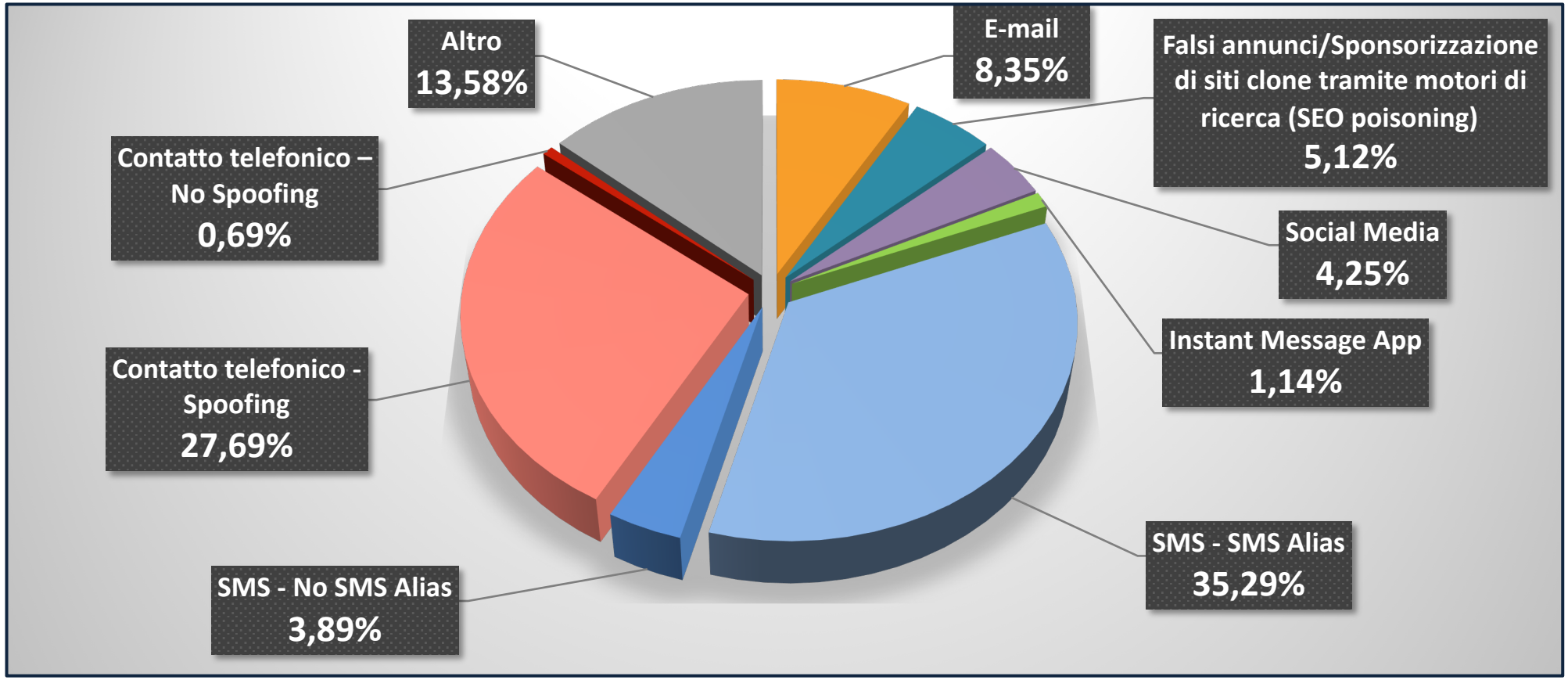
(complessivo Retail e Corporate)



Fraud Chain

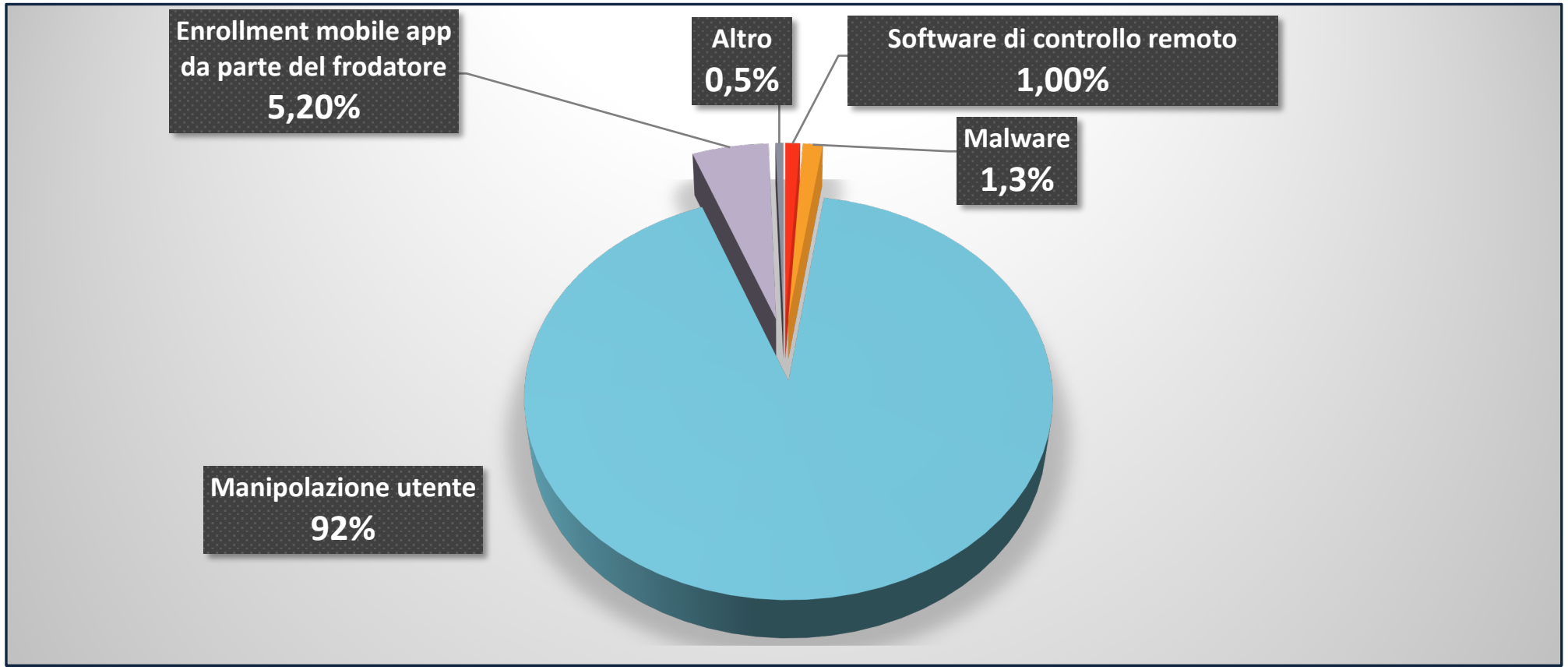
Punto di primo contatto/vettore iniziale della frode

(segmento Retail)



Fraud Chain

Tecnica utilizzata per finalizzare la frode
(segmento Retail)



Attacchi Basati sulla Scarsa Consapevolezza (1/2)

#1

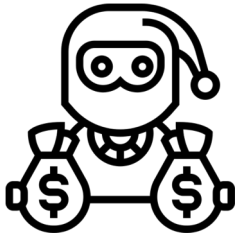
La vittima riceve una telefonata apparentemente proveniente dalla sua banca durante la quale un sedicente responsabile di sicurezza lo informa che il suo conto è in mano a degli hacker, che i suoi soldi sono in pericolo e che vanno **immediatamente spostati su un conto di appoggio.**

#2

La vittima, colta dal panico, si affretta a seguire le indicazioni fornite dal falso operatore di banca, tra cui vi è anche l'IBAN sul quale versare «temporaneamente» i soldi che saranno così messi «al sicuro».

#3

L'agitazione della vittima richiama però l'attenzione della moglie la quale si fa spiegare cosa sta accadendo e si unisce all'angoscia del marito. Il frodatore a quel punto **chiede se anche la signora ha un c/c presso la stessa banca**, in modo da poter effettuare una verifica anche sul suo conto.



#4

Alla risposta affermativa, la dinamica viene replicata: **il frodatore riferisce che purtroppo anche sul conto della signora risultano accessi non autorizzati** e che «per sicurezza» è meglio trasferire temporaneamente anche i suoi soldi sul conto di appoggio.

***Durata Totale**: 70 minuti circa*

Il frodatore insinua ansia nella vittime, legittimato da una comunicazione apparentemente proveniente dalle banca. Lascia sgomenti la «fortuna» dei criminali nel trovare, con una sola chiamata, due vittime che si «gettano» tra le loro braccia senza esitazione.

Attacchi Basati sulla Scarsa Consapevolezza (2/2)

#1

Il cliente viene agganciato attraverso banner o attraverso normali telefonate nelle quali vengono proposti investimenti in crypto-valute. **Attratto dai rendimenti apparentemente molto appetibili**, la vittima decide di aprire un account e di fare un primo versamento.

#2

La vittima ottiene l'accesso ad una piattaforma di trading ed **inizia a versare con regolarità fondi** che, seguendo le indicazioni dei frodatori, sembrano portargli alti rendimenti.

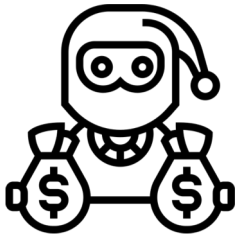
#3

Dopo un certo tempo, ad esempio quando prova a trasferire i presunti grandi guadagni sul suo c/c, **la vittima comprende di essere stata truffata e subentra la disperazione.**

#4

I frodatori ricattano la vittima e, dietro la promessa di restituirgli parte dei suoi stessi soldi, **lo costringono a mettere a disposizione il suo c/c ed operare come «mulo»** oppure a prestare la sua identità per altre attività illecite.

***Durata Totale**: variabile*



I criminali sfruttano due volte l'ingenuità delle vittime: prima inducendole a investire denaro in attività senza nessuna possibilità di ritorni e poi costringendole a mettersi a disposizione della stessa organizzazione criminale che li ha colpiti.

Attacchi Basati sulla Creatività (1/2)

#1

I frodatori sottraggono la corrispondenza contenente carte in via di rinnovo durante le varie fasi di consegna.
I criminali si ritrovano con le carte ma **non conoscono né i codici di sicurezza né i numeri di telefono delle potenziali vittime.**

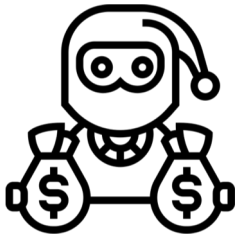
#2

I frodatori, conoscendo l'indirizzo dei clienti, si recano presso le loro abitazioni ed appongono sulle cassette delle lettere **falsi adesivi DHL** che annunciano una mancata consegna ed invitano i clienti a concordarne una nuova chiamando il numero di cellulare ivi riportato.

#3

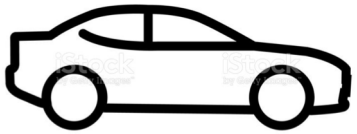
Quando il cliente chiama i frodatori memorizzano il suo cellulare e successivamente lo richiamano **inducendolo abilmente a riferire il proprio PIN**.
A quel punto i criminali procedono ad utilizzare la carta senza difficoltà.

***Totale**: variabile*

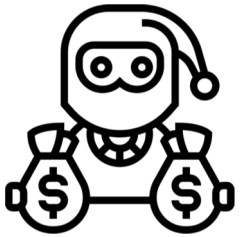


Qui i criminali mescolano reati tradizionali con reati informatici, facendo leva sulle loro abilità di social engineering per ottenere le informazioni necessarie ad operare in maniera non autorizzata.

Attacchi Basati sulla Creatività (2/2)



#1
Le vittime si trovano a dover parcheggiare in grandi centri urbani in cui non è facile trovare abbondanza di posti auto.
Invariabilmente, **l'auto viene parcheggiata male o in divieto di sosta.**



#3
Le vittime procedono al pagamento seguendo le istruzioni a cui il QR code rimanda, il quale però **non è legato al conto corrente della polizia municipale bensì a quello dei criminali**.

#2
Al momento di ritornare presso la propria autovettura, **le vittime ritrovano sul parabrezza una (falsa) multa per divieto di sosta**. Sul documento sono riportate anche le istruzioni per il pagamento, il quale, **se effettuato subito ed attraverso il QR code allegato**, sarà ridotto in una certa misura.

Durata Totale: *minuti*

Attacco tanto semplice quanto efficace, fa leva sul sensazione della vittima di trovarsi in difetto e può contare su uno schema non ancora diffuso e dunque non facilmente riconoscibile dal cittadino comune.

Attacchi basati su tecniche miste

10:37

#0
Premessa: i frodatori sono già in possesso di alcuni dati della vittima: nome, numero di cellulare, a volte anche delle credenziali di accesso al conto.

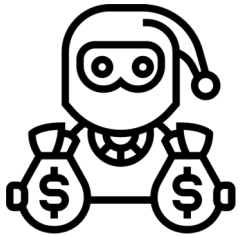
#1
La vittima riceve una telefonata, **apparentemente proveniente dal 113**, in cui un falso agente lo avvisa che il suo conto è stato compromesso, che sono già in corso indagini e che la banca lo chiamerà a breve per riportare in sicurezza il suo conto corrente.

10:40

#2
Poco dopo, la vittima riceve una chiamata da un (falso) operatore del reparto antifrode che lo induce a disinstallare l'app della banca e ad installare un malware mascherato da tool di sicurezza.

11:02

#3
il malware inoltra tutti gli OTP ricevuti sul device della vittima ad un numero in mano ai frodatori, che in questo modo possono finalizzare un certo numero di transazioni.

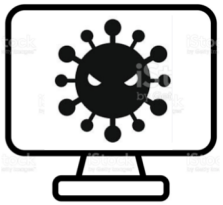


***Totale**: meno di 30 minuti*

Il frodatore insinua ansia nella vittima, legittimata attraverso una comunicazione apparentemente proveniente dalle forze dell'ordine. Alla successiva chiamata, già annunciata, la vittima si «getta» nelle mani dei frodatori ed esegue senza esitare quanto gli viene detto di fare.

Attacchi basati su una componente tecnica significativa

#2
Il software malevolo resta silente anche per settimane, limitandosi a raccogliere info del PC su cui si trova. Solo quando l'infetto viene valutato «idoneo» a diventare vittima, il sw invia le info al suo C&C e scarica una nuova componente software che **combinata con la precedente diventa concretamente dannosa**.



#4
il malware, **al fine di ritardare la detection** e utilizzando specifici webinject, **maschera la compromissione** sia alterando i dati mostrati a video sia alterando eventuali pdf richiesti dall'utente relativi all'estratto del conto corrente aziendale.

#1
L'azienda riceve una **PEC** apparentemente attendibile ma il cui allegato è malevolo.
Spinto dal falso senso di sicurezza il destinatario apre l'allegato infettando il PC.

#3
All'atto della sottomissione di una nuova transazione da parte dell'utente, **il malware interviene sostituendo l'iban del destinatario legittimo con un altro** ed alterando i dati riepilogativi mostrati al termine dell'operazione.

***Durata Totale**: Diverse Settimane*

Attacco molto sofisticato le cui vittime sono scelte con cura. La frode viene condotta sfruttando il falso senso di sicurezza indotto dalla PEC e mettendo in campo una componente tecnica decisamente superiore alla media.

Thank You!

CERTFin

Defend. Inform. Evolve.

For more info visit www.certfin.it or write to ricerca@certfin.it