CERTFin

29.11.2024

Threat Landscape Scenario for the Italian Financial Sector

Romano Stasi Direttore Operativo **CERTFin**
Segretario Generale **ABI Lab**

An Italian Threat Landscape Scenario

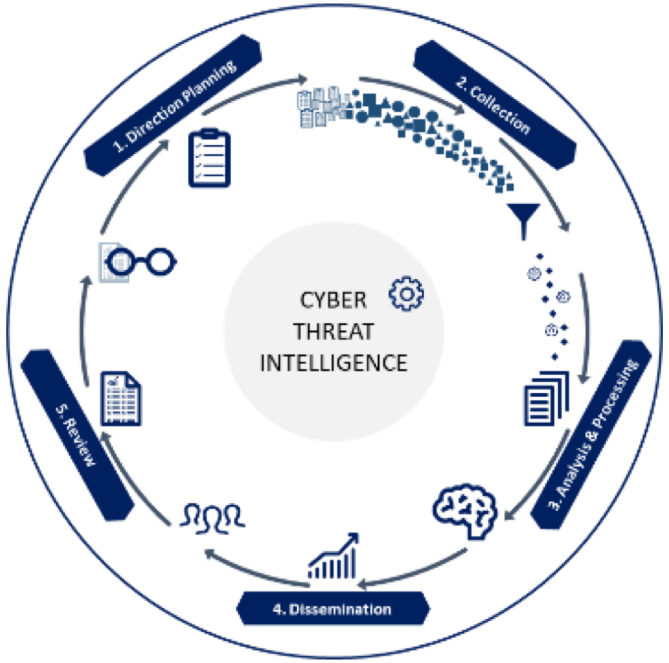
CERTFin

With the TLS, CERTFin describes

THE CYBER THREATS LANDSCAPE

to inform the Italian financial sector.

INTELLIGENCE ACTIVITIES PLAY A KEY ROLE: they increase the amount of intelligence of various organizations to help understanding the evolution of cyber threats (well-established or emerging), and to guide towards the preparation of countermeasures.



A national Landscape to promote the development of Targeted Threat Intelligence within the Constituency

Threat Landscape Scenario (2024 H2)

CERTFin

Russia–Ukraine / Israel-Hamas conflicts & Hacktivism

- By far the biggest impact on the cyber threat landscape in 2023/2024 has been caused by the Russia-Ukraine and Israel-Hamas wars.
- PSPs with operations in geopolitically conflicted jurisdictions could encounter severe business disruption.
- Existing geopolitical tensions exacerbated by the ongoing conflicts sparked a flood of hacktivist activity that continues unabated.
- New synergies and collaborations arise between hacktivist groups (e.g., NoName057(16), Anonymous Russia, Mysterious Team Bangladesh, 22C, etc.).
- **Forecast: We may observe new coalitions and attempted attacks on critical Western infrastructure.**

Generative AI

- Generative AI technology is a form of artificial intelligence that can generate texts, images, sounds, and other content based on natural language instructions or data inputs (e.g., ChatGPT).
- Enterprise use cases are emerging with the goal of increasing the efficiency of security teams conducting operational tasks.
- In contrast, there are concerns that AI systems like ChatGPT could be used to:
  - Identify and exploit vulnerabilities
  - To create phishing e-mails for malware delivery and fraud activity
  - Generate malware
  - Clone voice

DDos Attacks

- DDoS attacks are increasing globally and sometimes associated with extortion.
- As for the attack size and duration the majority of attacks are short and small and the most popular attack vectors were DNS-based DDoS attacks, SYN floods and UDP based attacks.
- Increase of L7 DDoS attacks, sometime mixed with L4 DDoS attacks, mostly carried out and claimed by hacktivist groups.
- While most of these attacks have low or no impact, the financial services sector remains one of the sectors most targeted.
- **Forecast: Possible increase of DDoS attacks' success rate.**

Supply chain attacks & 3rd party compromise

- As organizations become increasingly interconnected and complex, the supply chain threat is growing.
- Italian SMEs, usually providers of PSPs, continue to be targeted by notorious ransomware groups. Despite the registered impacts have been limited so far, the risk of propagation to other PSPs remains high.

- **Forecast: Supply chain threats will continue to be a key theme, as organizations become increasingly interconnected and complex.**

TLP:AMBER

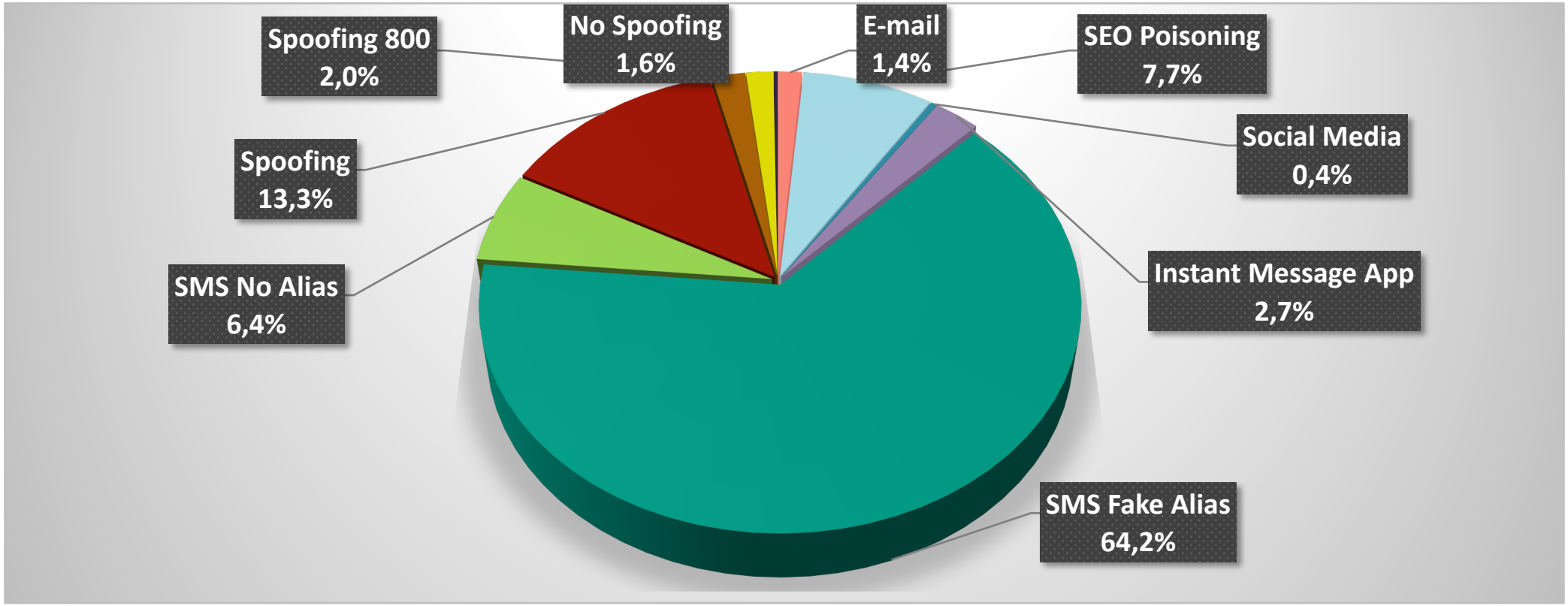
CERTFin

29 novembre 2024

La collaborazione come strumento per prevenire le frodi: l'esperienza della campagna I Navigati

Romano Stasi
Direttore Operativo CERTFin

Fraud chain: inizializzazione della frode

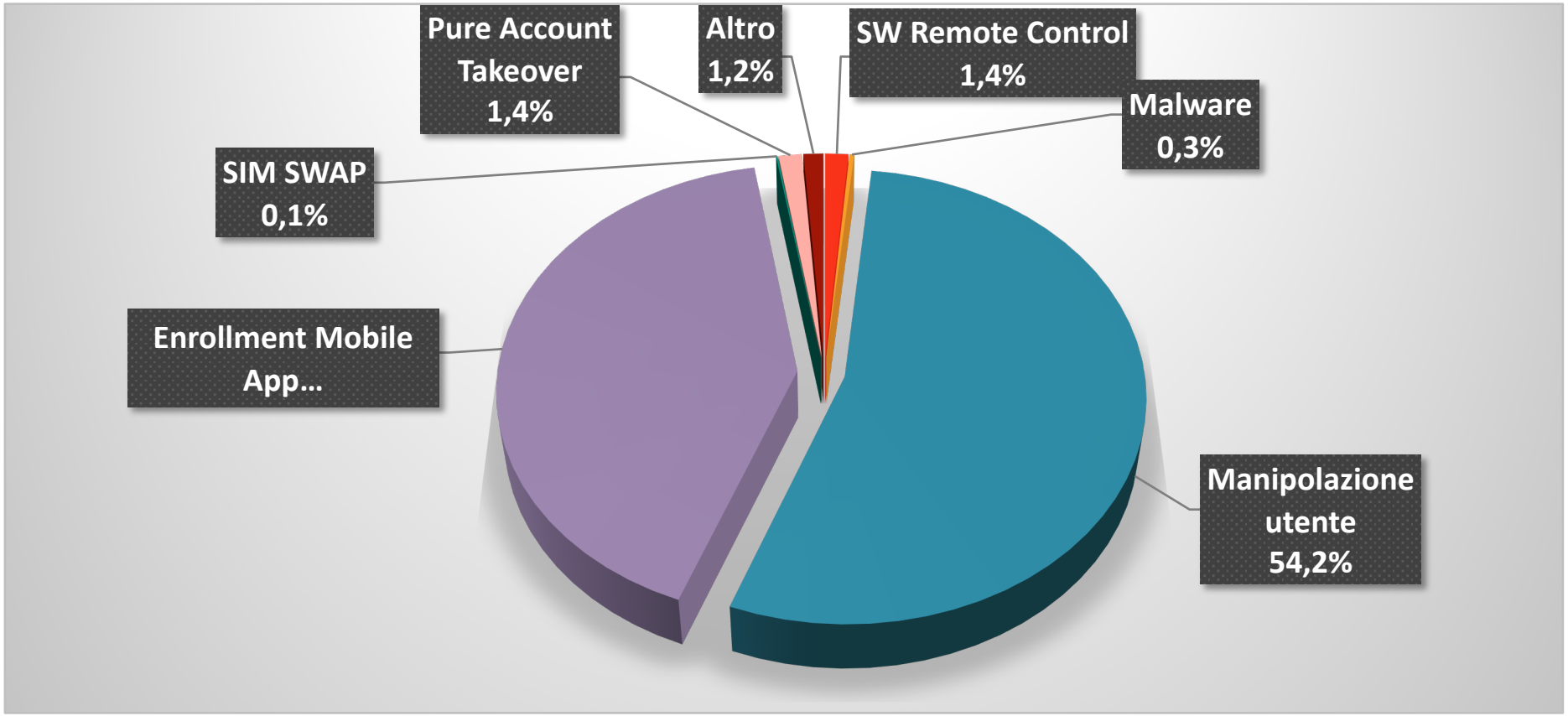


Fonte: Report CERTFin Sicurezza e frodi informatiche in banca, 2024

Nel 2023, in Italia, oltre l'87% delle frodi riuscite è stato effettuato utilizzando chiamate telefoniche e messaggi SMS come punto di contatto iniziale.

E' necessaria un azione congiunta con gli operatori di telecomunicazione per ridurre alias e spoofing

Fraud chain: finalizzazione della frode



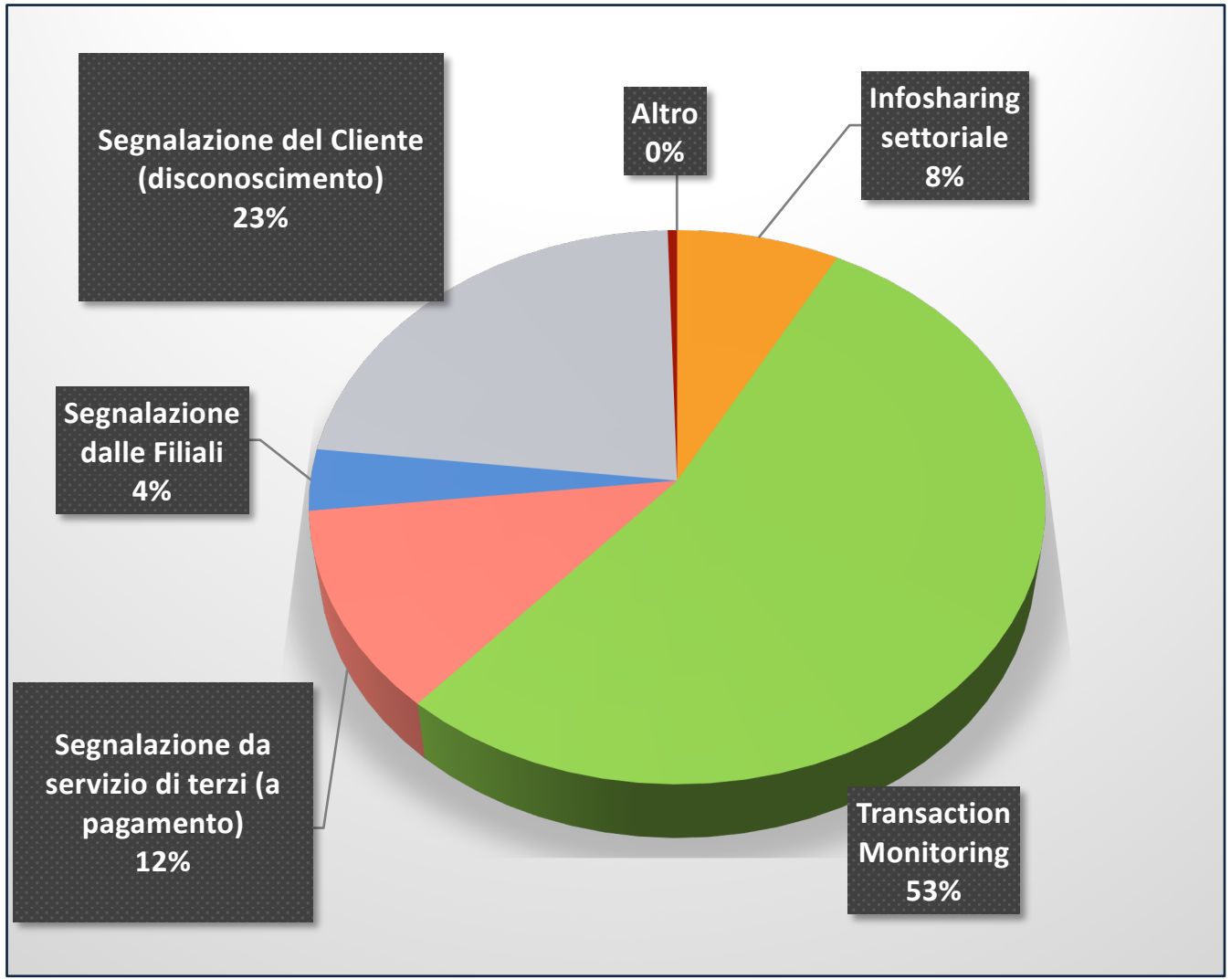
Fonte: Report CERTFin Sicurezza e frodi informatiche in banca, 2024

La manipolazione dell'utente è lo schema fraudolento più comune per portare a termine la frode (oltre il 50%).

Il cliente viene convinto a dare informazioni utili ad effettuare un pagamento o a farlo direttamente

Deve crescere la consapevolezza del cittadini per non cadere in raggiri e truffe digitali !!!

Fonti di segnalazione di operazioni fraudolente



Fonte: Report CERTFin Sicurezza e frodi informatiche in banca, 2024

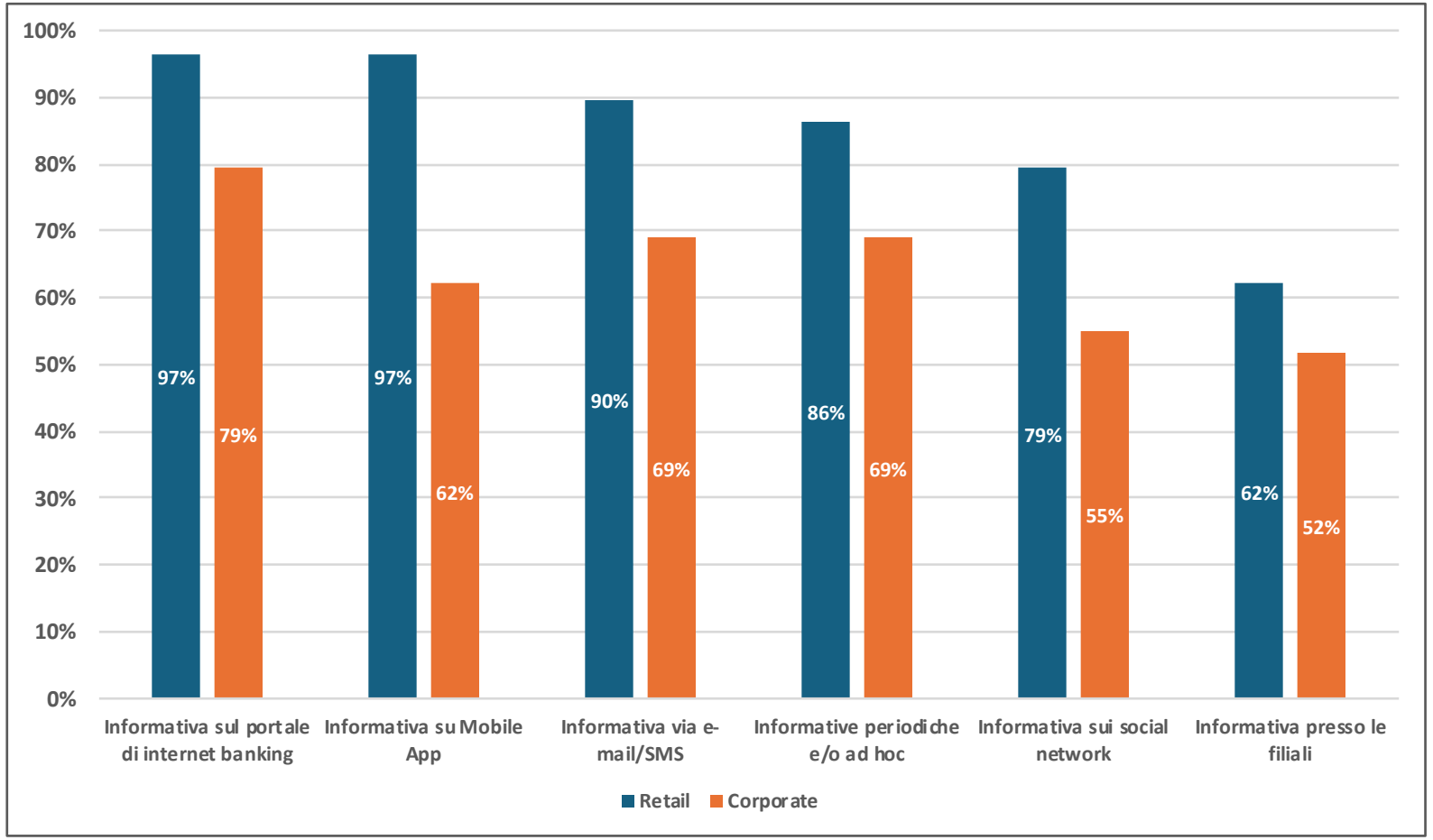
Il **disconoscimento del cliente** resta la seconda modalità di rilevazione nel segmento retail (23%).

Le **iniziative di cybersecurity awareness** svolgono un ruolo fondamentale perché sempre più clienti siano in grado di **non autorizzare una transazione anomala o** di **disconoscerla** il prima il possibile.

Tempismo e velocità nel comunicare un disconoscimento coinvolgendo banche e forze dell'ordine.

La sensibilizzazione dei rischi cyber - Canali

Le banche si adoperano su tutti i propri canali di comunicazione con la clientela, sia retail che corporate. per aggiornare continuamente sulle attenzioni da avere per ridurre al minimo i rischi.

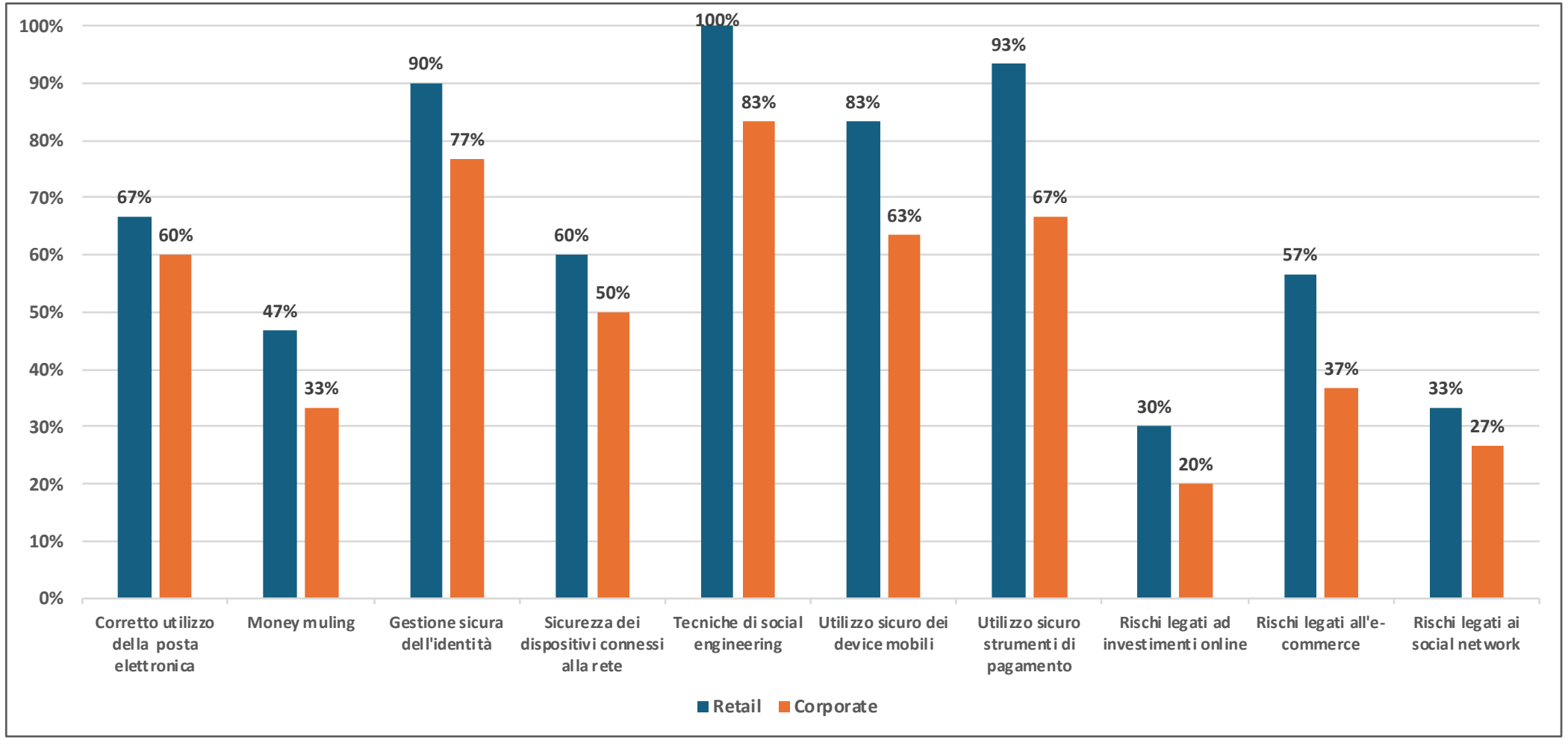


Canali utilizzati dalle organizzazioni per sensibilizzare la clientela sull'evoluzione delle frodi informatiche

Fonte: CERTFin, Report sicurezza e frodi informatiche in banca, maggio 2024, 28 rispondenti

La sensibilizzazione dei rischi cyber - Tematiche

Numerose sono le tematiche sui cui è importante che la clientela sia informata nel continuo.



Tematiche affrontate durante le sessioni di sensibilizzazione della clientela corporate e retail

Fonte: CERTFin, Report sicurezza e frodi informatiche in banca, maggio 2024, 30 rispondenti

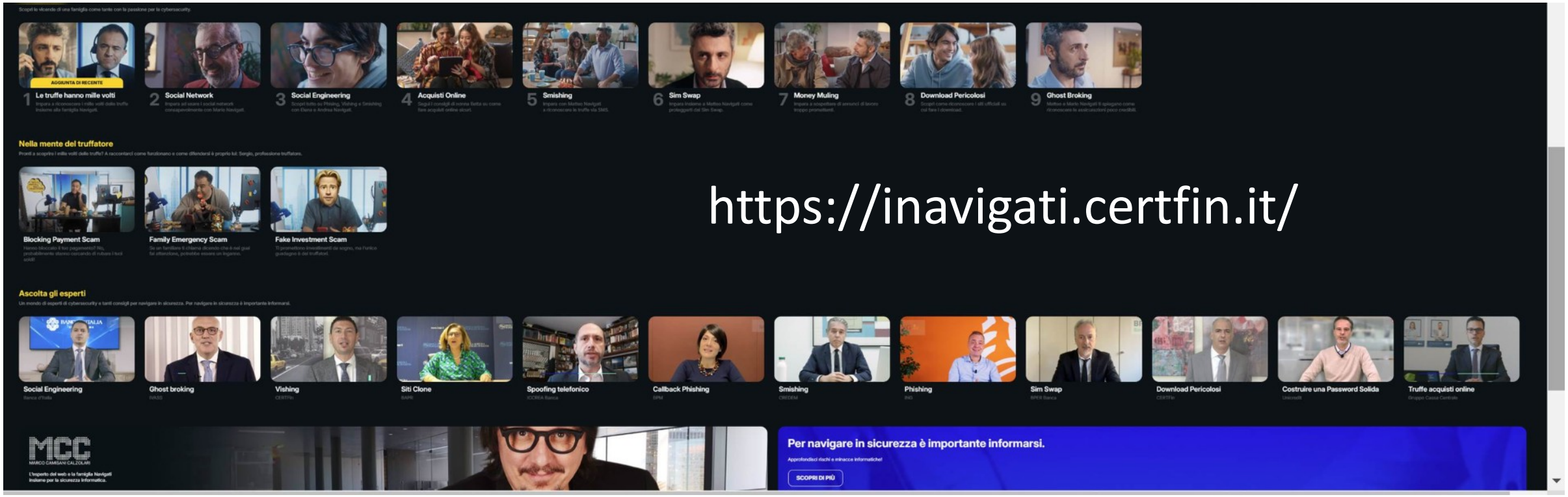
I Navigati 2024 campagna per i clienti retail

Partita il 7 ottobre, in coincidenza con il mese della cybersecurity, la nuova campagna presenta un nuovo claim: “**Le truffe hanno mille volti — impara a riconoscerle**”, un messaggio che pone l'accento sull'importanza della verifica.

L'iniziativa invita il pubblico a non fidarsi ciecamente di chiamate, messaggi o email che sembrano provenire da fonti affidabili, ma a **verificare sempre l'identità del mittente**. L'**obiettivo** è far comprendere che dietro una comunicazione apparentemente innocua potrebbe nascondersi chiunque, inclusi truffatori esperti.

Forte impulso alla diffusione del messaggio sui social network è stato dato da META che ha aderito alla campagna 2024 con convinzione e spirito di collaborazione.

I Navigati 2024



Nel sito si possono trovare video che parlano di:

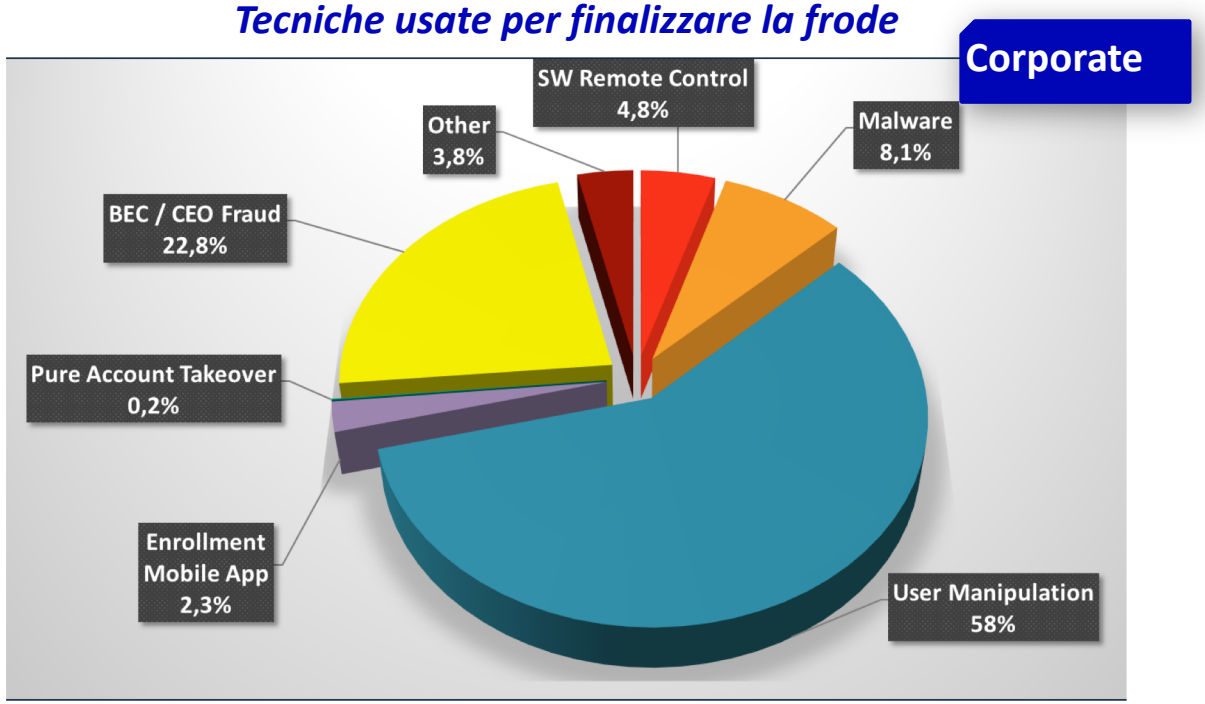
Spoofing, Social Network, Social engineering, acquisti on line, Smishing, Sim Swap, Money Muling, Download Pericolosi, Ghost Broking, Blocking payment scam, Family emergency scam, Fake investment.

Cybersicuri – campagna per i clienti corporate

Partita nel 2023 la campagna vuole sottolineare le frodi legate all'impersonificazione, ad esempio il CEO, nelle quali il dipendente di azienda amministrativo viene indotto ad effettuare un pagamento o aiuto il frodatore nel finalizzare un pagamento.

La campagna sottolinea anche l'importanza di investire in sicurezza informatica nelle aziende.

Tecniche usate per finalizzare la frode



Source: 2024 CERTFin report on information security and fraud in the banking sector

CYBERSICURI IMPRESA POSSIBILE

https://cybersicuri.certfin.it/