19 MAGGIO 2022

GRUPPO CASSA CENTRALE

Andamento fenomeno delle frodi 1 gennaio 2021- 30 aprile 2022

Simone Maga

GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO

GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO

CAPOGRUPPO

COORDINAMENTO DEL GRUPPO

LOCALISMO

EFFICIENZA

COOPERAZIONE

Cassa Centrale Banca ricopre il ruolo di direzione e coordinamento del Gruppo, che grazie all'elevata solidità patrimoniale e al basso profilo di rischio, si impegna a mantenere il Gruppo stabile, sicuro ed efficiente.

CASSA CENTRALE BANCA
CREDITO COOPERATIVO ITALIANO

SOCIETÀ CONTROLLATE

CLARIS RENT

ASSICURA

CENTRALE CREDIT SOLUTIONS

CENTRALE CASA
AGENZIA DI INTERMEDIAZIONE IMMOBILIARE

CLARIS LEASING

Centrale Trading

CENTRALE SOLUZIONI IMMOBILIARI

Prestipay

NEAM

allitude
empower your bank attitude

Allitude S.p.A nasce dall'esigenza di disporre di un'unica società di servizi informatici e bancari, in linea con le aspettative della Vigilanza. La struttura è finalizzata a sviluppare sinergie operative e costruire nel tempo poli specialistici al servizio dell'evoluzione del Gruppo e delle banche.

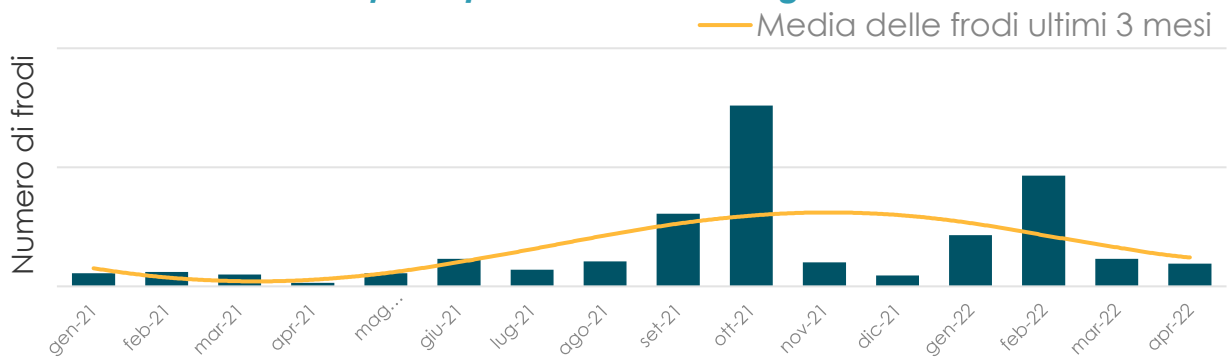
70 BANCHE DI CREDITO COOPERATIVO

>11.000 DIPENDENTI

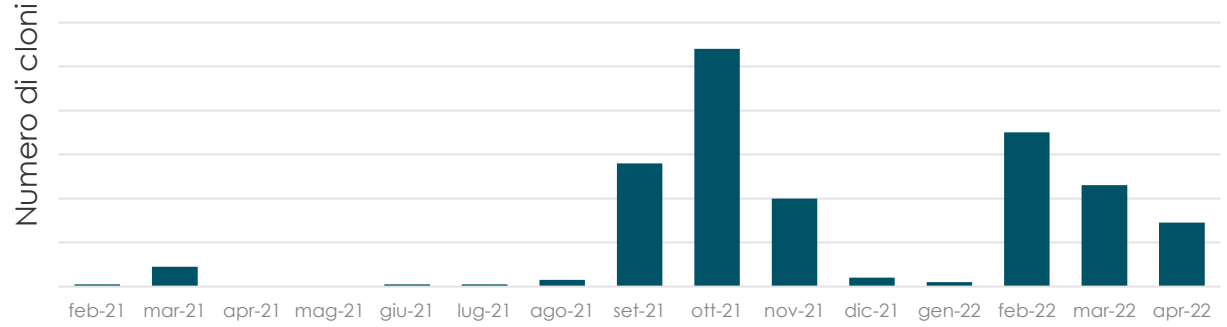
CONTESTO DI GRUPPO: FRODI INTERNET

Il Gruppo Cassa Centrale ha rilevato un significativo incremento dei fenomeni fraudolenti: in particolare tra i mesi di **settembre** 2021 e **febbraio** 2022 sono stati registrati volumi fino a **10 volte superiori alla media**. Il fenomeno è stato efficacemente contrastato nonostante si sia osservato un costante raffinamento delle tecniche e modalità di attacco.

Numero di frodi per mese e media degli ultimi 3 mesi*



Takedown siti di phishing



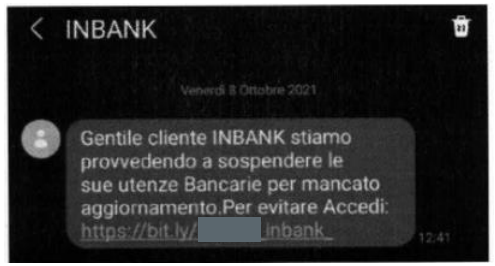
Principali caratteristiche del fenomeno

- Il **Social Engineering** rappresenta la principale tecnica di attacco ad oggi osservata: in tal senso le tecniche combinate di **Smishing**, **Phishing** e **Vishing** rappresentano oltre il 90% dei casi su retail.
- Si è osservato un mutamento del fenomeno per cui i frodatori **utilizzano** prevalentemente **IBAN Italiani** di **carte conto** (es. Banco di Bilbao BBVA), **IBAN esteri** di **carte conto** (es. Revolut) ed IBAN di **servizi** di **conversione Euro** in **Criptovaluta** utilizzati anche da clienti "reali".
- Con l'introduzione dei servizi **SCT INSTANT** si sono osservati nuovi pattern frodatori: la frode viene perpetrata **direttamente** al **telefono con il Cliente**, **limitando** le **capacità** di **detection dell'operazione**, in quanto autorizzata dai terminali legittimi.
- I threat actor risultano di **origine italiana**, ben organizzati e con a disposizione numerosi strumenti (oltre **200 device fisici**, decine di conti compromessi, script per la creazione automatica di siti cloni, etc...).
- **Fraud Rate** in % of total volume: Media Europea** 0,0012% Media Gruppo 35% migliorativa.

*numero di frodi avvenute sui canali di internet e mobile banking gestiti da Allitude S.p.a., società di Servizi del Gruppo Cassa Centrale
**report EBA payment fraud under PSDII

SCHEMI FRODATORI OSSERVATI: CONTATTO TELEFONICO

1 SMS (SMISHING)



Sul cellulare del Cliente arriva un **SMS a nome Inbank** che segnala la **sospensione temporanea dell'utenza dell'Internet Banking** e che invita ad aggiornare le informazioni legate all'utenza stessa, o pretesti similari.

Il 57,9% dei numeri di telefono dei clienti del gruppo risulta presente nel Data Breach di Facebook divulgato ad Aprile 2021. Spesso il mittente utilizza il caller-id della Banca.

2 SITI FASULLI (PHISHING)

Il link presente nell'SMS porta ad un sito clone di Inbank, in cui il Cliente inserisce le **credenziali personali**, il numero di **telefono**, il numero della **carta di credito**, la scadenza e il CVV2 della stessa.

Rilevati e chiuse decine di **siti clone**, rilevati fino a **19 nuovi siti cloni** in un giorno.
Identificate **4 diverse organizzazioni criminali.**

3 CONTATTO TELEFONICO (VISHING)

Il Cliente riceve una telefonata dal **finto numero di assistenza Inbank** da parte del truffatore che impersona un impiegato con lo scopo di convincere il cliente ad effettuare un Bonifico istantaneo a suo vantaggio.

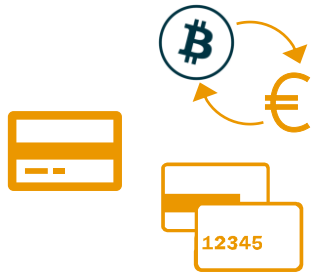
La tecnica di emulare i numeri telefonici dell'assistenza è resa possibile a causa di un non sempre «allineamento» **dei gestori telefonici** (es chiamate da numeri verdi).

4 BONIFICO ISTANTANEO

Il Cliente viene convinto dal finto operatore della Banca ad effettuare un **Bonifico Istantaneo** a vantaggio del frodatore. Dato che viene utilizzato il **dispositivo del Cliente** verranno aggirati i controlli tipici sulle anomalie.

Elemento fondamentale di difesa è rappresentato dal rilevamento del potenziale **mismatch** tra il profilo di rischio del Cliente e l'operazione effettuata.

5 DISPOSIZIONI FRAUDOLENTE

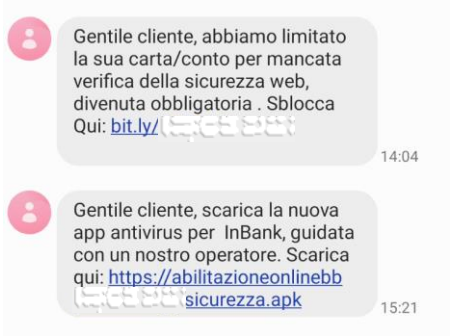


Le destinazioni verso le quali vengono indirizzati i bonifici sono normalmente lecite: **carte conto italiane, carte conto estere o servizi Euro-Bitcoin.**

Poiché le **destinazioni sono legittime** non possono essere escluse a priori, in quanto genererebbero un elevato numero di **falsi positivi**.

SCHEMI FRODATORI OSSERVATI: APPLICAZIONI MALEVOLE

1 SMS (SMISHING)

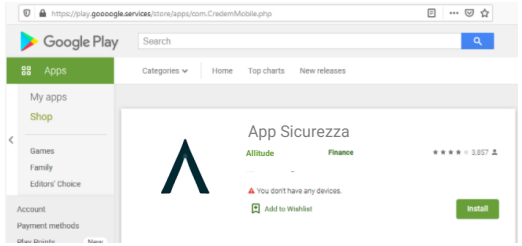


Sul cellulare del Cliente arriva un **SMS a nome Inbank** che segnala la **sospensione temporanea dell'utenza dell'Internet Banking** e che invita ad aggiornare le informazioni legate all'utenza stessa, o pretesti similari.

Condotte numerose campagne info/formative verso i Clienti. Tali campagne multicanale (web, in filiale, sugli ATM) sono state riconosciute a livello nazionale (Premio AIFIN).

2 STORE FASULLO (PHISHING)

Esemplificativo



Il link presente nel messaggio porta ad un **sito clone** di uno **store** digitale, dal quale il Cliente provvede a scaricare l'applicativo malevolo.

Rilevati e chiusi gli store malevoli tramite le soluzioni di take down adottate dal Gruppo.

3 APP MALEVOLA

Esemplificativo

Il Cliente viene invitato ad installare sul proprio Device un **app clone di Inbank** il cui scopo sarà esclusivamente quello di inviare al frodatore le OTP che altrimenti sarebbero ricevute dal Cliente a seguito dell'avvio di una transazione.

Le analisi del comportamento delle app malevole hanno evidenziato il redirect degli OTP tramite SMS verso i frodatori.

4 DISPOSIZIONI FRAUDOLENTE

Il frodatore è ora in grado di operare in autonomia per **effettuare le disposizioni fraudolente:** ricariche di carte prepagate, acquisto di beni immateriali come Bitcoin o altre criptovalute.

Le modalità per il trasferimento del denaro risultano molto dinamiche ed opportunistiche come evidenziano le analisi nel dettaglio del comportamento eseguite dai sistemi antifrode.

INTERVENTI REALIZZATI DAL GRUPPO

Per far fronte al forte incremento dei fenomeni fraudolenti registrati a partire dal secondo semestre 2021 il Gruppo ha indirizzato molteplici interventi tra cui:

Attività di comunicazione multicanale

Sono state condotte **attività** di **formazione**, con Workshop verticali con i **Referenti frode Banche** e verso i **Clienti**. Il Gruppo ha avviato inoltre una **campagna multicanale** info-formativa sulle principali minacce, aggiornando di conseguenza anche la **sezione sicurezza** della piattaforma **Inbank** per renderla più chiara e **accessibile**. Vi è stata inoltre piena adesione alle **iniziative** di **settore** (cfr. «I Navigati»).

Rafforzamento notifiche

Rafforzamento di tutti i **messaggi** di **notifica** e **allerta** a fronte di specifiche operazioni realizzate dall'utente (e.g. modifica delle anagrafiche, attivazione dell'app di mobile banking, disposizioni effettuate).

Threat Intelligence e Info-Sharing

Le attività di **Threat Intelligence** condotte dal Gruppo hanno permesso **l'aggiornamento** del **threat modeling** specifico (focus specifico su panorama italiano FS). Inoltre è stato possibile **favorire** ulteriormente lo **scambio** di **informazioni** con le altre **realtà** del panorama **FS** italiano e le **associazioni** di categoria, come il CERTFin.

Evoluzione processi di gestione delle frodi

Ottimizzazione dei **processi** interni ad esempio:

- **Blocco preventivo** dei **conti** da parte del team antifrode;
- **Processi snelli** per la **modifica** del **comportamento** applicativo e funzionale;
- **KIT** predefinito per risposta e la gestione di **reclami** e contenziosi ABF.

Ottimizzazione continua delle regole anti-frode

Aggiornamento costante delle logiche anti frode, raffinandole di volta in volta in modo dinamico a partire dagli schemi fraudolenti osservati anche dal mercato.
Elevato il supporto del team cyber, per la comprensione approfondita delle tecniche utilizzate e delle relative azioni di contenimento

Automazione Workload

Automazione di alcuni **workload** (e.g. take down siti phishing, standardizzazione raccolta evidenze anche ai fini probatori basati sulle minacce, monitoraggio preventivo siti cloni), tramite RPA e IPA e soluzioni custom dedicate, ha **velocizzato in modo significativo** il processo di contrasto e gestione delle frodi.

PROSSIMI INTERVENTI PREVISTI DAL GRUPPO

Supporto aree legali

Al fine di garantire una **migliore gestione** dei **reclami** e dei **contenziosi**, verranno **monitorate** in maniera continuativa le **sentenze ABF**, al fine di:

- garantire la produzione delle evidenze necessarie;
- **migliorare** la **traduzione** tra **evidenza tecnica** e **necessità probatoria** in termini legali.

Evoluzioni Tecnico/Funzionali

Al fine di mantenere aggiornati i presidi di prevenzione e contrasto alle frodi verranno **integrate** ulteriori **logiche** di **analisi comportamentale** del **cliente** e nuove soluzioni che garantiranno una **migliore confidenza** nella **correlazione cliente/device**.
Infine, il processo di evoluzione delle logiche di fall back vedrà una **progressiva dismissione** dello strumento **SMS**.

Efficientamento processi interni

La progressiva **centralizzazione** ed **automazione** della raccolta evidenze garantirà al Gruppo maggiore **efficacia**, così da permettere un sempre più rapido contrasto dei fenomeni.

Evoluzione Threat Intelligence driven

Il **nuovo processo** per l'aggiornamento del **threat model** garantirà una **maggiore focalizzazione** e un **allineamento** costante del modello.

Inoltre, verranno **raffinati** i **processi** per il **calcolo** del **rischio «cliente»** e i **relativi score** tramite l'introduzione di nuovi feed.

Il **Gruppo Cassa Centrale** considera inoltre **fondamentale** la **sensibilizzazione** e la **formazione** nei confronti dei **Clienti**, al fine di renderli **consapevoli** dei **rischi** connessi all'utilizzo dei metodi di pagamento digitali. Per questa ragione **continuerà ad investire** in **campagne** di sensibilizzazione multicanale, anche con il supporto di partner esterni.

Ω

Per approfondimenti o confronti: https://www.linkedin.com/in/**simonemaga**

Sede legale e Direzione Generale

Via Segantini, 5 - 38122 Trento

Tel. 0461.313111

gruppocassacentrale.it

GRUPPO CASSA CENTRALE
CREDITO COOPERATIVO ITALIANO