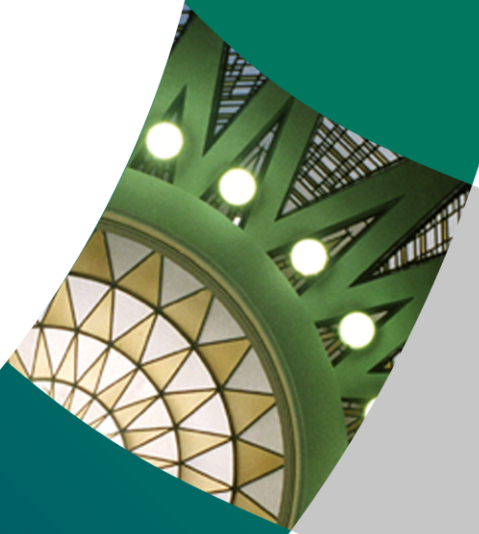
BANCO BPM

REATI INFORMATICI E RICICLAGGIO



Convegno annuale AICOM Netech Arkes 2023

3 OTTOBRE 2023

Funzione Antiriciclaggio – Segnalazioni operazioni sospette BANCO BPM

Legenda

Slides 3 - 12

CONTESTO ATTUALE RELATIVO ALLE FRODI INFORMATICHE

Slides 13 - 20

FRODE INFORMATICA VS RICICLAGGIO

CONTESTO ATTUALE RELATIVO ALLE FRODI INFORMATICHE

Premessa

Negli ultimi anni si è registrato un considerevole aumento del rischio di essere vittima di reati informatici.

*La **Comunicazione UIF del 16.4.2020** richiama l'importanza del monitoraggio delle attività a distanza, in particolare di quella on line.*

«Assumono rilievo gli strumenti di pagamento elettronici, il cui impiego – senz'altro positivo per assicurare la tracciabilità dei flussi finanziari – è destinato ad aumentare ulteriormente nei prossimi mesi, in conseguenza delle misure di distanziamento sociale, che hanno determinato il passaggio di molte attività di compravendita dal canale tradizionale a quello telematico. Nell'attuale situazione emergenziale aumenta il rischio che tali strumenti possano essere impiegati per le truffe on line, mediante il sistema della compravendita di beni inesistenti o contraffatti, ovvero a prezzi sproporzionati».

***Il maggior utilizzo di servizi on line accresce, inoltre, l'esposizione al rischio di reati informatici in danno di singoli utenti ovvero di imprese o enti**. Si fa riferimento ai fenomeni di phishing, di cd. Business email compromise o CEO frauds ovvero agli attacchi ransomware, anche collegati a richieste di riscatto in valuta virtuale.*

Premessa

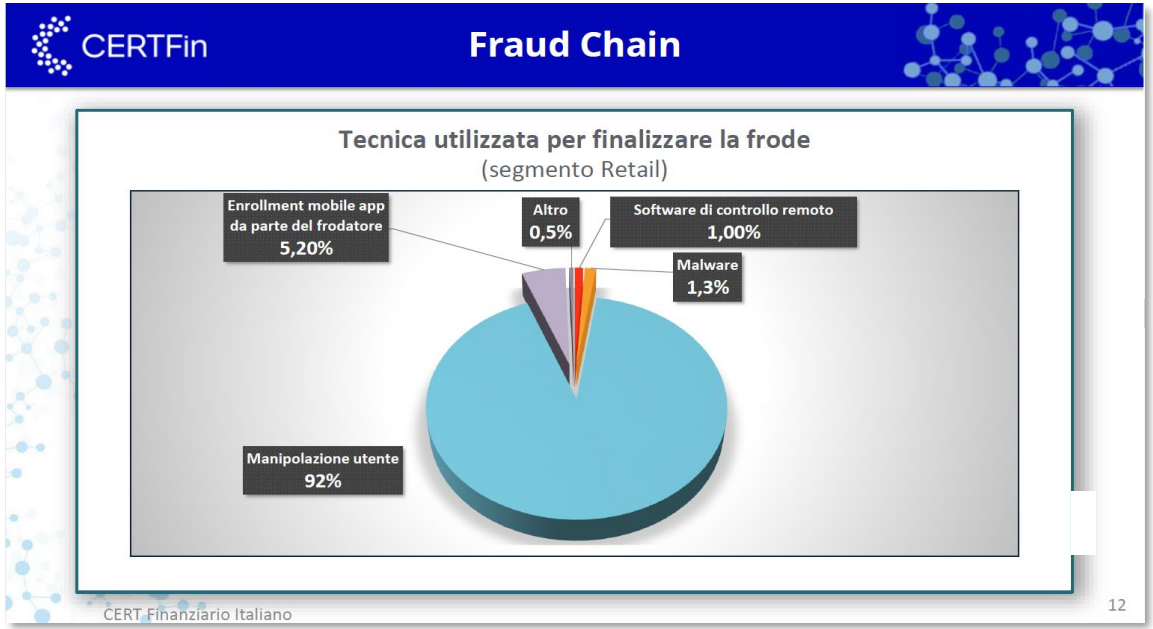
*Nel **RAPPORTO ANNUALE UIF 2022** si parla di frode informatica laddove:*

- *si sottolinea che sul fronte delle **valute virtuali** i sospetti più ricorrenti attengono all'origine dei fondi utilizzati per l'acquisto degli asset, spesso correlati tra gli altri a frodi informatiche o episodi di ransomware. Sono state rilevate ipotesi di truffe nel trading online e di investimenti eseguiti dalle vittime dei raggiri presso piattaforme estere;*
- *si ricorda che il comparto dei **giochi** e delle **scommesse** si presta a favorire fenomeni di riciclaggio. Nel corso del 2022, diverse segnalazioni inoltrate da altrettanti concessionari di gioco online hanno portato all'attenzione dell'Unità presumibili meccanismi di **chip dumping** intercettati dalle piattaforme di gioco **nell'ambito delle procedure interne antifrode**. La fattispecie prevede la canalizzazione, resa apparentemente legittima dal ricorso al chip dumping, di fondi aventi origine illecita verso conti di gioco, successivamente incassati in contanti tramite voucher presso punti vendita ricorrenti e concentrati nella medesima area geografica. È stato ipotizzato che le somme illecite riciclate provenissero da frodi informatiche, clonazioni di carte di pagamento e truffe di vario genere.*

La UIF sta proseguendo con i progetti di portata trasversale sulle frodi informatiche (cyber-enabled fraud) a conferma dell'importanza che il fenomeno riveste.

Nuove modalità di attacco informatico

Da recenti analisi svolte dal CERTFin emerge come la tecnica usata per finalizzare la frode sia oramai prevalentemente di **natura manipolativa**



Nuove modalità di attacco informatico

Oggi assistiamo a uno spostamento dell'**oggetto dell'attacco rispetto al passato**.

IERI	OGGI
	
Tecnologia	**Persone**
	
Malware	**Manipolazione**

Gli attaccanti, senza abbandonare i vecchi schemi, affiancano all'approccio precedente un nuovo approccio, spostando il focus dell'attacco dalle tecnologie di sicurezza alle persone, agli utenti.

Abbandonano il malware ed evolvono il vecchio phishing in 'manipolazione'.

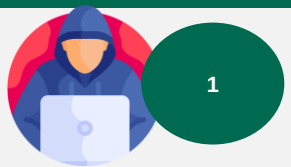
Nuove modalità di attacco informatico

Il **social engineering** consiste in un insieme di **tecniche** utilizzate dai **criminali informatici** per acquisire informazioni ed attaccare una singola persona o intere organizzazioni. Facendo leva sull'applicazione di **conoscenze psicologiche** e di **manipolazione** finalizzate a produrre determinati comportamenti, le metodologie di attacco hanno più a che fare con l'**interazione diretta tra persone** piuttosto che con i *tool* tipici dei «normali» attacchi hacker. L'obiettivo è **guadagnare** la **fiducia** delle vittime, così che abbassino la guardia e siano incoraggiate a compiere azioni pregiudizievoli, come divulgare informazioni personali, fare clic sui link oppure aprire allegati **dannosi**.

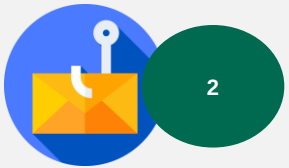
Panorama dei principali attacchi

Utilizzando un sapiente **mix tra sms, siti fake e telefonate fraudolente**, i criminali frodano i clienti attraverso il loro home banking

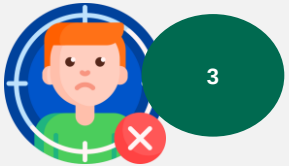
SCENARIO DI ATTACCO



L'attaccante invia **sms a pioggia** verso numeri acquistati nel **black market**. Gli sms talvolta danno l'impressione di essere inviati dalla banca. Contengono un messaggio allarmistico ed un **link.** Il cliente, allarmato dal contenuto del messaggio, viene indotto a cliccare sul link.



Atterra su una **pagina fake** su cui digita i propri dati di **login**. Il malfattore, identificata l'identità ed altri dati corrispondenti ad un determinato numero telefonico, contatta la persona.
Si finge un operatore della banca (es: antifrode) e ne **carpisce la fiducia**, dimostrando di conoscere i dati che il cliente stesso ha fornito direttamente o tramite l'accesso al proprio home banking.

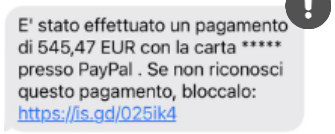


L'attaccante **induce il cliente** ad effettuare una serie di attività volte ad attuare la frode.
Di seguito esempi reali delle conclusioni più frequenti dell'attacco.

Panorama dei principali attacchi

Truffa PayPal

L'attaccante ha raccolto le **credenziali PayPal** dalla vittime tramite il **link** precedentemente inviato, che ora si adopera di utilizzare per effettuare **pagamenti** ad esempio verso i siti di gioco o di acquisto di criptovalute.

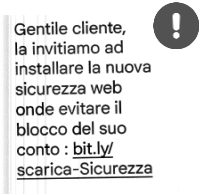


Truffa dello storno

L'attaccante induce il cliente ad effettuare un' operazione di **storno** di un presunto pagamento fraudolento, invitandolo ad inserire una causale specifica che contiene sempre la parola 'storno'; lo storno in realtà è un **bonifico**.
Spesso più di uno e possibilmente **di tipo instant**. L'operazione è eseguita in toto dal cliente.

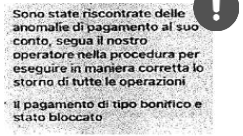
Frode remote app

L'attaccante ottiene dalla vittima le credenziali e le conferme per installare un'app di **controllo remoto** per operare poi le disposizioni in autonomia, minimizzando le richieste di quantità di sicurezza al cliente.



Frode dello storno

Il frodatore accede via web o app all'**Home Banking** del cliente utilizzando le credenziali carpite ed inserisce le disposizioni a proprio beneficio.
Invia un nuovo SMS per avvisare il cliente che dovrà fornire un **OTP** alla persona al telefono per completare lo storno. Avuto l'OTP dalla vittima, invia un SMS ulteriore segnalando la corretta **esecuzione** dello storno.
L'operazione è eseguita dal truffatore utilizzando le credenziali **cedute** dal cliente.



BANCO BPM

* Frode: l'operazione è svolta dal frodatore carpite le credenziali
**Truffa: l'operazione è svolta direttamente dal cliente manipolato dal frodatore

Panorama dei principali attacchi

INVOICE FRAUD

Un'azienda viene contattata da un finto rappresentante di un **fornitore**.

Lo strumento più usato dal frodatore è la mail. La stessa può essere la casella vera hackerata di un fornitore, piuttosto che una mail diversa creata con un indirizzo simile all'originale o comunque ingannevole

Il truffatore richiede che vengano modificate le **coordinate bancarie** per il pagamento di fatture (nella fattispecie l'IBAN del beneficiario).

CEO FRAUD

Un dipendente di alto livello nella gerarchia aziendale viene contattato via mail da qualcuno che finge di essere una figura apicale (es:l'amministratore delegato).

L'indirizzo mittente sembrerà appartenere effettivamente all'apicale scrivente

Il truffatore richiede che venga effettuato un pagamento di importo molto rilevante verso un beneficiario non conosciuto. Si tratta di un importo destinato a perfezionare una operazione molto riservata ed estremamente urgente di cui la persona ingaggiate non deve fare menzione con alcuno

BANCO BPM

Panorama dei principali attacchi

CERTFin

Attacchi Basati sulla Creatività

#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.

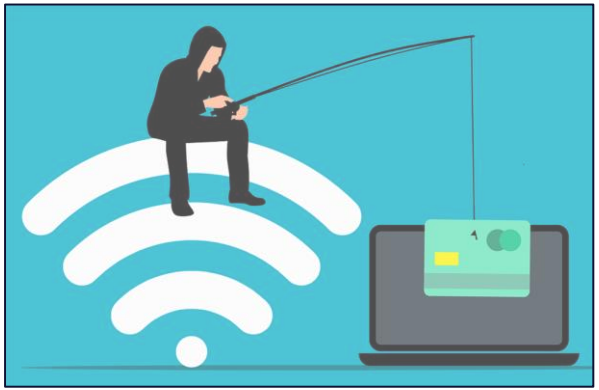
BANCO BPM

FRODE INFORMATICA

VS

RICICLAGGIO

Frode informatica e Riciclaggio



PRODOTTO/PROFITTO

FRODE INFORMATICA

Art. 640 ter c.p.

*Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, **procura a sé o ad altri un ingiusto profitto con altrui danno**, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032. […]*

RICICLAGGIO

Art. 648 bis c.p.

*Fuori dei casi di concorso nel reato, chiunque sostituisce o trasferisce **denaro, beni o altre utilità provenienti da delitto** [non colposo]; ovvero compie in relazione ad essi altre operazioni, in modo da ostacolare l'identificazione della loro provenienza delittuosa, è punito con la reclusione da quattro a dodici anni e con la multa da euro 5.000 a euro 25.000. […]*

Frode informatica vs Riciclaggio

Sentenza n. 16023 del 2020 della II Sezione della Cassazione Penale

Nel caso di specie, l'imputato è stato condannato in I e II grado per il **delitto di frode informatica ex art. 640 ter c.p.,** nella forma tentata, per **aver messo a disposizione di un terzo ignoto il proprio conto corrente** per ricevere un bonifico mediante un'operazione di "phishing" volta ad acquisire le credenziali di accesso al sistema telematico di gestione del conto corrente della vittima del reato.

La Corte ha sottolineato che il delitto in questione **si consuma nel momento in cui il soggetto agente consegue l'ingiusto profitto con correlativo danno patrimoniale**, sicché la condotta del ricorrente, che ha messo a disposizione di terzi rimasti ignoti il proprio conto corrente per ricevere direttamente la somma di denaro sottratta utilizzando le credenziali della persona offesa, si è inserita nella **fase di esecuzione del reato di frode informatica** e non costituisce un evento successivo.

Frode informatica vs Riciclaggio

Sentenza n. 29346 del 6 luglio 2023 della II Sezione della Cassazione Penale

La pronuncia origina dal ricorso presentato per 'erronea qualificazione del fatto' dai due imputati che si erano visti condannati ex art. 648 bis c.p. in secondo grado.

Integra il delitto di riciclaggio la condotta di chi, **senza aver concorso nel delitto presupposto**, **metta a disposizione il proprio conto corrente per ostacolare l'identificazione della provenienza delittuosa del denaro, da altri precedentemente ricavato quale profitto conseguito del reato di frode informatica, consentendone il trasferimento tramite bonifici bancari**. La Corte ha analizzato il caso specifico, sottolineando **che l'autore della frode informatica aveva già ottenuto il profitto** attraverso somme di denaro ricevute in modo fraudolento. L'operazione successiva, ovvero l'immissione di tali fondi su conti correnti di terzi, è stata considerata una condotta ulteriore e successiva, finalizzata a "ripulire" il denaro, rientrando così pienamente nell'ambito del reato di riciclaggio.

Money Mules

1. Fondi di provenienza illecita confluiscono sul c/c
2. Il soggetto trasferisce le provviste ad altri c/c intestati a terze persone
3. I fondi sono trasferiti nuovamente dal cd. *Money Mule* come da istruzioni ricevute
4. La pulizia avviene tipicamente attraverso prelievi in denaro **contante**, oppure con l'acquisto di **valute virtuali**

Processo di gestione dei casi di money mules

1 INDIVIDUAZIONE DEL MONEY MULE

1. Detection sistemi di monitoraggio banca
2. Segnalazione da soggetti esterni
   a. Recall da altra banca
   b. Comunicazioni da parte delle autorità
   c. Reclamo del cliente truffato
3. Individuazione da parte della filiale di radicamento del rapporto del sospetto money mule

2 Blocco del rapporto del sospetto money mule, compreso se possibile il bonifico fraudolento in uscita

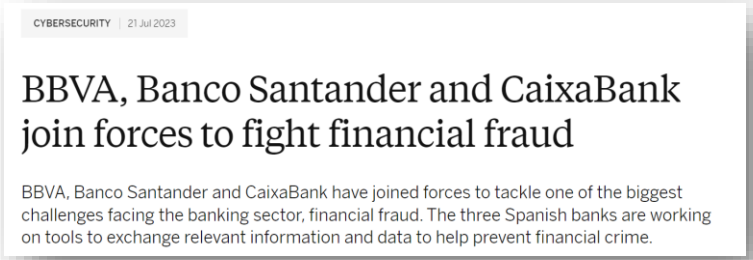
3 Segnalazione di operazione sospetta a UIF

Aspetti problematici di gestione del rapporto di sospetto money mule

- Le somme pervenute al soggetto ritenuto money mule, una volta accreditate sul suo conto, non possono essere restituite al mittente se non previa autorizzazione del soggetto ricevente.
- In caso di rifiuto alla restituzione la procedura da seguire prevede la richiesta di recall della somma trasferita, la denuncia del nominativo oggetto di truffa/frode e il decreto di sequestro

In attesa che la procedura di sequestro si concluda la filiale può trovarsi in difficoltà nel gestire il cliente, che anche ricorrendo a minacce sollecita continuamente le disposizioni di bonifico da lui impartite

Prospettive future … Data Sharing



CYBERSECURITY | 21 Jul 2023

BBVA, Banco Santander and CaixaBank join forces to fight financial fraud

BBVA, Banco Santander and CaixaBank have joined forces to tackle one of the biggest challenges facing the banking sector, financial fraud. The three Spanish banks are working on tools to exchange relevant information and data to help prevent financial crime.

È stata creata e presentata ai regolatori **FrauDfense**: una società che unirà le iniziative antifrode delle 3 distinte Banche.

Nella prima fase, l'alleanza affronterà la creazione di un tool di condivisione delle informazioni inerenti il 'modus operandi' fraudolento e le misure di contrasto attuate positivamente.

Il Progetto è volto a contrastare le pratiche frudolente che possono essere davvero sofisticate e diversificate tra loro come le admission frauds o le digital or card payment frauds.

È previsto che la collaborazione venga aperta alla partecipazione di altre società e istituzioni anche non finanziarie interessate nello sharing di informazioni antifrode, con l'obiettivo di fornire la massima protezione ai clienti.