TRUFFE SU CONTI CORRENTI MEDIANTE SMS E TELEFONATE DI PHISHING: LA POLIZIA DI STATO ESEGUE 18 PERQUISIZIONI E SEQUESTRI DI MATERIALE INFORMATICO NELLE PROVINCE DI CASERTA, NAPOLI, SALERNO E LIVORNO

Pubblicato il10 Febbraio 2024 di redazione

Categoria: CRONACA E ATTUALITA'

Dopo circa un anno di indagini, scaturite dalla querela di un ottantenne milanese, la Polizia di Stato ha eseguito diciotto perquisizioni tra Toscana e Campania a carico di altrettanti soggetti indagati, in concorso tra loro, per truffa aggravata.

L'attività investigativa, condotta dal Centro Operativo per la Sicurezza Cibernetica Lombardia sotto la direzione della Procura della Repubblica di Milano, ha permesso di ricostruire l'insidioso meccanismo truffaldino che ha indotto la vittima a trasferire l'ingente somma complessiva di 241.000 euro su conti correnti aperti e gestiti dagli indagati.

In particolare, il cittadino milanese ha ricevuto un SMS, apparentemente riconducibile al servizio clienti del proprio istituto di credito, che lo avvisava di un attacco informatico in corso sul suo dispositivo mobile e sui conti correnti ad esso collegati; cliccando su un *link* riportato nel medesimo SMS, avrebbe avviato la fantomatica procedura di blocco per la messa in sicurezza del capitale.

Subito dopo aver seguito le indicazioni dei criminali, il malcapitato ha ricevuto la telefonata di un sedicente operatore del servizio antifrode della propria banca, il quale, dopo avergli confermato che il suo conto corrente era sotto attacco, lo ha indotto a spostare tutti i propri risparmi verso conti "sicuri" al fine di interrompere i "prelievi non autorizzati". Tale trasferimento è avvenuto attraverso diversi bonifici eseguiti dalla vittima verso IBAN riconducibili a conti correnti italiani.

Uno dei principali espedienti che hanno tratto in inganno il truffato è consistito nel cosiddetto *spoofing* del numero di telefono da cui ha ricevuto l'SMS e la successiva telefonata. Grazie a tale tecnica, infatti, è possibile inviare SMS ed effettuare telefonate di tipo VoIP (*Voice over Internet Protocol*), mediante personal computer e altri dispositivi informatici, potendo scegliere liberamente il numero di telefono che apparirà sul display dello smartphone ricevente.

Gli accertamenti svolti dal C.O.S.C. Lombardia hanno consentito agli investigatori di risalire a 18 soggetti - 11 dei quali con precedenti penali, anche specifici - di cui 7 residenti nell'agro aversano, 8 a Napoli, 2 a Battipaglia e uno a Livorno. Le perquisizioni informatiche svolte con il coordinamento del Servizio Polizia Postale e delle Comunicazioni sui cellulari e sugli altri dispositivi informatici sequestrati agli indagati hanno già fornito agli inquirenti milanesi importanti riscontri sulla vasta portata dell'attività delinquenziale oggetto di indagine, nonché interessanti spunti per la prosecuzione e l'ampliamento delle investigazioni, che puntano alla ricostruzione dell'intera filiera delittuosa e alla disarticolazione dell'organizzazione criminale che, verosimilmente, progetta le frodi e ne ricicla i proventi illeciti.

Come difendersi: i consigli della Polizia di Stato

Negli ultimi tempi si sta registrando un notevole incremento di questo genere di frodi, perpetrate secondo uno schema sostanzialmente sovrapponibile a quello appena descritto. È stata anche segnalata una variante che prevede la ricezione di una telefonata da parte di soggetti che si fingono operatori della Polizia Postale. Anche in questo caso, grazie alla tecnica dello *spoofing*, la telefonata sembra giungere dal vero numero di telefono dell'ufficio della Polizia Postale competente per territorio, così come visibile sui canali web e social ufficiali della Polizia di Stato.

Per evitare di cadere in simili raggiri, la Polizia di Stato consiglia di diffidare totalmente di chi, spacciandosi per un assistente del servizio clienti della propria banca o per un operatore della Polizia Postale, richiede l'esecuzione di bonifici o pagamenti in qualsiasi forma.

Come spesso ricordato dagli stessi istituti di credito, la Polizia di Stato ribadisce che le banche non chiedono mai ai propri clienti - né per telefono né per email - di eseguire movimentazioni di somme di denaro o di comunicare le proprie credenziali di accesso ai servizi di *home banking*.