Polizia di Stato

Rubavano codici di carte e svuotavano i conti, 5 arresti a Padova

Carpivano i dati relativi a carte di credito e bancomat e poi li utilizzavano in vari modi per sottrarre soldi dai conti correnti o acquistare costosi beni e servizi.

Al termine dell'operazione "Jacking" gli investigatori della Squadra mobile di Padova hanno individuato i responsabili delle numerose frodi messe in atto in tutta Italia da un gruppo di criminali, destinatari delle misure cautelari emesse dal giudice per le indagini preliminari.

Sono due le persone finite in carcere e tre quelle agli arresti domiciliari, mentre ad una sesta persona è stato notificato l'obbligo di dimora; altre due sono indagate in stato di libertà.

Le accuse nei loro confronti sono di associazione per delinquere finalizzata alla commissione di truffe aggravate mediante indebito utilizzo e falsificazione di strumenti di pagamento online. Per alcuni degli indagati anche l'accusa di autoriciclaggio e traffico di sostanze stupefacenti.

L'attività investigativa ha preso il via nel gennaio 2020, dopo che i poliziotti della Mobile padovana si erano recati in un ristorante per acquisire informazioni in merito ad alcuni tentativi di utilizzo di carte bancomat clonate.

Grazie alla descrizione fornita dal titolare del locale, al quale il responsabile si era presentato con il nome di Jack (da qui il nome dell'operazione), all'analisi delle celle telefoniche e delle immagini delle telecamere di sicurezza interne ed esterne, gli investigatori sono risaliti alle utenze e all'auto utilizzata dall'uomo e dai suoi due complici.

L'indagine ha anche evidenziato diversi tentativi, da parte degli indagati, di effettuare operazioni con carte poste pay evolution a loro intestate, bloccate a causa di transazioni sospette o per bonifici anomali.

Come avveniva la truffa

Tutto iniziava con il classico phishing: gli indagati inviavano un messaggio alla vittima con l'avviso di problemi di sicurezza sul conto corrente, risolvibili cliccando su un link che riproduceva fedelmente quello della sua banca online, ma che in realtà, al momento di inserire i dati per effettuare l'accesso, trasmetteva le credenziali ai truffatori.

A quel punto i cybercriminali attivavano l'app dell'home banking. Per risolvere il problema dell'Otp, il codice di verifica che la banca invia sul telefono del cliente quando compie delle operazioni, i truffatori, utilizzando documenti falsi, denunciavano lo smarrimento o il furto della sim del titolare del conto; poi con la denuncia si recavano in un negozio del gestore di telefonia ed ottenevano una nuova sim con lo stesso numero (tecnica del sim-swap). E il gioco era fatto.

In questo modo quando utilizzavano l'app dell'home banking potevano gestire anche il codice di sicurezza Otp ed effettuare pagamenti o bonifici.

Utilizzando l'app i truffatori potevano anche effettuare prelievi cardless, effettuati dalle casse veloci automatiche senza usare la carta fisica, ma utilizzando l'app sullo smartphone che, inquadrando il Qr

code, permette di ottenere il denaro.

Anche grazie a questi prelievi, immortalati dalle telecamere di sicurezza delle banche, gli investigatori sono riusciti ad individuare gli indagati.

L'analisi di alcune chat ha, inoltre, consentito di accertare nei confronti di alcuni elementi del gruppo, l’attività relativa alla cessione di sostanze stupefacenti.

Sergio Foffo

03/05/2022