Polizia di Stato

Napoli: operazione "Numero Verde"

In data odierna la Polizia di Stato, a conclusione di una complessa e articolata attività investigativa finalizzata al contrasto dei crimini finanziari in danno di ignari correntisti bancari, coordinata dalla Procura della Repubblica presso il Tribunale di Torre Annunziata (NA), in esecuzione di un'ordinanza di custodia cautelare in carcere emessa dal Giudice per le indagini preliminari del Tribunale di Torre Annunziata, ha proceduto all'arresto di sette persone, tutte residenti a Torre del Greco, gravemente indiziate dei reati di frode informatica e di associazione per delinquere finalizzata alla commissione di tali frodi. Contestualmente si sta procedendo all'esecuzione di un decreto di sequestro preventivo emesso dal medesimo GIP su richiesta di questa Procura della Repubblica per un importo di euro 94.700, pari al totale delle somme di denaro indebitamente introitate dagli autori dei reati per cui si procede.Gli arrestati, appartenenti ad un sodalizio criminale sedente sul territorio di Torre del Greco (NA), ma operante su tutto il territorio nazionale, erano dediti al phishing bancario di ultima generazione i cui proventi venivano monetizzati presso sportelli ATM della città metropolitana di Napoli.L'indagine trae spunto da un normale controllo operato su strada nei confronti di un indagato trovato in possesso di un gioiello di valore, acquistato online con i proventi di una frode.Quella che apparentemente poteva sembrare una semplice truffa, fin dai primi accertamenti effettuati, ha mostrato i complessi risvolti e le problematiche tecnico investigative ad essa correlate.Il coordinamento investigativo tra la Polizia Postale di Napoli, il Commissariato PS di Torre del Greco e la Aliquota della PS della Sezione di Polizia Giudiziaria presso la Procura della Repubblica, ha permesso di individuare gli odierni arrestati quali autori dei reati informatici.L'attività investigativa del Servizio di Polizia Postale e delle Comunicazioni ha consentito di ricostruire il modus operandi degli indagati all'esito anche di approfonditi accertamenti tecnici, delineando uno scenario estremamente esteso del fenomeno, consentendo, tra l'altro, di individuare diverse vittime sull'intero territorio nazionale.Le indagini hanno consentito di disvelare una struttura criminale molto complessa sia sotto il profilo organizzativo che tecnologico.I truffatori, attraverso una stabile organizzazione, riuscivano a procurarsi liste di numeri telefonici di ignari destinatari della frode online — phishing, per poi inviare, agli stessi, sms (smishing il fenomeno tecnico) ai quali faceva seguito una telefonata effettuata da falsi operatori bancari, con chiamate provenienti apparentemente dal Numero Verde / Servizi Bancari.Le attività tecniche hanno permesso di riprendere ed intercettare gli indagati mentre effettuavano le varie operazioni fraudolente, anche mentre erano ospiti di un albergo nel centro della capitale e dove si accingevano a monetizzare i proventi.Queste frodi perpetrate attraverso lo "Smishing-Vishing" consistono nel ricevere comunicazioni che sembrano provenire dalla propria banca, che invitano il cittadino ad accedere al proprio conto on-line mediante un web-link.Lo "smishing" in particolare si concretizza attraverso messaggi sms malevoli che, per una mera affinità semantica, si collocano in coda ad altri messaggi autentici ricevuti dalla banca; tali sms contengono link di rinvio a pagine di phishing dove l'utente, ritenendo di operare sulla pagina veritiera, è indotto ad inserire le proprie credenziali bancarie consegnando così i propri dati ai cyber-criminali.La tecnica del vishing invece consiste nel contattare la potenziale vittima tramite una chiamata telefonica nella quale un finto operatore di banca, attraverso raggiri ed argomentazioni capziose, la persuade a fornire i codici dispositivi del proprio rapporto finanziario; è frequente, nel corso di tali chiamate, che il truffatore prospetti alla vittima la necessità di ottenere il suo codice al fine di bloccare alcuni tentativi illeciti di prelievo operati da terzi.Sfruttando questo momento di incertezza i criminali ottengono le credenziali di accesso ai conti correnti che subito dopo provvedono a svuotare.La frode è particolarmente subdola poiché le chiamate sembrano arrivare dal numero della propria banca, da qui l'appellativo di "Alias" e, parlando con un operatore, il correntista è convinto di trovarsi in un ambiente favorevole, nella sua cosiddetta "comfort zone" ed abbassa il proprio livello di allerta.La frode si concludeva poi attraverso i complici che procedevano agli incassi fraudolenti con ingenti prelievi di somme di denaro presso ATM abilitati all'incasso con modalità cardless.L'attività di indagine ha consentito di accertare il compimento di 92 frodi e di ricostruire l'importo del danno complessivo cagionato alle vittime identificate, pari ad euro 94.700,00. Contestualmente alla emissione della misura cautelare, il GIP si è dichiarato incompetente, avendo ritenuto la competenza delle Procure Distrettuali di Napoli e Roma, alle quali saranno tempestivamente trasmessi gli atti, avendo ravvisato la configurabilità, in luogo del reato di cui all'art. 493 ter c.p. originariamente contestato, di quello di cui all'art. 640 ter c.p.

25/05/2021