Polizia di Stato

Catania: frode informatica

Le indagini della Polizia Postale di Catania, coordinate dalla Procura Distrettuale della Repubblica, hanno messo in luce l'esistenza di un gruppo organizzato e stabile, operante nella zona jonica comprendente i comuni di Giarre, Riposto, Fiumefreddo di Sicilia e Comuni limitrofi, connotato da notevole capacità criminale e peculiari conoscenze tecniche informatiche, dedito con professionalità e spregiudicatezza alla pianificazione continua di frodi informatiche e telematiche e truffe on-line su noti portali.L'indagine è stata avviata dalla Polizia Postale a fine 2015 a seguito di una frode informatica ai danni di una banca on-line ai cui clienti, residenti in varie parti d'Italia, erano stati sottratti 300.000,00 euro.L'associazione era dedita soprattutto alla realizzazione di frodi informatiche del tipo "SIM SWAP".La SIM SWAP è una avanzata tipologia di frode informatica articolata in vari passaggi. Una volta individuata la vittima si procede alla acquisizione dei suo dati e delle credenziali di home banking tramite tecniche di hacking ovvero di ingegneria sociale e, successivamente, utilizzando documenti falsificati ad hoc, si sostituisce la sim card della vittima e, attraverso lo stesso numero telefonico, si ottengono dalla banca le credenziali per operare sul conto corrente on-line.Nel caso specifico, carpiti i dati anagrafici e il numero di telefono della vittima, nonchè i dati dei conti correnti e le relative credenziali di accesso, gli indagati, utilizzando un falso documento di identità intestato alla vittima, si recavano presso un dealer al fine di chiedere la sostituzione della SIM in uso alla persona offesa. La scheda SIM del titolare veniva allora disabilitata in quanto sostituita da quella attivata fraudolentemente. La vittima rilevava il mancato funzionamento della sua SIM ma, generalmente, non associava immediatamente l'evento ad una frode in corso.Sostituita la SIM, gli autori del reato penetravano nel sistema informatico dell'istituto di credito presso cui la vittima aveva acceso il conto corrente, riuscendo il più delle volte a reimpostare le credenziali di accesso attraverso una telefonata all'assistenza clienti, presentandosi come il titolare del conto e rispondendo alle varie domande di sicurezza. Una volta effettuato l'accesso, gli indagati erano abilitati ad operare sul conto corrente on-line della vittima, disponendo bonifici e/o ricariche di carte prepagate in favore di altri conti correnti e/o carte prepagate nella loro disponibilità, in quanto appositamente accesi da complici e prestanome, così ostacolando l'identificazione della provenienza delittuosa delle somme e l'individuazione degli effettivi beneficiari dei proventi del reato attraverso il tracciamento dei flussi finanziari generati dall'operazione dispositiva indebita.La serrata successione temporale delle varie sequenze attraverso le quali si snoda la frode informatica in esame non consentiva alla vittima di attivare tempestivamente i dispositivi di sicurezza; la vittima acquisiva dunque consapevolezza del prelievo indebito solo al momento della lettura dell'estratto del conto corrente.Alcuni componenti del sodalizio criminale sono stati molto attivi anche nella commissione delle più comuni truffe on-line, ovvero quelle perpetrate inserendo falsi annunci di vendita sui portali specializzati e, in particolare, sul sito www.subito.it Al pari delle frodi "swap sim", anche in questa fattispecie è stata necessaria la partecipazione di soggetti che si intestassero carte prepagate sulle quali far pervenire i proventi dei reati nonché schede telefoniche utili a mantenere i contatti con le vittime.Il meccanismo, sebbene più semplice rispetto alle frodi informatiche, ha richiesto buone conoscenze tecniche nonché padronanza delle dinamiche che regolano le compravendite on-line.Tipicamente, tale tipologia di truffa si fonda sull'inserimento di falsi annunci di vendita di beni (in particolare, smartphone, pezzi di ricambio per auto, apparecchiature elettroniche) sui portali internet dedicati. Alla descrizione del bene veniva associata un'utenza di contatto alla quale fare riferimento per la trattativa. L'acquirente, dopo aver visionato la descrizione del bene, contattava l'asserito venditore, con il quale concordava le modalità di pagamento indicate di volta in volta sotto forma di IBAN sui quali far pervenire i bonifici. Ottenuto il pagamento, gli indagati si rendevano irreperibili, frustrando i tentativi della vittima di conseguire il bene, nonostante l'avvenuto pagamento del corrispettivo.Al fine di accreditarsi con le vittime e di rassicurarle in ordine alla disponibilità effettiva del bene offerto in vendita e alla serietà dell'annuncio, gli indagati ricorrevano ad insidiosi escamotage, in particolare presentandosi quali dipendenti di una società di recupero crediti realmente esistente, riferendo che i beni erano provento di aste fallimentari, fornendo un IBAN sul quale far pervenire il pagamento e indicando numeri telefonici di rete fissa che, in realtà, altro non erano che utenze cellulari di cui gli indagati disponevano.Oltre 600.000,00 gli euro provento degli illeciti guadagni, realizzati dal sodalizio criminale durante il periodo delle indagini.Nel corso delle attività d'indagine gli operatori della Polizia Postale hanno bloccato numerose frodi, alcune delle quali per importi pari a decine di migliaia di euro.L'operazione odierna si è avvalsa dell'ausilio degli specialisti nel contrasto al fenomeno del Financial Cyber Crime dei Compartimenti Polizia Postale di Messina, Palermo e Reggio Calabria. Nel corso delle perquisizioni è stato sequestrato materiale informatico che sarà sottoposto ad analisi da parte del personale specializzato della Polizia Postale.