

Operazione “Dominio”, arrestato in Sicilia un hacker 24enne

Nel corso di una operazione finora inedita nel nostro Paese, è stato arrestato questa notte in provincia di Caltanissetta dai poliziotti del Cnaipic (Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche) del Servizio polizia postale e dei Centri operativi per la sicurezza cibernetica (Cosc) di Napoli e Catania, diretti dalla Procura di Napoli e coordinati dalla Procura nazionale antimafia, un hacker di 24 anni, che si è reso responsabile di numerosi attacchi alle infrastrutture dei sistemi informatici della giustizia e di alcuni domini critici di enti nazionali strategici.

L'hacker 24enne era stato in precedenza collegato ad alcuni procedimenti penali per la gestione di un black market illegale insieme ad altre persone, sottoposti anche loro alle indagini e alle perquisizioni di stanotte effettuate dagli agenti della Postale. Proprio per verificare la sua posizione in merito aveva iniziato la sua attività di intrusione nei sistemi della Giustizia.

Gli esperti informatici della Polizia postale hanno ricostruito i passaggi del giovane che, per raggiungere l'anonimato, era riuscito a nascondere la sua attività criminale dietro a ben quattro livelli di sicurezza e cifratura passando per server esteri, Vpn (Virtual private network) anonime, macchine virtuali e meccanismi di cifratura.

Forte di questa sua presunta inafferrabilità, era riuscito a penetrare sistemi informatici critici utilizzando varie tecniche, tra cui la violazione di reti per lo smart working, campagne di phishing e la violazione di credenziali di amministratore; una volta entrato poi, si era appropriato di migliaia di informazioni riservate, modificando le difese del sistema colpito per cancellare accuratamente le proprie tracce.

Il bottino dell'hacker, dopo aver compromesso i sistemi informatici fino a tentare di prenderne il totale controllo, è stato accertato consistere in migliaia di documenti riservati, atti giudiziari e dati personali trafugati, che si aggiungono ai guadagni, già di per se illeciti, ottenuti prendendo il controllo di alcuni black market presenti sul darkweb, per i quali è scattato il sequestro di milioni di euro presso agenzie di exchange in tutto il mondo.

Dalle indagini è emerso inoltre che il ragazzo, informatico di professione, era inserito in un più ampio ambito criminale ancora tutto da definire e che, grazie alle chat e agli spazi del dark web monitorati dai poliziotti, se ne stanno ricostruendo i legami di appartenenza con reti di gruppi hacker, italiani ed esteri, più articolati e collegati anche alla criminalità dell'isola.

Tra le vittime finora accertate ci sono gestori telefonici e telematici, fornitori di servizi satellitari e persino i sistemi della Guardia di Finanza.

Alessio Evangelista

02/10/2024