Operazione “People1” contro il cybercrime

Violate centinaia di credenziali di accesso a dati sensibili, rubate migliaia di informazioni private contenute in archivi informatici della pubblica amministrazione relative a posizioni anagrafiche, contributive, di previdenza sociale e dati amministrativi appartenenti a centinaia di cittadini e imprese del nostro Paese.

È quanto è stato scoperto dagli investigatori del Servizio Polizia postale e delle comunicazioni, che hanno arrestato, a Sanremo (Imperia), un uomo di 66 anni esperto di sistemi informatici e denunciato altre sei persone. Durante l’operazione sono state eseguite diverse perquisizioni che hanno interessato anche alcune agenzie investigative.

Gli indizi raccolti durante le indagini indicavano proprio il 66enne come il principale responsabile di ripetuti attacchi ai sistemi informatici di numerose Amministrazioni centrali e periferiche italiane, attraverso i quali sarebbe riuscito ad intercettare illecitamente centinaia di credenziali di autenticazione (userID e password).

L’uomo ha attaccato i sistemi informatici di alcuni Comuni italiani riuscendo a introdursi in banche dati di rilievo istituzionale, come Agenzia delle Entrate, Inps, Aci ed Infocamere.

Le sei persone denunciate erano, invece, coloro che, a vario titolo impiegati all’interno di note agenzie investigative e di recupero crediti, commissionavano all’uomo gli accessi abusivi e il furto delle preziose credenziali, per poi farne uso nelle rispettive attività professionali.

L’attività investigativa degli uomini del Cnaipic ha permesso di capire come l’esperto informatico, nel corso degli anni, avesse creato un vero e proprio sistema di servizi, tra cui il portale illecito “PEOPLE1”, commercializzato clandestinamente ed offerto alle agenzie interessate, le quali, pagando una sorta di canone, potevano istallare il software con una semplice pen-drive USB, e riuscire così a connettersi clandestinamente alle banche dati istituzionali e fare interrogazioni dirette.

Per ottenere l’accesso clandestino alle banche dati, venivano utilizzati messaggi di posta elettronica (phishing), apparentemente provenienti da istituzioni pubbliche, ma in realtà contenenti in allegato pericolosi malware. I messaggi arrivavano a migliaia di dipendenti di Amministrazioni centrali e periferiche, in particolare a quelli dei piccoli Comuni e dei patronati, che venivano, con l’inganno, portati a cliccare sull’allegato “malevolo” aprendo così la porta al sofisticato virus informatico che, in poco tempo, consentiva agli hacker di assumere il controllo dei computer.

L’arrestato, nella sua attività criminale, si è avvalso anche della “consulenza” di hacker freelance stranieri ingaggiati all’interno del Darkweb, che sono in fase di identificazione.

Le indagini degli specialisti della postale, iniziate nel 2017, a seguito di una segnalazione di una società di sicurezza informatica che, per prima, aveva individuato la minaccia di una campagna di spear-phishing, hanno evidenziato anche gli ingenti guadagni dell’attività criminale.

Una singola interrogazione alle banche dati istituzionali veniva venduta a partire da 1 euro “a dato”, e sono state decine di migliaia le interrogazioni illecite accertate.

22/11/2019