

Chiusa Genesis Market, la piattaforma che vendeva credenziali rubate

Era uno dei più grandi mercati neri virtuali del mondo, dedicato alla vendita di credenziali rubate. Si tratta della piattaforma Genesis Market, oggetto dell'operazione internazionale di polizia informatica conclusa oggi negli Stati Uniti e in Europa.

Sono 16 i Paesi coinvolti dall'indagine "Cookie monster" condotta da Fbi (Federal bureau of investigation) e polizia olandese, coordinata da Europol ed Eurojust e diretta, per il territorio italiano, dalla Procura della Repubblica di Roma.

La piattaforma oggetto dell'indagine, specializzata nella vendita di credenziali di accesso e dati rubati, con un giro di affari di oltre 2 milioni di identità virtuali sottratte, è stata disattivata, con sequestri, eseguiti in tutta Europa, dei server sui quali poggiava l'infrastruttura informatica.

Nel nostro Paese risultano coinvolte migliaia di credenziali, individuate dagli specialisti del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) della Polizia, relative sia a spazi informatici della vita privata di comuni cittadini (email, social network, account di e-commerce, ecc.), sia password in grado di garantire l'accesso illecito a spazi informatici istituzionali della pubblica amministrazione, nonché a spazi appartenenti a banche e grandi imprese nazionali, erogatrici di servizi pubblici essenziali.

Solo in Italia sono stati eseguiti 37 decreti di perquisizione personale, locale e informatica dagli specialisti del Cnaipic e dei Centri operativi per la sicurezza cibernetica della Polizia postale di Campania, Basilicata, Molise, Lazio, Lombardia, Puglia, Emilia Romagna, Calabria, Veneto, Sicilia occidentale, Abruzzo, Friuli Venezia Giulia, Liguria, Toscana, Trentino Alto Adige ed Umbria. Oggetto dei provvedimenti sono stati i clienti della piattaforma che, nel corso del tempo, avevano acquistato migliaia di credenziali di accesso.

Le perquisizioni hanno portato al sequestro di diversi dispositivi informatici, l'analisi dei quali consentirà agli investigatori di comprendere con esattezza quale sia stato l'utilizzo, da parte degli indagati, delle credenziali illecite acquistate, e che tipo di informazioni riservate, e a quale livello di segretezza, siano state compromesse.

Sergio Foffo

05/04/2023