

Cyber crime: colpito uno dei maggiori gruppi hacker

Uno dei gruppi hacker più noti al mondo, Ragnar Locker, è stato colpito da un'operazione di polizia internazionale condotta per l'Italia dalla Polizia di Stato.

L'indagine svolta dal Centro operativo per la sicurezza cibernetica (COSC) della Lombardia, con il coordinamento del CNAIPIC del Servizio Polizia postale, ha consentito di individuare e fermare in Francia un informatico trentacinquenne considerato figura di spicco all'interno della gang criminale per il suo ruolo di sviluppatore dei software malevoli utilizzati per la cifratura dei dati delle aziende attaccate.

Ragnar Locker è uno dei maggiori gruppi criminali specializzati in attacchi informatici di tipo ransomware: attacchi distruttivi, in grado di cifrare, e quindi paralizzare, i sistemi colpiti, pregiudicando così l'erogazione di servizi pubblici essenziali in vari settori.

L'ospedale israeliano "Mayanei Hayeshua" di Tel Aviv e la principale compagnia aerea portoghese sono solo due tra le recenti e più importanti vittime del gruppo, che in Italia ha colpito, dal 2020, l'Azienda Ospedaliera di Alessandria, la Campari s.p.a., multinazionale leader nel settore food & beverage e la Dollmar s.p.a., importante distributore di prodotti chimico-industriali.

Per ottenere il ripristino dei dati i criminali richiedevano riscatti da 5 a 70 milioni di dollari, ma a fronte del pagamento la restituzione non aveva luogo; seguiva piuttosto l'ulteriore ricatto della pubblicazione sul darkweb dei dati esfiltrati (tecnica della "doppia estorsione").

Inoltre il gruppo criminale dissuadeva le vittime dal rivolgersi alla polizia, minacciando, in caso contrario, di pubblicare i dati sulla propria pagina nel darkweb, chiamata Wall of Shame (il "Muro della Vergogna"), ora sotto sequestro.

Le indagini della Polizia Postale, coordinate dalla Procura della Repubblica di Milano, si sono unite alle indagini della Gendarmeria Francese, del FBI americano e di altri 7 Paesi. L'attività investigativa è poi confluita in una settimana di azione operativa congiunta, supportata da Eurojust ed Europol e condotta in quattro diversi Paesi, che ha portato al fermo del trentacinquenne presso l'aeroporto di Parigi. Gli investigatori hanno eseguito anche la perquisizione informatica dei device nella sua residenza a Praga, e il sequestro dei computer su cui poggiava l'infrastruttura criminale in vari Paesi europei, tra cui Germania, Lettonia, Svezia e Olanda.

L'attività investigativa, condotta dagli specialisti della Polizia postale anche mediante intercettazioni telematiche transnazionali dei server in mano al gruppo criminale, è partita dall'analisi forense dei sistemi informatici attaccati da Ragnar Locker nell'ottobre del 2020; i poliziotti sono riusciti a identificare, ricostruire e localizzare l'intera infrastruttura criminale, protetta da un complesso sistema di anonimizzazione multilivello, che sfruttava server dislocati in tutto il mondo.

L'operazione denominata "TALPA", che ha visto coinvolti gli organi investigativi di ben 12 Paesi, costituisce un salto di qualità nelle indagini in materia di ransomware, che sono molto complesse a causa della distribuzione internazionale delle infrastrutture criminali, all'utilizzo di sistemi di cifratura e del ricorso a criptovalute per i pagamenti.

Serena Felici

20/10/2023