PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5935 di Lunedì 06 ottobre 2025

Bloccata una delle più temibili organizzazioni di crimine informatico

Il 24 luglio del 2025, le forze di polizia del Dipartimento di giustizia degli Stati Uniti sono riuscite a bloccare le attività di del gruppo criminoso BlackSuit (Royal), chiudendo quattro server e nove domini.

I brillanti risultati ottenuti da questa attività di indagine dimostrano come oggi il contrasto al crimine informatico sia oltremodo complesso e richieda la collaborazione di forze di polizia di vari paesi, di qua e di là dell'Atlantico.

Le indagini sono state condotte dal dipartimento di sicurezza nazionale-HSI, dal servizio segreto, dall'FBI e dalle forze dell'ordine di vari paesi, come il Regno Unito, la Germania, le Olanda, la Francia, il Canada e l'Ukraina e le azioni di blocco hanno compreso l'emissione di un mandato per il sequestro di criptovalute del valore di 1.091.453 dollari, al momento del sequestro.

«Il targeting persistente della gang di ransomware BlackSuit sulle infrastrutture critiche degli Stati Uniti rappresenta una seria minaccia per la pubblica sicurezza degli Stati Uniti», ha dichiarato il vice procuratore generale per la sicurezza nazionale John A. Eisenberg.

«La Divisione per la Sicurezza Nazionale è orgogliosa di far parte di un team coordinato di agenzie governative e partner che lavorano per proteggere la nostra Nazione dalle minacce alle nostre infrastrutture critiche».

«Questa azione esemplifica l'approccio proattivo e prioritario alla neutralizzazione, che stiamo adottando per affrontare questa minaccia», ha affermato il procuratore statunitense Erik S. Siebert per il Distretto Orientale della Virginia.

«Quando si tratta di proteggere le imprese statunitensi, le infrastrutture critiche e altre vittime dai ransomware e da altri attori delle minacce informatiche, non ci tireremo indietro». «Troppo spesso vediamo i danni che i ransomware causano ai sistemi, che poi consentono ai criminali informatici di scatenare il caos su aziende e altri», ha affermato il procuratore statunitense Jeanine Ferris Pirro per il Distretto di Columbia.

"Interrompere l'infrastruttura del ransomware non riguarda solo il mettere offline i server, ma riguarda lo smantellare l'intero ecosistema, che consente ai criminali informatici di operare con impunità," ha dichiarato il vicedirettore assistente Michael Prado del Centro per i crimini informatici (C3) dell'HSI. "Questa operazione è il risultato di un'incessante coordinamento internazionale e dimostra la nostra risolutezza collettiva nel ritenere gli attori del ransomware responsabili." "Questa operazione infligge un colpo critico all'infrastruttura di BlackSuit."

Come dettagliato in un annuncio dell'HSI, un'operazione delle forze dell'ordine statunitensi, in stretto coordinamento con partner internazionali, ha portato con successo al sequestro di server, domini e beni digitali utilizzati dal gruppo BlackSuit Ransomware per distribuire ransomware, estorcere denaro dalle vittime e riciclare i proventi di queste attività. Alcuni di questi proventi includevano circa $1.091.453 in valuta virtuale (valutata al momento del furto) ? che è stata sequestrata separatamente dall'Ufficio del Procuratore degli Stati Uniti per il Distretto di Columbia, utilizzando prove raccolte dall'Ufficio del Procuratore degli Stati Uniti per il Distretto Orientale della Virginia il 21 giugno 2024.

Le vittime di questi attacchi sono tipicamente costrette a pagare riscatti in BTC, accedendo a un sito web del darknet. Intorno al 4 aprile 2023, una vittima ha pagato un riscatto di 49.3120227 Bitcoin, per decrittografare i propri dati. Questo riscatto valeva 1.445.454,86 dollari al momento della transazione.

Una parte di questi proventi (1.091.453 dollari) è stata ripetutamente depositata e ritirata su un conto di scambio di valuta virtuale, fino a quando i fondi sono stati congelati. L'HSI, il Servizio Segreto degli Stati Uniti, l'IRS-CI e l'FBI stanno indagando sul caso, insieme all'Agenzia Nazionale per la Criminalità del Regno Unito e all'Unità di Criminalità Organizzata della Regione Nord-Occidentale, al Landeskriminalamt Niedersachsen della Germania, all'An Garda Síochána - Garda National Cyber Crime Bureau dell'Irlanda, all'Office Anti-Cybercriminalité della Francia, alla Royal Canadian Mounted Police e al Delta Police Department del Canada, alla National Police ? Cyber Police Department dell'Ucraina e al Criminal Police Bureau della Lituania.

Se qualcuno dubita che l'unione delle risorse non sia fruttuosa, ecco una clamorosa smentita.

Adalberto Biasiotti

www.puntosicuro.it