PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6117 di Mercoledì 08 luglio 2026

BlackCat: due professionisti della cybersecurity finiscono in carcere

La storia di questa indagine, che ha portato alla condanna di due criminali informatici, può costituire un potente dissuasore per possibili imitatori.

Due professionisti americani della sicurezza informatica sono stati condannati, il 30 aprile 2026, a quattro anni di carcere ciascuno per il loro ruolo in una cospirazione volta a ostacolare, ritardare o influenzare il commercio attraverso l'estorsione, in relazione ad attacchi ransomware avvenuti nel 2023. Ecco come si sono svolte le indagini.

Secondo i documenti del tribunale, i due malviventi ed un altro complice hanno diffuso con successo il ransomware, noto come ALPHV BlackCat, tra aprile 2023 e dicembre 2023 contro diverse vittime, situate in tutti gli Stati Uniti.

I tre uomini si accordarono per pagare agli amministratori di ALPHV BlackCat una quota del 20% di qualsiasi riscatto ricevuto, in cambio dell'accesso al ransomware e alla piattaforma di estorsione di ALPHV BlackCat. Tutti e tre lavoravano nel settore della sicurezza informatica, il che significa che possedevano competenze ed esperienze specifiche nella protezione dei sistemi informatici, compreso il tipo di danno che stavano infliggendo alle vittime. Dopo aver estorto con successo circa 1,2 milioni di dollari in Bitcoin ad una vittima, gli uomini si divisero l'80% del riscatto in tre parti e riciclarono i fondi attraverso vari canali.

Secondo i documenti del tribunale, ALPHV BlackCat ha preso di mira le reti informatiche di oltre 1.000 vittime in tutto il mondo. Il gruppo ha utilizzato un modello di ransomware-as-a-service (RAS), in cui gli sviluppatori erano responsabili della creazione e dell'aggiornamento del ransomware e della manutenzione dell'infrastruttura internet illegale.

"Le sentenze emesse oggi dal tribunale riflettono il danno che questi imputati hanno inflitto con i loro attacchi informatici alle aziende vittime in tutti gli Stati Uniti", ha dichiarato il viceprocuratore generale A. Tysen Duva della Divisione penale del Dipartimento di Giustizia. "Hanno danneggiato importanti aziende che fornivano servizi medici e ingegneristici. Si sono anche divisi i riscatti ricevuti e hanno riciclato i proventi illeciti. Questi avrebbero dovuto essere specialisti in sicurezza informatica, vale a dire persone che agivano per il bene delle imprese e dei cittadini. Invece, hanno usato le loro elevate competenze informatiche per soddisfare la loro avidità. Gli autori di attacchi ransomware come questi dovrebbero essere puniti e allontanati dalla società, per scontare la pena che spetta loro, in modo che non possano nuocere ad altri."

"Questi imputati hanno sfruttato le loro conoscenze specialistiche in materia di sicurezza informatica non per proteggere le vittime, ma per estorcere loro denaro", ha dichiarato il procuratore degli Stati Uniti Jason A. Reding Quiñones, per il Distretto Meridionale della Florida. "Hanno utilizzato ransomware per bloccare sistemi critici, rubare dati sensibili e costringere le aziende americane a pagare per riottenere l'accesso alle proprie informazioni. La condanna odierna a quattro anni riflette non solo la portata di questo piano, ma anche il danno reale inflitto ad aziende, dipendenti e vittime, le cui informazioni private sono state utilizzate a scopo di lucro. In questo distretto, i criminali informatici saranno condannati al carcere federale e perderanno i proventi dei loro crimini".

"Le condanne odierne dimostrano che i criminali informatici specializzati in ransomware possono operare ovunque e che l'FBI si sta impegnando attivamente per rintracciarli e smantellare le loro reti, ovunque si trovino", ha dichiarato il vicedirettore Brett Leatherman della Divisione Cyber ??dell'FBI. I malviventi hanno sfruttato le loro competenze tecniche e le loro conoscenze in materia di sicurezza informatica per estorcere milioni di dollari a vittime in tutti gli Stati Uniti, ma la indagine globale dell'FBI ha garantito che alla fine siano stati assicurati alla giustizia. Quando un malvivente ha cercato di fuggire all'estero per sottrarsi al processo, l'FBI lo ha tracciato attraverso ben 10 paesi, dimostrando fino a che punto siamo disposti ad arrivare per assicurare alla giustizia i criminali informatici e proteggere le vittime. L'FBI ringrazia i suoi partner del Dipartimento di Giustizia per il loro contributo al risultato odierno."

L'annuncio odierno fa seguito alle precedenti azioni del Dipartimento di Giustizia del dicembre 2023 per smantellare il ransomware ALPHV BlackCat, grazie alle quali l'FBI ha sviluppato uno strumento di decrittazione, che ha permesso agli uffici sul territorio nazionale e alle forze dell'ordine, partner in tutto il mondo, di offrire a centinaia di vittime la possibilità di ripristinare i propri sistemi, risparmiando loro circa 99 milioni di dollari in pagamenti di riscatto. All'epoca, l'FBI sequestrò anche diversi siti web gestiti da ALPHV BlackCat.

Nel dicembre 2025, i malviventi si sono dichiarati colpevoli di un capo d'accusa di cospirazione per ostacolare, ritardare o influenzare il commercio o la movimentazione di qualsiasi articolo o merce mediante estorsione. Nell'aprile 2026, anche il co-cospiratore si è dichiarato colpevole di un capo d'accusa di cospirazione per ostacolare, ritardare o influenzare il commercio o la movimentazione di qualsiasi articolo o merce mediante estorsione. Oltre a cospirare con i primi due malviventi per attaccare le vittime con il ransomware, egli ha anche abusato del suo ruolo di negoziatore con le vittime del ransomware. condividendo con gli autori delle minacce informazioni riservate sulle vittime, per aumentare il valore del riscatto pagato. La sua sentenza è stata emessa il 9 luglio 2026.

L'ufficio dell'FBI di Miami sta conducendo le indagini, con l'assistenza del Servizio Segreto degli Stati Uniti.

Un contributo significativo a questa indagine è stato fornito dal viceprocuratore Paul B. Morris per il Distretto Orientale della Florida e dal viceprocuratore degli Stati Uniti Daniel W.A. Peach per il Distretto Centrale della Georgia. Ulteriore assistenza è stata fornita dalla Policía de Investigación dell'Aeropuerto Internacional de la Ciudad de México.

Quando si dice: "l'unione fa la forza!".

Adalberto Biasiotti

www.puntosicuro.it