

Polizia di Stato

Polizia Postale "Operazione Palmbeach"

La Polizia Postale, sotto la direzione della Procura della Repubblica di Milano, nel corso di un'operazione di polizia internazionale, ha sequestrato un'infrastruttura di rete VPN, in grado di anonimizzare e cifrare le tracce informatiche usata da gruppi criminali che colpivano le loro vittime attraverso i ransomware. L'operazione, condotta dalla Polizia Postale di Milano, che ha coinvolto forze dell'ordine e autorità giudiziarie in Europa, Stati Uniti e Canada, è stata coordinata dall'Europol, Eurojust e dalla procura nazionale olandese. La Polizia Postale ha chiuso uno dei nodi dell'infrastruttura della rete che forniva un rifugio sicuro ai criminali informatici da cui attaccare le vittime. In varie parti del mondo sono stati sequestrati i server dove DoubleVPN ospitava contenuti, mentre i relativi domini web sono stati sostituiti da una splash page con i loghi delle forze dell'ordine partecipanti. Tale sequestro coordinato è stato effettuato nel quadro della piattaforma europea multidisciplinare contro le minacce criminali (EMPACT). DoubleVPN era ampiamente pubblicizzato sui forum underground di criminalità informatica, sia russi che anglofoni, come mezzo per consentire a operatori di ransomware e truffatori di phishing di mascherare la propria ubicazione e identità. Il servizio si vantava di fornire un alto livello di anonimato offrendo connessioni VPN singole, doppie, triple e persino quaduple ai suoi clienti. DoubleVPN è stato utilizzato per compromettere reti in tutto il mondo e la sua connessione VPN più economica costava solo 22 euro (25 dollari). Coordinamento internazionale :La cooperazione internazionale è stata fondamentale per il successo di questa indagine, poiché le infrastrutture critiche erano sparse in tutto il mondo. - Il Centro europeo per la criminalità informatica di Europol (EC3) ha supportato l'indagine fin dall'inizio, riunendo tutti i paesi coinvolti per stabilire una strategia comune. I suoi specialisti di criminalità informatica hanno organizzato oltre 30 riunioni di coordinamento e quattro workshop per preparare la fase finale del takedown, oltre a fornire assistenza analitica e di cripto-tracing. Nel giorno dell'operazione, presso Europol è stato istituito un posto di comando virtuale per garantire un coordinamento continuo tra tutte le autorità coinvolte nell'operazione. - Eurojust ha facilitato la cooperazione giudiziaria transfrontaliera e il coordinamento, per garantire una risposta adeguata al fine di smantellare la rete. A questo scopo, fin dall'ottobre dello scorso anno, si sono svolte sei riunioni di coordinamento dedicate, organizzate da Eurojust, e si è creato un centro di coordinamento nel giorno del takedown. Il procuratore olandese Wieteke Koorn ha dichiarato: "Questa indagine penale riguarda i criminali che pensano di poter rimanere anonimi, agevolando le operazioni di criminalità informatica su larga scala. Con la nostra iniziativa, compreso il potere investigativo speciale sulle intrusioni digitali, vogliamo rendere molto chiaro che non ci possono essere rifugi sicuri per questo tipo di criminali. I loro atti delinquenti danneggiano la società digitalizzata ed erodono la fiducia dei cittadini e delle aziende nelle tecnologie digitali, quindi il loro comportamento deve essere fermato". Il capo dell'EC3 di Europol, Edvardas Šileris, ha commentato: "Le forze dell'ordine sono più efficaci quando lavorano insieme e il comunicato di oggi manda un messaggio forte ai criminali che usano questi servizi: l'età dell'oro delle VPN criminali è finita. Insieme ai nostri partner internazionali, siamo impegnati a far arrivare questo messaggio forte e chiaro".

Autorità e polizie partecipanti:

- Paesi Bassi: Polizia nazionale (Politie), Procura nazionale (Landelijk Parket)
- Germania: Ufficio federale di polizia criminale (Bundeskriminalamt), Ufficio del procuratore generale di Francoforte sul Meno - Centro per la criminalità informatica
- Regno Unito: Agenzia Nazionale del Crimine (NCA)
- Canada: Polizia Canadese (RCMP)
- Stati Uniti: Federal Bureau of Investigation (FBI), US Secret Service (USSS), US Department of Justice (DOJ)
- Svezia: Autorità di polizia svedese (Polisen), Autorità giudiziaria svedese (Åklagarmyndigheten)

- Italia: Compartimento Polizia Postale e delle Comunicazioni Lombardia, Servizio Polizia Postale e delle Comunicazioni Roma, Procura della Repubblica di Milano

- Bulgaria: Direzione generale per la lotta contro la criminalità organizzata del Ministero dell'Interno bulgaro (?????? ????????? "????? ? ?????????????????? ?????????????" ??? ?????????????????? ?? ?????????????? ??????? ?? ????????????? ??????????)

- Svizzera: Polizia Cantonale Ticino (Polizia Cantonale del Canton Ticino), Ministero Pubblico del Canton Ticino

- Europol: Centro europeo per la criminalità informatica (EC3)

- Eurojust .

01/07/2021