

Cyber crimine, 77mila alert Faro su terrorismo e spionaggio

Polizia Postale. Verifiche anti terrorismo: 182mila contenuti web controllati, 2.700 siti oscurati Oltre 10.700 illeciti finanziari, 927 indagati e 6,2 milioni recuperati. Controlli a tutela delle imprese

I.Cimm. S.Mo.



Polizia di Stato. Oggi i festeggiamenti del 172° anniversario della fondazione

Alle campagne di «disinformazione» attuate contro l'Occidente da collettivi hacker riconducibili a Russia, Cina e Corea del Nord ora si aggiungono le crescenti tensioni di matrice terroristica. Piattaforme di comunicazione online, social network e chat di messaggistica istantanea, come Signal e Telegram, sono sempre più il vettore per veicolare fake news e propagande jihadiste, cui sono da aggiungere le campagne di finanziamento al terrorismo, sempre più "camuffate" da false raccolte fondi per beneficenza. Come è emerso anche nella dichiarazione finale in occasione del vertice sull'agenda Nato 2030, saremo «chiamati ogni giorno di più a confrontarci con minacce cyber e ibride, comprese le campagne di disinformazione, e l'uso dannoso di tecnologie emergenti sempre più sofisticate, come l'intelligenza artificiale, per fini malevoli». In Italia il fenomeno è sotto l'attenta analisi investigativa del Servizio di Polizia Postale e delle Comunicazione, come emerge dal rapporto sulle attività svolte nel 2023, diffuso oggi in occasione del 172° anniversario della fondazione della Polizia di Stato.

Disinformazione

Stando ai rapporti dell'intelligence europea, Mosca, in particolare, ha intensificato gli sforzi per manipolare le informazioni, diffondendole sulla rete allo scopo di veicolare l'opinione pubblica. Un fenomeno particolarmente preoccupante, che nell'ultimo periodo, ha fatto registrare una pericolosa impennata. Come nel caso delle fake news all'indomani dell'attacco terroristico di Isis-K al Crocus City Hall di Mosca, che

ambienti vicini al Cremlino hanno provato a legare a iniziative di spionaggio dell'Ucraina con i servizi Occidentali. La Polizia Postale ha alzato il livello dell'allerta in occasione delle consultazioni elettorali europee previste per l'8 e il 9 giugno. Ci sono alert di iniziative "opache" da parte di organizzazioni e collettivi di matrice "statuale", cioè legati a stati esteri, su campagne di disinformazione. L'obiettivo è duplice: veicolare il voto e muovere pressioni sull'opinione pubblica per manipolare le agende politiche.

Cyber-terrorismo

In tema di terrorismo, soprattutto islamico, il Governo ha elevato l'allerta dopo l'attentato di Mosca. La Polizia Postale nell'ultimo anno (in materia di estremismo religioso e politico, area antagonista) ha indagato 51 persone. Nel monitoraggio della rete sono stati visionati 182.209 spazi web e in 2.037 casi sono stati rilevati contenuti illeciti; mentre 2.700 sono state le risorse oscurate per attività info-investigative (come anticipato sul Sole 24 Ore del 26 marzo).

Cybercrime finanziario

Con riferimento a financial cybercrime le statistiche fanno registrare 10.755 casi per i quali sono state indagate 927 persone. Nonostante la difficoltà operativa di bloccare e recuperare le somme frodate, dirottate soprattutto verso paesi extraeuropei (Cina, Taiwan, Hong Kong), grazie alla versatilità della piattaforma OF2CEN (On line fraud cyber centre and expert network) per l'analisi e il contrasto avanzato delle frodi del settore, sono stati bloccati e recuperati alla fonte 6.232.280 euro, su una movimentazione di 18.897.566. Sono in corso attività di cooperazione internazionale finalizzate al recupero delle restanti somme.

Infrastrutture e imprese

Il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (Cnaipic) ha gestito, a livello nazionale, 632 attacchi a sistemi informatici di strutture nazionali di rilievo strategico, 79 richieste di cooperazione nel circuito High Tech Crime Emergency e avviato 96 indagini e indagato 98 persone. L'attività di prevenzione è stata caratterizzata dalla diramazione di 77.012 alert. Attraverso i Nosc (Nuclei operativi sicurezza cibernetica), è stata coordinata la gestione di 11.469 attacchi a infrastrutture critiche, operatori di servizi essenziali, privati e aziende e indagato 126 persone.

© RIPRODUZIONE RISERVATA