

## NUCLEO OPERATIVO SICUREZZA CIBERNETICA LOMBARDIA (N.O.S.C.)

Nell'attuale e particolare contesto internazionale, l'escalation delle tensioni geopolitiche connesse al conflitto in Ucraina continua ad avere significativi riverberi anche in materia di sicurezza cibernetica. Risultano, infatti, in corso campagne massive a livello internazionale dirette verso infrastrutture critiche, sistemi finanziari e aziende operanti in settori strategici quali comunicazione e difesa, tra le quali figurano campagne di phishing, diffusione di malware distruttivi (specialmente Ransomware), attacchi Ddos, campagne di disinformazione e leak di database. Inoltre, alcuni tra i più pericolosi gruppi di hacker criminali hanno deciso di schierarsi a favore della Russia, altri con l'Ucraina, prendendo di fatto parte al conflitto nel c.d. "dominio cibernetico". Il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche (CNAIPIC) del Servizio Polizia Postale e delle Comunicazioni, attraverso dedicati alert diffonde ai NOSC gli indicatori di compromissione e gli avvisi di informazione di sicurezza da riportare ai potenziali target di azioni ostili. In tale contesto il Centro Operativo per la Sicurezza Cibernetica della Polizia Postale della Lombardia, ha svolto adeguati servizi di monitoraggio e analisi, condividendo ogni evidenza utile in relazione al quadro internazionale in parola; in caso di attacco, oltre ai necessari approfondimenti investigativi, ha tempestivamente svolto l'analisi tecnica della minaccia, nonché fornito il supporto operativo, per il veloce ritorno alla piena operatività dei sistemi informatici colpiti. Nella sottostante tabella si riportano i dati relativi alle attività svolte dal C.O.S.C. Lombardia nell'ambito del computer crime.

Attacchi infrastrutture critiche ad istituzioni, aziende e privati

2021 2022

Variazione percentuale

Casi Trattati 548 1312 +139% Persone Indagate 22 25 +13%

Al fine di potenziare l'attività di prevenzione e contrasto dagli attacchi/danneggiamenti alle infrastrutture informatiche critiche della Lombardia, sono stati siglati nel corso del 2022, due protocolli d'intesa con i colossi "Feralpi Siderurgica S.p.A." e "Industrie DeNora S.p.A.".

In tale ambito si segnalano anche le seguenti operazioni:

Operazione "Rear Window" ove questo C.O.S.C., coordinato dalla Procura della Repubblica di Milano, è riuscito a disarticolare un vero e proprio "sistema" criminale finalizzato alla violazione, mediante intrusioni informatiche, di impianti di videosorveglianza installati per lo più presso private abitazioni effettuando 10 perquisizioni su tutto il territorio nazionale. L'inquietante fenomeno è stato scoperto grazie alla segnalazione di un cittadino e agli sviluppi dell'analisi forense compiuta sullo smartphone sequestrato a uno degli indagati nell'ambito di un altro procedimento penale, relativo a reati di altra natura.

Operazione "Dark Resolution" – L'attività è stata avviata a seguito delle informazione acquisite dal Servizio Polizia Postale e delle comunicazioni nel corso del consueto scambio informativo con le collaterali forze di Polizia estere; in particolare detective stranieri, nel corso di un'autonoma attività di indagine, avevano accertato che un cliente sconosciuto aveva commissionato sul "dark web" un

omicidio per la somma di 5.000 dollari in criptovalute – bitcoin, avente come vittima un cittadino straniero residente nella provincia di Sondrio. L'indagine ha consentito di individuare il mandante nonché l'indirizzo "onion" della piattaforma ove è materialmente avvenuto l'assoldamento del presunto sicario.

#### FINANCIAL CYBERCRIME

Nell'ambito delle competenze della Polizia Postale si segnala il rafforzamento dell'attività di prevenzione attraverso il monitoraggio attivo della rete e un'articolata attività di contrasto alle truffe online con 267 persone deferite all'Autorità Giudiziaria, in particolare nel settore dell'e-commerce, market place e del trading online.

#### Truffe OnLine 2021 2022

Variazione percentuale Casi trattati 1.816 2.780 +53% Persone indagate 269 203 -24% Somme sottratte € 16.261.747 € 24.654.654 +52%

Nell'ambito delle citate truffe sul web, nel corso del 2022, si è registrato un importante l'incremento degli illeciti legati al fenomeno del trading online, da attribuire anche all'aumento del numero di portali che propongono programmi speculativi, apparentemente redditizi, e l'utilizzo di tecniche molto sofisticate per contattare le vittime. L'attività investigativa, qualora la denuncia sia tempestiva, prevede l'immediata attivazione dei canali di Cooperazione Internazionale di Polizia, con la richiesta del blocco urgente delle somme versate e l'espletamento di accertamenti sui flussi finanziari normalmente destinati all'estero.

Particolare attenzione è rivolta inoltre ai fenomeni del revenge porn, con 45 casi trattati e 6 persone denunciate e delle truffe romantiche, con 66 casi trattati e 9 persone denunciate, spesso sommersi in quanto caratterizzati da un forte coinvolgimento emotivo che induce la vittima a non denunciare.

Specifiche iniziative sono state rivolte all'attività di prevenzione e contrasto al fenomeno degli atti intimidatori nei confronti della categoria dei giornalisti e servizi di monitoraggio dei canali di diffusione, costituiti da siti web, piattaforme di digitali, profili e pagine presenti sui social network più noti (Facebook, Twitter, Instagram, Telegram, Pinterest e Youtube), finalizzati ad arginare la diffusione del linguaggio d'odio (hate speech).

Il monitoraggio di siti e spazi web (blog, gruppi social e siti dedicati) dediti a giochi e scommesse clandestine è un'altra attività operativa particolarmente seguita dalla Polizia Postale e delle Comunicazioni, sia per contrastare la diffusione irregolare o illegale, che per tutelare gli interessi dei consumatori, specie se minori d'età: numerosi sono i siti con sedi legali presso paesi esteri, che operano in Italia anche se privi della prevista autorizzazione per poter esercitare legalmente la raccolta di scommesse.

In ultimo, ma comunque di primaria importanza, è stata l'attività rivolta all'individuazione di quelle persone che, sfruttando principalmente la cassa di risonanza che i social media offrono, hanno manifestato intenti suicidari in conseguenza dei quali sono state attivate tutte le procedure necessarie per la salvaguardia delle persone coinvolte con l'ausilio degli uffici di polizia competenti territorialmente.

#### SEZIONE CYBERTERRORISMO

Nel corso degli ultimi anni, il continuo e vertiginoso incremento dell'utilizzo delle piattaforme di comunicazione online, social network e di applicazioni di messaggistica istantanea, ha determinato un'allarmante diffusione di contenuti propagandistici riconducibili al terrorismo, ad una platea pressoché illimitata, sia di matrice islamista (jihadista, ISIS, Al Qaeda, Al Shabaab ed altre articolazioni locali), sia di formazioni suprematiste di estrema destra (neonazismo, neofascismo, tifoserie strutturate), nonché di estrema sinistra (movimenti di lotta armata, anarco/insurrezionalisti, antagonisti).

In tale ambito, la Polizia Postale garantisce sia l'esecuzione di una costante attività di monitoraggio investigativo della rete e dei canali di messaggistica istantanea, per l'identificazione e il deferimento all'Autorità Giudiziaria dei responsabili della diffusione dei contenuti illeciti, sia un costante scambio informativo con la Digos della locale Questura.

La costante attività di monitoraggio informativo ed investigativo ha permesso di accertare come nel corso degli ultimi mesi si sia stato registrato un notevole incremento dei trend e delle discussioni all'interno di chat in diverse piattaforme; si passa dai tradizionali gruppi Facebook (molti dei quali risultano essere già stati bloccati) a social meno noti, come Reddit, fino a piattaforme come 8chan, vk.com (Vkontakte), nonché Telegram, privilegiando tutte quelle piattaforme che per la propria policy garantiscono l'anonimato e rendono più complicata l'identificazione degli autori dei messaggi.

Alla luce di quanto premesso, appare opportuno evidenziare come gli operatori della sezione antiterrorismo abbiano intensificato le attività di monitoraggio proprio in tali contesti e, in raccordo con la Direzione Centrale della Polizia di Prevenzione, abbiano avviato numerose attività investigative, con il deferimento alle competenti Autorità Giudiziarie dei soggetti identificati – anche attraverso attività sotto copertura e perquisizioni – quali autori dei messaggi connotati dalla discriminazione razziale, etnica e religiosa.

Tra le numerose attività investigative espletate nel corso del 2022, si segnala quelle che ha condotto al deferimento alla competente A.G. di Milano di un uomo di 60 anni, residente nella provincia di Como, quale utilizzatore di un account Twitter, autore di due messaggi contenenti gravi minacce nei confronti del Capo dello Stato. Un'ulteriore attività d'indagine che merita di essere menzionata per importanza, è quella avviata dal Servizio Polizia Postale e coordinata dalla Procura della Repubblica di Roma, all'esito della quale, operatori dei Centri Operativi di Milano, Trieste e Venezia, unitamente a personale delle DIGOS di Milano, Vicenza ed Udine hanno eseguito perquisizioni delegate a carico di tre internauti nei cui confronti sono stati riscontrati elementi indiziari tali da farli ritenere autori della pubblicazioni di messaggi minatori rivolti all'ex Ministro degli Esteri Luigi Di Maio.

#### ATTIVITA' DI PREVENZIONE

La Polizia Postale se da un lato svolge un' incisiva attività di repressione dei reati informatici, dall'altro lato svolge un' importante azione preventiva a tutela dei minori, soprattutto per quanto concerne il fenomeno del cyberbullismo e di tutte le forme di prevaricazione online, fenomeni che destano grande allarme sociale. L'impegno profuso dagli specialisti della Polizia Postale nell'azione di sensibilizzazione e

informazione ha consentito, nell'anno appena trascorso, di realizzare incontri con docenti e genitori in oltre 614 istituti scolastici, coinvolgendo oltre 55.277 mila studenti, 3.223 insegnanti e 6.731 famiglie.