Polizia Postale: ecco il bilancio nel 2019

Data: Invalid Date | Autore: Redazione

Resoconto attività della Polizia Postale e delle Comunicazioni nel 2019 **CATANZARO, 31 DIC -**In uno scenario nel quale la continua evoluzione tecnologica influenza ogni azione del nostro vivere quotidiano, lo sforzo della Polizia Postale e delle Comunicazioni nell'anno 2019 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati di precipua competenza di questa Specialità.

C.N.C.P.O.

• Il ritmo frenetico delle innovazioni tecnologiche e dei nuovi mezzi di comunicazione, conseguenti alla diffusione di Internet su larga scala e, in particolare, la progressiva diffusione di *smartphones* e *tablets* tra i minori, sono solo alcuni degli elementi che agevolano le forme di aggressione in rete verso l'infanzia e l'adolescenza, determinando, di conseguenza, un notevole incremento non solo di reati che vedono coinvolti i minori online, quali la pornografia minorile e il *cyberbullismo*, ma anche della diffusione di altre forme di aggressione nei loro confronti, come le condotte autolesioniste, le c.d. *challenges* (es.: *Blue Whale, Binge Drinking), etc.*

• Considerato che uno degli aspetti propri del web che caratterizzano tali fenomeni, nonché tutte le comunità virtuali, è l'assenza di confini e, quindi, la sovranazionalità, che implica la presenza di utenti che si connettono dall'estero con server attestati in altri Paesi, l'attività di cooperazione internazionale, instaurata nel corso degli anni dal *Centro Nazionale per il Contrasto alla Pedopornografia Online*(C.N.C.P.O.) tramite EUROPOL e INTERPOL, sia con paesi dell'UE, sia extraeuropei, è di assoluta importanza, in quanto consente uno scambio info investigativo, nonché di condivisione di nuove tecniche di indagine e buone prassi nella materia.

In tale contesto, di assoluto rilievo risulta il ruolo svolto dalla Polizia Postale e delle Comunicazioni, in particolare, nell'ambito dei reati relativi allo **sfruttamento sessuale dei minori online**.Nell'anno in

corso sono state indagate **650** persone.

Le indagini relative al fenomeno dell'**adescamento di minori online**, invece, hanno consentito di indagare **180**soggetti.

Tra le citate attività di polizia giudiziaria, sono state eseguite **8 operazioni**di particolare rilievo, condotte dagli Uffici territoriali della Specialità e coordinate dal Centro, alcune delle quali svolte in modalità sotto copertura online e scaturite da segnalazioni pervenute nell'ambito dell'attività di cooperazione internazionale svolta dal C.N.C.P.O. che, complessivamente, hanno consentito di indagare in stato di libertà **151**soggetti.

Un fenomeno particolarmente insidioso che ha fatto breccia tra giovani e giovanissimi è rappresentato dagli *stickers*, fenomeno in crescente diffusione, che consiste nella condivisione, sulle piattaforme di messaggistica istantanea, di *adesivi digitali*gratuiti, a contenuto offensivo, violento, discriminatorio, antisemita, nonché pedopornografico.

Le piattaforme di messaggistica istantanea hanno offerto agli utenti la possibilità di utilizzare, accanto a *emoji(*simboli pittografici, simili agli emoticon e utilizzati negli SMS, nelle e-mail, nonché nei social), pacchetti di *stickers*messi a disposizione dai sistemi di messaggistica istantanea che offrono la possibilità di crearne di personalizzati e modificati ricavandoli da fotografie reali, tramite diverse "Applicazioni" gratuite, disponibili per IOS e Android.

Negli ultimi tempi, questo tipo di servizio sta ricevendo il consenso degli utenti preadolescenti e adolescenti, i quali, tuttavia, spesso ne fanno un uso improprio, diffondendo adesivi digitali dai contenuti illeciti (pedopornografici, xenofobi, discriminatori, etc.) ed esponendosi a responsabilità penali relative alla diffusione e divulgazione di materiale pedopornografico.

Attualmente sono stati rilevati **7** casi di *stickers*trattati da questa Specialità, conclusisi con altrettanti minori indagati per diffusione e detenzione di materiale pedopornografico.

Inoltre, tra le indagini più significative avviate direttamente dal Centro nell'ambito dei reati di sfruttamento sessuale dei minori, si segnala una complessa operazione, svolta in modalità sotto copertura online nelle ***Dark Net***, che ha consentito di trarre in arresto un 60enne per detenzione di materiale di sfruttamento sessuale dei minori, aggravato dall'ingente quantità, dall'utilizzo di mezzi di anonimizzazione e criptazione, nonché dalla particolare violenza di alcune immagini rinvenute, raffiguranti abusi sessuali su minori anche in tenerissima età. L'uomo è risultato di particolare interesse, anche a livello internazionale, per i ruoli di amministratore e moderatore che nel tempo ha ricoperto nelle comunità virtuali pedofile.

Contestualmente si segnalano le attività più importanti coordinate dal C.N.C.P.O., congiuntamente ai Compartimenti della Polizia Postale di Pescara, Torino, Venezia, Udine e Catania, nell'anno in corso, che sono le seguenti:

OPERAZIONE "TANA DELLA LUNA"

L'indagine è stata avviata dal Compartimento Polizia Postale di Catania e coordinata dal C.N.C.P.O., a seguito della denuncia della madre di un minore che ha scoperto, all'interno del telefono cellulare del figlio, un video di natura pedopornografica. Dall'analisi informatica dell'apparecchio telefonico è risultata, all'interno di un'applicazione di messaggistica istantanea, la presenza di due gruppi di utenti, uno dei quali denominato "Tana della luna", da cui trae spunto il nome dell'operazione, all'interno dei quali i partecipanti si sono si sono resi responsabili dei reati di divulgazione e detenzione di materiale pedopornografico. Al termine dell'indagine, sono stati eseguiti sul territorio nazionale 51 decreti di perquisizione personali e domiciliari. Si evidenzia che ben 28 dei

summenzionati decreti di perquisizione sono stati emessi dalla Procura della Repubblica per i minorenni di Catania nei confronti di soggetti di minore età che, tramite la precitata applicazione telefonica, hanno distribuito, diffuso, offerto e ceduto immagini e video a contenuto pedopornografico.

L'attività si è conclusa con**51 denunciati.**

OPERAZIONE "LITTLE PLAYERS"

L'Indagine, coordinata dal C.N.C.P.O. e condotta dalla Sezione Polizia Postale di Udine, trae spunto dalla segnalazione presentata da un sacerdote nei confronti di un suo ex alunno che attraverso il proprio profilo "Instagram" seguiva bambini e ragazzi in atteggiamenti provocanti, che presentavano altresì sul proprio profilo riproduzioni fotografiche pedo. La sezione di Udine effettuava la perquisizione informatica nei confronti dell'indagato e dall'analisi dei supporti informatici rinvenuti si acclarava la presenza, su tali supporti, di materiale pedopornografico. Inoltre, l'esame del materiale sequestrato consentiva agli operatori di verificare che il materiale illecito era stato oggetto di scambio con altri utenti del noto servizio di messaggistica istantanea "KIK", dove il soggetto era solito accedere, comunicando anche in lingua inglese.

Dalle risultanze emerse, prende il via una indagine molto più ampia e complessa, condotta in modalità sotto copertura, a seguito della quale sono stati individuati 36 soggetti che detenevano e divulgavano materiale pedopornografico tramite link a spazi cloud dove veniva archiviato il predetto materiale.

Pertanto sono state eseguite 36 perquisizioni, disposte dalla Procura della Repubblica di Trieste, volte ad individuare i soggetti responsabili di tali condotte delittuose.

L'attività si è conclusa con **35 denunciati e 1 arrestato**.

OPERAZIONE "X-FORCE"

Nell'ambito di un'attività coordinata dal C.N.C.P.O. e condotta dal Compartimento Polizia Postale di Venezia, su segnalazione della polizia canadese, sono state sviluppate tracce informatiche riconducibili a cittadini italiani indiziati per i reati di divulgazione e detenzione di materiale pedopornografico, perpetrati in Rete attraverso il noto servizio di messaggistica istantanea "KIK".

La Procura della Repubblica di Venezia ha, pertanto, emesso 10 decreti di perquisizione personale e domiciliare nei confronti di altrettanti utenti italiani.

Nel corso della perquisizione informatica espletata nei confronti di un arrestato è emerso, altresì, materiale autoprodotto in danno di tre minori italiani.

L'attività si è conclusa con **8 denunciati e 2 arrestati.**

OPERAZIONE "DIRTY WARE"

Nell'ambito di un'attività coordinata dal C.N.C.P.O. e dal Compartimento Polizia Postale di Pescara, su segnalazione della polizia canadese, sono state sviluppate tracce informatiche riconducibili a cittadini italiani indiziati per i reati di divulgazione e detenzione di materiale pedopornografico perpetrati in Rete attraverso i noti servizi di messaggistica istantanea "KIK" e "Wattpad".

La Procura della Repubblica de L'Aquila ha pertanto emesso 11 decreti di perquisizione personali e domiciliari, eseguiti sul territorio nazionale, nei confronti di altrettanti utenti italiani.

L'attività si è conclusa con **10 denunciati ed 1 arrestato.**

OPERAZIONE "LOST NET"

Nell’ambito di un’attività coordinata dal C.N.C.P.O. e dal Compartimento Polizia Postale di Torino, con modalità anche sotto copertura, sono stati eseguiti sul territorio nazionale 11 decreti di perquisizione personali e domiciliari emessi dalla Procura della Repubblica di Torino, volti ad identificare utenti italiani che si sono resi responsabili dei reati di divulgazione e detenzione di materiale pedopornografico perpetrati in Rete. L’attività sottocopertura si è svolta prevalentemente sul circuito Gigatribe, nonché sul noto servizio di messaggistica istantanea “TELEGRAM”, ove è stata riscontrata la presenza di canali trattanti specifiche tematiche.

Nel corso della perquisizione informatica è stato rinvenuto ingente quantitativo di materiale pedopornografico.

L’attività si è conclusa con **6 denunciati e 5 arrestati.**

Per quanto concerne l’attività di prevenzione svolta dal C.N.C.P.O. attraverso una continua e costante attività di monitoraggio della rete, sono stati individuati **46.077**siti internet, di cui **2.287**inseriti in *black list* ed oscurati in quanto presentavano contenuti pedopornografici.

SEZIONE OPERATIVA

Nell’ambito dei**reati contro la persona**perpetrati sul web, dal mese di gennaio ad oggi, sono state indagate **288**persone, per aver commesso estorsioni a sfondo sessuale, stalking, molestie e minacce sui social network.

Risultano in costante aumento le **diffamazioni on line**, soprattutto ai danni di persone che ricoprono incarichi istituzionali o comunque conosciute dal grande pubblico: **2426** i casi trattati e **738**le persone indagate.

Sono stati segnalati **514** casi di **ricatto on line** dall’inizio dell’anno.

Una particolare rilevanza ha assunto l’attività di contrasto al **revenge porn**, un fenomeno in continua crescita, per il quale sono **24**le persone indagate. Purtroppo i dati non rispecchiano la gravità e l’estensione del fenomeno, a causa della ritrosia a denunciare di molte persone.

Grande impegno è stato profuso al contrasto dei reati d’incitamento all’odio: sono oltre **2000**gli spazi virtuali monitorati nel 2019 per condotte discriminatorie di genere, antisemite, xenofobe e di estrema destra.

Si registra la continua crescita delle **truffe on line**: nel 2019 sono state ricevute e trattate oltre **196** mila segnalazioni che hanno consentito di indagare **3620**persone. Sempre più sofisticate sono state le condotte fraudolente commesse sulle piattaforme di e-commerce.

Sono aumentate le cosiddette **truffe romantiche**, che vedono come vittime delle donne di età compresa tra i 40 e i 60 anni, circuite da uomini conosciuti in rete e indotte con stratagemmi sentimentali a versare ingenti somme di denaro a truffatori senza scrupoli.

Si è evidenziato un significativo aumento del fenomeno delle **truffe** legate al **trading online**: molti utenti della rete, allettati dalla prospettiva di facili guadagni derivanti da investimenti “sicuri”, sono caduti nella rete di abili truffatori e finti intermediari finanziari investendo centinaia di migliaia di euro.

CNAIPIC

Di evidente incremento è l’attività di contrasto alla minaccia cyber svolta dal Centro Nazionale Anticrimine per la Protezione delle Infrastrutture Critiche (C.N.A.I.P.I.C.), attestata dal rilevante aumento del numero di alert diramati alle infrastrutture critiche nazionali che, rispetto al 2018, ha visto un aumento di oltre il 30%, sino a raggiungere **82484**alert.

La tempestiva condivisione dei c.d. “indicatori di compromissione” dei sistemi informatici con i fornitori di servizi pubblici essenziali ha consentito di rafforzare gli strumenti volti alla protezione della sicurezza informatica, garantita anche dalla costante attività di monitoraggio in contesti di interesse.

Il C.N.A.I.P.I.C. - Centro Nazionale Anticrimine Informatico nell’ambito del complessivo Sistema Informativo Nazionale per il Contrasto al Cyber Crime, progetto SINC3 finanziato con fondi ISF, ancora in fase di completamento e che mira ad estendere la rete di protezione cibernetica anche alle realtà più sensibili del Paese, ha gestito complessivi **1181** attacchi cyber significativi, di cui:

• **243**attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;

• **938** attacchi informatici diretti verso aziende sensibili e pubbliche amministrazioni locali;

• **79** richieste di cooperazione nell’ambito del circuito “High Tech Crime Emergency”.

Tra le attività investigative condotte, in tale ambito, si segnalano **155**indagini avviate nel **2019**per un totale di **117** persone indagate**.**

Tra le attività più significative si segnalano:

- **Operazione EXODUS**, ove il CNAIPIC, unitamente al Ros dei Carabinieri ed al Nucleo Speciale Tutela Frodi Tecnologiche della Guardia di Finanza, ha portato a termine una vasta operazione che ha consentito di acquisire elementi indiziari circa l’architettura e i criteri di gestione di quella sofisticata infrastruttura informatica atti a fondare il decreto di sequestro preventivo della medesima infrastruttura e delle aziende di E-Surv s.r.l. e STM s.r.l..

I dati intercettati dalla piattaforma informatica Exodus, fino a qualche mese fa utilizzata da diversi uffici inquirenti italiani, finivano tutti nei cloud di Amazon. Il pool cybercrime della Procura di Napoli (coordinato dal Procuratore Capo Giovanni Melillo e dal Procuratore Aggiunto Vincenzo Piscitelli) ha chiesto e ottenuto l’arresto di due persone, per le quali è stata disposta la misura cautelare degli arresti domiciliari.

Tali misure sono state emesse dopo indagini innovative, praticamente uniche in Italia, che hanno visto impegnati esperti della Polizia Postale (Cnaipic), dei Carabinieri del Ros e del Nucleo speciale tutela frodi tecnologiche della Guardia di Finanza.

Le forze dell’ordine hanno eseguito numerose perquisizioni e sequestrato decine di dispositivi informatici nelle sedi di alcune società (Ips spa, RPC spa, Innova spa e Rifatech srl) per conto delle quali la E-surv operava in subappalto ovvero quale fornitrice.

- **Operazione LUX**, nella quale il CNAIPIC nell’ambito di una lunga ed articolata attività di indagine ha dato esecuzione, con l’ausilio di personale del Compartimento Polizia Postale e delle Comunicazioni di Roma, alle perquisizioni locali e personali eseguite nei confronti di 9 persone, che in concorso tra loro avevano messo i piedi una complessa ed articolata attività criminale.

Al vertice del sistema 2 dipendenti infedeli di ACEA, oltre ad alcuni tecnici della municipalizzata ed elettricisti specializzati. Contestati agli indagati, a vario titolo, i reati di corruzione e frode.

Nel corso delle attività, svolte grazie alla collaborazione di ACEA e l’importante apporto della Protezione Aziendale e dei tecnici verificatori dell’azienda capitolina, è stato dato seguito inoltre a diversi provvedimenti di sequestro, con i quali sono stati assicurati altrettanti contatori manomessi dal sodalizio criminale, nell’ambito dei servizi offerti ai “clienti”, nella quasi totalità dei casi esercizi commerciali (bar, ristoranti, supermercati), i cui titolari sono stati denunciati per corruzione e frode.

L’indagine ha fatto ulteriormente emergere che diversi indagati fruivano a loro volta dei sistemi alterati, lucrando, in danno della municipalizzata capitolina fino al 75 % dell’effettivo consumo, fruendo di allacci totalmente abusivi alla rete di distribuzione elettrica.

- **Operazione People1,**nella quale il CNAIPIC ha portato a termine una delle più articolate attività di indagine nel contrasto agli attacchi cibernetici verso banche dati istituzionali.

Centinaia di credenziali di accesso a dati sensibili, migliaia di informazioni private contenute in archivi informatici della pubblica amministrazione relativi a posizioni anagrafiche, contributive, di previdenza sociale e dati amministrativi appartenenti a migliaia di cittadini e imprese del nostro Paese venivano massivamente sottratte da un pericoloso gruppo criminale. Questo quanto è stato scoperto dagli investigatori specializzati del Servizio Polizia Postale e delle Comunicazioni, che hanno dato esecuzione ad un’ordinanza di custodia cautelare in carcere e proceduto ad eseguire 6 decreti di perquisizione sul territorio nazionale; destinatarie anche diverse agenzie investigative.

I numerosi indizi raccolti durante le indagini indicano il soggetto a capo del “sistema” come il principale responsabile di ripetuti attacchi ai sistemi informatici di numerose Amministrazioni centrali e periferiche italiane, attraverso i quali sarebbe riuscito ad intercettare illecitamente centinaia di credenziali di autenticazione (userID e password).

L’indagato è riuscito così ad introdursi in banche dati di rilievo istituzionale, appartenenti ad esempio all’**Agenzia delle Entrate, INPS, ACI ed Infocamere**, veri obiettivi finali dell’attività delittuosa, da questi esfiltrando preziosi dati personali di ignari cittadini ed imprese italiane.

Denunciati a piede libero per le medesime violazioni, **6 complici**dell’arrestato, tutti a vario titolo impiegati all’interno di note agenzie investigative e di recupero crediti operanti in varie città d’Italia.

Per l’esecuzione dei provvedimenti restrittivi e di perquisizione, oltre che per l’espletamento della preliminare attività informativa, il CNAIPIC si è avvalso della collaborazione del personale dei Compartimenti di Polizia Postale di Roma, Milano, Napoli, Venezia, Genova e della Sezione di Imperia.

Nell’ottica di un’efficace condivisione operativa,il Centro ha proseguito la stipula di specifici Protocolli a tutela delle infrastrutture critiche nazionali: al riguardo, nel 2019 sono **state sottoscritte 7 nuove convenzioni** con le società **Alitalia, Istituto Poligrafico Zecca dello Stato, Cassa Depositi e Prestiti, E.ON, Assaeroporti, Fastweb ed Italgas,**oltre al rinnovo delle convenzioni in essere con **CONSOB**, **Dipartimento della Protezione Civile e Vodafone**.

Si rappresenta, altresì, che analoghe forme di collaborazione, nell’ambito del progetto SINC3, sono state avviate dagli uffici territoriali della Specialità con strutture sensibili di rilevanza locale, sia pubbliche che private, al fine di garantire un sistema di sicurezza informatica capillare e coordinato.

CYBERTERRORISMO

Nell’ambito della prevenzione e del contrasto al terrorismo internazionale di matrice jihadista ed, in particolare, ai fenomeni di radicalizzazione sul web, il personale della Polizia Postale e delle Comunicazioni effettua quotidianamente il monitoraggio del web, affiancato da qualificati mediatori linguistici e culturali, il cui contributo, per la peculiarità della materia e dei relativi contenuti multimediali presenti sulla rete, fornisce un valore aggiunto di fondamentale importanza.

Come noto, infatti, il web assurge ad un ruolo fondamentale quale strumento strategico di propaganda dell’ideologia del *Daesh*, di reclutamento di nuovi combattenti, di finanziamento, di scambio di comunicazioni riservate nella pianificazione degli attentati e di rivendicazione degli stessi.

In tale contesto, la Specialità ha svolto attività sia di iniziativa, che su specifica segnalazione, anche grazie alle informazioni pervenute dai cittadini tramite il Commissariato di P.S. Online, al fine di individuare i contenuti illeciti presenti all'interno degli spazi e servizi di comunicazione *online*di ogni genere, come, ad esempio, siti, weblog, forum, board, social network e gruppi chiusi presenti su piattaforme di comunicazione.

L'attività, funzionale al contrasto dei fenomeni di radicalizzazione e cyberterrorismo, ha portato al monitoraggio di oltre **32.170**spazi web ed alla rimozione di centinaia di contenuti.

Appare opportuno evidenziare come l'attività di monitoraggio del web effettuata negli ultimi mesi da questa Specialità abbia permesso di riscontrare come l'attuale struttura centrale dell'apparato di propaganda del *Daesh*, con produzione mediatica più o meno costante nel tempo, risulti essere costituita da vari *Media Center*insistenti nelle province del Califfato che, mentre in passato risultavano dotati di canali di comunicazione propri, oggi si appoggiano ai c.d. *Supporter Generated Content* per la diffusione del materiale di propaganda.

Si tratta, dunque, di una struttura basata su una miriade di *account*, attivati quotidianamente da singoli *cyber mujahid*(supporter del Califfato sui media) o in forma automatizzata tramite apposite strutture dipendenti dal *Daesh*e deputate al mantenimento dell'operatività mediatica, per fare fronte all'azione restrittiva messa in atto dagli amministratori delle piattaforme Social, con l'obiettivo di divulgare *magazine online*del Califfato, aggiornamenti sulle attività dei combattenti nei teatri operativi, video, documenti, manuali o pubblicazioni di esponenti di spicco della corrente radicale islamica, infografiche di minaccia etc.

Al fine di contrastare tale strategia di comunicazione dell'IS, personale del Servizio Polizia Postale e delle Comunicazioni ha partecipato agli "Action Day" che si sono svolti nel mese di novembre 2019 presso la sede di Europol, a L'Aia, e che hanno coinvolto, oltre a tutte le Forze dell'Ordine degli Stati Membri, anche i rappresentanti dei maggiori *Internet Service Provider*, tra cui *Telegram* –che è stato il fornitore di servizi online che ha ricevuto la maggior parte delle richieste di *referral*e che ha allontanato dalla propria piattaforma una parte significativa degli attori chiave all'interno della rete di diffusione della propaganda IS – nonché *Google, Files.fm, Twitter, Instagram*e*Dropbox*.

In tale contesto, dunque, le attività poste in essere hanno permesso di ottenere un massiccio "*take down*" di migliaia di gruppi, canali ed*account*(molti dei quali oggetto di un precedente accesso abusivo ed un successivo impiego come *bots*) che sono stati oggetto di preventiva segnalazione da parte del *law enforcement*, in quanto considerati responsabili della pubblicazione del settimanale di settore *al-Naba*.

Nella medesima circostanza, inoltre, mediante un rilevante lavoro di monitoraggio e *Open Source Intelligence,* si è provveduto all'analisi dei tentativi di reazione da parte dei *cyber mujahid*, ed all'immediato contrasto delle prove di ricostruzione della macchina di propaganda *online* dell'IS.

Appare evidente, dunque, come il carattere transnazionale delle operazioni descritte, sia per la natura internazionale del fenomeno, che per la stessa connaturata struttura della rete, determini l'imprescindibile attivazione efficiente di strumenti di cooperazione sovranazionale che riescono ad apportare un indiscusso valore aggiunto alle attività di prevenzione messe in atto dalle diverse Forze di Polizia nazionali.

Ad ulteriore conferma della proiezione internazionale del Servizio Polizia Postale e delle Comunicazioni, quale punto di contatto nazionale dell'*Internet Referral Unit*(IRU) di Europol (Unità preposta a ricevere dai Paesi Membri le segnalazioni relative ai contenuti di propaganda jihadista diffusi in rete e di orientarne l'attività), appare opportuno segnalare la partecipazione di propri

operatori anche al “CBRNE Action Day”, che si sono svolti sempre presso la sede di Europol alla fine del mese di novembre.

Nel dettaglio, partendo dall’analisi dei tragici eventi terroristici avvenuti negli ultimi anni in Europa, a partire dall’attacco alla Manchester Arena del 22 maggio 2017 per arrivare fino ai recente episodio di Halle (Germania) dello scorso 9 ottobre, si è constatato come sempre più spesso i **lupi solitari**(sia di matrice jihadista, così come di matrice neonazista) abbiano fatto ricorso ad esplosivi e armamenti realizzati seguendo le istruzioni presenti in manuali e linee guida pubblicate online.

Nel corso “CBRNE Action Day” l’operazione congiunta è stata rivolta proprio alla individuazione *online* di manualistica e di c.d. “*Tutorials*” di stampo terroristico, nei quali viene spiegato come preparare ordigni esplosivi improvvisati utilizzando materiali radiologici, biologici, chimici e nucleari.

Nel dettaglio, durante l’operazione le forze di polizia hanno identificato oltre 1700 risorse online di interesse investigativo che sono state segnalate ai *Provider*dei Servizi Internet per la relativa rimozione e per l’ottenimento di utili elementi di prova indispensabili per la prosecuzione delle indagini.

L’operazione congiunta ha altresì compreso ulteriori attività investigative, anche all’interno del *Dark Web,*al fine di individuare operazioni di compravendita di materiali necessari alla preparazione di ordigni, con la successiva analisi delle transazioni sospette relative alla vendita di precursori chimici su piattaforme *online* generiche.

Sempre nell’ambito della lotta al terrorismo di matrice jihadista, appare opportuno segnalare anche le attività d’indagine svolta dal personale del Compartimento Polizia Postale e delle Comunicazioni “Emilia Romagna” di Bologna, all’esito delle quali la Procura della Repubblica di Bologna ha emesso un decreto di perquisizione locale, personale e informatica nei confronti di un cittadino tunisino di 24 anni.

Le indagini, scaturite dall’attività posta in essere da operatori sotto copertura della Specialità in materia di contrasto al cyber terrorismo, hanno condotto all’individuazione di un account Whatsapp, riconducibile all’indagato, inserito all’interno di gruppi di esplicito sostegno alle ideologie dello Stato Islamico.

In relazione a tali fatti, la Procura della Repubblica di Bologna ha iscritto a carico del cittadino tunisino le ipotesi di reato di apologia di reato in ordine ai delitti di “Terrorismo e crimini contro l’umanità” commessi a mezzo di strumenti telematici.

Ed ancora, all’esito della perquisizione sono stati rinvenuti oltre ad alcuni smartphone, uno dei quali conteneva l’utenza telefonica associata all’account *WhatsApp* ed ai diversi canali *Telegram*utilizzati per la diffusione della propaganda jihadista, anche apparati informatici nei quali era presente materiale multimediale avente il medesimo tenore, nonché alcuni manoscritti in lingua araba inneggianti lo Stato Islamico.

Nell’anno che volge al termine, oltre alle suindicate attività di polizia giudiziaria connesse al terrorismo di matrice jihadista, la Polizia Postale e delle Comunicazioni ha registrato un notevole incremento delle attività nel settore della propaganda online legata all’estremismo razzista e xenofobo, riscontrando un trend di forum e discussioni dedicate all’argomento in costante aumento.

Tale tendenza, che ha coinvolto la popolazione “virtuale” di tutto il globo, evidenzia una dimensione transnazionale della minaccia in argomento, basti pensare alla strage di Christchurch – avvenuta il 15 marzo 2019 – nella quale hanno perso la vita 50 persone (mentre altre 50 sono state ferite) in seguito all’attacco da parte di un uomo che, motivato da ideologie suprematiste, ha aperto il fuoco su

due luoghi di culto musulmani nella terza città più grande della Nuova Zelanda, trasmettendo le immagini in diretta su Facebook.

L'indottrinamento, come nel caso del radicalismo jihadista, avviene anche in questo ambito quasi sempre sulla rete, attraverso una graduale autoformazione che inizia con la visualizzazione di contenuti diffusioni di numerose *board*, diverse dai principali *social network*.

All'interno di tali *board*, inoltre, trovano ampio spazio anche messaggi pubblicati ad opera di ignoti mediante i quali vengono minacciate azioni terroristiche (nella maggior parte dei casi rivelatesi fake).

Sul punto, inoltre, appare opportuno evidenziare come, grazie alla buona collaborazione con il *Federal Bureau of Investigation*, operatori della Sezione Cyberterrorismo del Servizio Polizia Postale e delle Comunicazioni, hanno indentificato un soggetto italiano che, tramite la piattaforma 4Chan aveva minacciato l'esecuzione in data 30 agosto 2019 di un'azione terroristica sulla tratta ferroviaria Roma/Milano; in particolare, gli investigatori riuscivano ad effettuare la perquisizione nei confronti del reale autore del messaggio in data 29 agosto 2019, accertando l'inconsistenza della minaccia.

Ed ancora, nell'anno in corso, grazie alla collaborazione dei Compartimenti di Firenze e Perugia, sono stati identificati ed indagati due soggetti che, rispettivamente, risultavano essere gli autori di un messaggio *online*con il quale veniva minacciato un omicidio di massa a New York per il giorno 26 novembre p.v., e di un messaggio in cui l'autore avrebbe affermato che il giorno dopo sarebbe diventato un killer ed aggiungendo che l'eccidio di Columbine – massacro avvenuto il 20.4.99 presso la Columbine High School negli USA, dove vennero uccisi molti studenti– al confronto sarebbe sembrato uno scherzo.

Inoltre, al fine di contrastare la presenza sul territorio italiano di gruppi aventi tra i propri scopi l'incitamento alla discriminazione o alla violenza per motivi razziali, etnici e nazionali, il personale della Polizia Postale e delle Comunicazioni ha collaborato con gli Uffici della Polizia di Prevenzione per l'esecuzione di perquisizioni informatiche nei confronti di oltre **28 soggetti**dislocati sul territorio nazionale.

In seguito a tale evidente innalzamento del rischio, si è assistito ad un parallelo incremento del livello di attenzione anche nei tavoli di lavoro internazionali, e, proprio in seno all'*E.U. Internet Forum*, personale del Servizio Polizia Postale e delle Comunicazioni ha contribuito – unitamente a rappresentanti degli Stati Membri e di Europol, nonché di alcuni delegati delle maggiori compagnie fornitrici di servizi internet (tra le quali Facebook, Google, Microsoft, Telegram, Twitter, Snap, JustPaste.it e Dropbox) – all'elaborazione di un protocollo di crisi dell'Unione Europea finalizzato al contrasto ed al contenimento della rapida diffusione virale di contenuti terroristici e di estremismo violento online.

FINANCIAL CYBERCRIME

Con riferimento al **financial cybercrime,**le statistiche dell'anno in corso fanno registrare ben **4930 casi** a livello nazionale.

Il fenomeno del phishing, finalizzato alla captazione illecita di codici personali e dati sensibili, conosce un notevole aumento soprattutto attraverso il ricorso a malware e siti-clone. In aumento, tuttavia, sono anche i casi riguardanti il cd. "Vishing" (phishing vocale) e "Smishing" (phishing attraverso messaggi ed sms).

La violazione dei sistemi bancari di privati ed imprese vede un aumento nel ricorso alle tecniche criminali del cd. Sim-Swap (vedi *infra*).

Il tessuto economico-produttivo del Paese continua ad essere oggetto degli attacchi noti a livello mondiale con le espressioni BEC e CEO Fraud. Scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando ingenti somme verso conti correnti nella disponibilità dei truffatori. Il BEC (business e-mail compromise) fraud o CEO (Chief Exeutive Officer) fraud sono la moderna applicazione della tecnica di attacco denominata "man in the middle".

Nonostante la difficoltà operativa di bloccare e recuperare le somme provento di frode informatica, soprattutto perché inviate 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, nell'anno 2019, la Specialità ha potuto bloccare e recuperare alla fonte, su una movimentazione di **18.763.446 €,** ben **13.544.042 €.**

La piattaforma in questione, frutto di specifiche convenzioni intercorse mediante **ABI**con gran parte del mondo bancario, consente di intervenire in tempo quasi reale sulla segnalazione, bloccando la somma prima che venga polverizzata in vari rivoli di prestanome.

Al riguardo, con riferimento al fenomeno del **cyber-riciclaggio**, di rilievo è la recente operazione internazionale denominata "**Emma5"**, coordinata dal Servizio Polizia Postale con la collaborazione di **24 Paesi**Europei e di Europol, volta a identificare i c.d. "money mules", primi destinatari delle somme provenienti da frodi informatiche e campagne di phishing, che offrono la propria identità per l'apertura di conti correnti e/o carte di credito, sui quali vengono poi accreditate le somme illecitamente acquisite.

L'operazione in parola ha consentito sul territorio nazionale di identificare e denunciare **170 *money mules*.**

Le transazioni fraudolente sono state **374**, per un totale di circa **10 milioni di euro,**di cui**circa 3.5 milioni euro**sono stati bloccati e/o recuperati grazie alla piattaforma per la condivisione delle informazioni denominata "OF2CEN", realizzata appositamente al fine di prevenire e contrastare le aggressioni criminali ai servizi di home banking e monetica.

Di seguito, un dettaglio delle **operazioni più significative**portate a termine dalla Specialità nel corso del 2019.

1) **Nel settore del BEC e CEO Fraud**si segnala un'operazione eseguita dalla Polizia Postale di Napoli e di Torino, coordinata dal Servizio centrale, ai danni di un'azienda campana operante nel settore della commercializzazione di gas industriale, per un importo di **€ 236.000,00**, trasferito dal conto corrente della vittima a saldo di una fattura commerciale, ad un diverso conto, in uso ai cyber criminali che si erano sostituiti al reale partner d'affari.

I complessi accertamenti tecnologici e finanziari compiuti dalla Polizia Postale hanno condotto gli investigatori ad una filiale di Poste Italiane di Torino, ove risultava aperto un conto corrente a nome di un cittadino nigeriano, residente nel capoluogo piemontese.

Da lì, il denaro era stato poi trasferito immediatamente dai frodatori su un conto intestato allo stesso cittadino nigeriano, ed ancora su una diversa carta di pagamento riconducibile ad una donna, anch'essa di nazionalità nigeriana e residente a Torino.

Immediatamente dopo aver ricevuto la denuncia, la Polizia Postale di Napoli ha posto sotto sequestro tutti i citati conti correnti, riuscendo a recuperare gran parte della somma sottratta dai truffatori.

Successivamente, al termine delle indagini, sono stati prontamente attivati i colleghi della Polizia Postale di Torino, luogo in cui le tracce conducevano, i quali hanno eseguito una perquisizione nei

confronti dei due cittadini nigeriani, rinvenendo in loro possesso tutti i conti correnti strumento del riciclaggio del denaro provento del reato.

Una ulteriore operazione,eseguita dalla Polizia Postale di Torino, ha condotto all'arresto di due uomini, autori di due distinti episodi di reato, recuperando complessivamente oltre **380 mila euro**di profitti illeciti.

Al termine di una articolata indagine fatta di ricostruzione delle tracce informatiche, pedinamenti ed analisi dei dati, gli investigatori della Specialità hanno individuato i responsabili delle frodi, il primo, un liberiano di 43 anni, presso uno sportello bancario di Settimo Torinese, colto nel tentativo di dirottare verso altri conti correnti la ragguardevole somma di **370.000,00 euro,**che aveva incassato appena il giorno prima come frutto di una frode BEC perpetrata ai danni di un'azienda del Comasco, la quale avrebbe dovuto ricevere tale denaro come pagamento di una importante fornitura di arredamenti per un cliente statunitense; l'uomo, arrestato, è stato infine sottoposto alla misura dell'obbligo di dimora su disposizione del GIP.

Stessa sorte è toccata ad un cittadino nigeriano, bloccato mentre era intento a prelevare **4.000€**dal proprio conto corrente. L'arrestato con precedenti per reati specifici, è stato tratto in arresto.

Anche il mondo dello Sport è finito nelle spire di tale tipologia di frode online. La **FITET, Federazione Italiana Tennis Tavolo** , è stata infatti attirata nel sinistro meccanismo delle frodi informatiche in occasione di un torneo internazionale, che vedeva la partecipazione di ben quaranta Paesi da tutto il mondo, nel quale l'Italia avrebbe preso parte.

Mentre erano in corso gli ultimi preparativi per l'organizzazione della trasferta della Squadra azzurra, due soggetti italiani, abili hacker, si sono introdotti clandestinamente nella rete della Federazione italiana, rubando le credenziali di accesso alle caselle di posta elettronica federali, e riuscendo in tal modo ad intercettare tutte le comunicazioni scambiate fra le varie società sportive.

A finire sotto la lente degli hacker sono state, in particolare le email contenenti i dati e gli estremi per procedere ai pagamenti per la partecipazione al prestigioso torneo.

Carpiti tali dati infatti, i criminali informatici sono riusciti a rubare l'identità digitale degli organizzatori del torneo, ed abilmente falsificando tutte le fatture relative ai pagamenti per l'iscrizione, hanno contattato le varie Federazioni sportive e squadre partecipanti (tra cui, oltre l'Italia, vi erano la Cina, la Polonia e l'Ungheria), convincendole della necessità di effettuare i pagamenti su conti correnti del tutto falsi, accesi presso banche estere ed in realtà riconducibili ai due italiani, i quali, nel giro di pochissimi click, avevano già incassato oltre **30.000 euro** di profitti illeciti.

Attraverso attività tecniche e complessi accertamenti informatici, superando gli strumenti di anonimizzazione che gli hacker avevano impiegato per camuffare le loro tracce, gli uomini della Polizia Postale hanno in breve tempo puntato l'obiettivo sui due italiani, ufficialmente residenti a Sanremo; pedinati e rintracciati a Torino, i due sono stati sottoposti a perquisizione, anche informatica, che ha consentito di ricostruire tutte le prove del reato all'interno del copioso materiale hardware e software in loro possesso, poi sottoposto a sequestro.

2) **Nel settore del phishing**teso alla illecita captazione di codici bancari, si segnala un'operazione eseguita dalla Polizia Postale di Salerno, con il coordinamento del Servizio centrale, la quale ha condotto all'arresto di un abile truffatore informatico, che, in pochissimo tempo, gli aveva permesso di appropriarsi di quasi 200 mila euro sottratti dai conti delle ignare vittime.

L'uomo, un italiano di 66 anni residente a Scafati, agiva secondo un modus operandi particolarmente insidioso.

A monte vi era l'utilizzo abusivo di credenziali informatiche di carte di credito e conti correnti delle ignare vittime. L'attività di reperimento delle credenziali e dei dati personali degli utenti, come noto, è purtroppo resa oggi possibile grazie all'utilizzo di molteplici e sofisticate tecniche criminali: si va dal phishing massivo, attuato mediante l'invio di email con allegati contenenti virus, al phishing attuato mediante falsi siti internet sui quali l'utente è invitato, con l'inganno, a cedere i propri dati, alle attività di hacking dirette verso i sistemi informatici con lo scopo di esfiltrare pacchetti di migliaia di dati personali di cittadini e imprese – poi rivenduti sui mercati neri del darkweb - sino alle più "tradizionali" ma sempre attuali clonazioni delle carte di pagamento.

Acquisito il prezioso patrimonio di credenziali di accesso e dati bancari, il pericoloso frodatore accedeva abusivamente all'interno dei sistemi di pagamento online delle vittime, facendo partire dai loro conti diversi ordini di pagamento, attraverso bollettini postali online. Gli ordini di pagamento, in particolare, originavano da account che il frodatore aveva aperto a nome di ulteriori ignari cittadini, vittime di furto di identità digitale.

Per ostacolare ulteriormente la ricostruzione delle tracce, i pagamenti apparivano formalmente intestati ad ulteriori cittadini, anch'essi del tutto estranei alla truffa.

Dal conto del criminale, poi, il denaro aveva già iniziato ad essere ulteriormente spacchettato, su conti correnti in Italia e all'estero, in attività di cyber-riciclaggio.

3) **Nel settore della violazione dei sistemi di home-banking**di privati ed imprese, è soprattutto la frode nota con il termine "Sim-swap" ad aver caratterizzato le attività investigative dell'anno in corso.

14 arresti sono stati compiuti dalla Polizia Postale e delle Comunicazioni di Messina, Palermo e Reggio Calabria, con il coordinamento del Servizio centrale, nel corso dell'**Operazione Sim-swap.**

La SWAP SIMè una avanzata tipologia di frode informatica articolata in vari passaggi. Una volta individuata la vittima si procede alla acquisizione dei suoi dati e delle credenziali di home banking tramite tecniche di hacking ovvero di ingegneria sociale; successivamente, utilizzando documenti falsificati ad hoc, si sostituisce la sim card della vittima e, attraverso lo stesso numero telefonico, si ottengono dalla banca le credenziali per operare sul conto corrente on-line.

Nel caso specifico, carpiti i dati anagrafici e il numero di telefono della vittima, nonché i dati dei conti correnti e le relative credenziali di accesso, gli indagati, utilizzando un falso documento di identità intestato alla vittima, si recavano presso un dealer al fine di chiedere la sostituzione della SIM in uso alla persona offesa. La scheda SIM del titolare veniva allora disabilitata in quanto sostituita da quella attivata fraudolentemente. La vittima rilevava il mancato funzionamento della sua SIM ma, generalmente, non associava immediatamente l'evento ad una frode in corso.

Sostituita la SIM, gli autori del reato penetravano nel sistema informatico dell'istituto di credito presso cui la vittima aveva acceso il conto corrente, riuscendo il più delle volte a reimpostare le credenziali di accesso attraverso una telefonata all'assistenza clienti, presentandosi come il titolare del conto e rispondendo alle varie domande di sicurezza. Una volta effettuato l'accesso, gli indagati erano abilitati ad operare sul conto corrente on-line della vittima, disponendo bonifici e/o ricariche di carte prepagate in favore di altri conti correnti e/o carte prepagate nella loro disponibilità, in quanto appositamente accesi da complici e prestanome, così ostacolando l'identificazione della provenienza delittuosa delle somme.

Nel corso delle attività d'indagine e di osservazione delle attività del sodalizio criminale, grazie all'intervento degli operatori della Polizia Postale, sono state bloccate numerose frodi, alcune delle quali per importi pari a decine di migliaia di euro.

Un’altra rilevante operazioneha avuto ad oggetto l’insidiosa variante vocale del phishing, il cosiddetto “**Vishing**”.

Con **l’Operazione Double-Vishing**, la Polizia Postale e delle Comunicazioni ha eseguito 6 misure cautelari a carico di una organizzazione criminale, residente nell’hinterland napoletano ma operativa su tutto il territorio nazionale, i cui appartenenti sono indagati per i reati di associazione per delinquere finalizzata alla sostituzione di persona, al furto aggravato e all’indebito utilizzo di carte di pagamento elettronico.

L’organizzazione criminale procedeva secondo un complesso modus operandi che vedeva i sodali divisi in compiti specifici e ben delineati. Il primo passo consisteva nell’effettuare i furti della corrispondenza nei centri di smistamento di Poste Italiane nel Centro-Nord Italia.

All’interno di questi centri di raccolta della corrispondenza, nottetempo parte della banda, con maestria consolidata, individuava i dispacci contenenti le carte di credito e/o debito spediti da parte degli istituti di credito. Impossessatisi dei preziosi titoli, entrava in gioco un esperto gruppo di “telefonisti” che metteva in atto la tecnica del Vishing (Neologismo anglosassone ottenuto dalla crasi tra le parole voice + phishing).

Il gruppo dei “telefonisti” chiamava i vari Istituti emittenti delle carte e, presentandosi come Maresciallo o Ispettore delle Forze dell’ordine, affermava di aver appena sequestrato un consistente numero di carte di credito rinvenute in possesso a malviventi. Con fare perentorio e con la scusa di riconsegnare i titoli in sequestro, si faceva indicare il numero di telefono dei clienti.

A questa seguiva una complessa attività di Social Engineering compiuta da esperti tecnici che provvedevano a reperire tutte le informazioni e gli ulteriori dati necessari. Una volta ottenuti i dati, l’organizzazione rivolgeva la sua abilità criminale proprio verso i clienti ai quali, spacciandosi per dipendenti della banca, paventava problemi connessi nell’attivazione del titolo riuscendo infine, con abilità persuasive, a farsi indicare il PIN dei titoli.

L’associazione per delinquere, disponeva di un proprio “apparato tecnico-finanziario” che si occupava di dotare gli associati di conti correnti e carte prepagate con funzioni on-line. I criminali potevano così monetizzare i proventi degli indebiti utilizzi che, prelevati per contanti su sportelli ATM, poi confluivano su strumenti prepagati riciclando consistenti somme di denaro su carte di credito in possesso dei vari “money mules” gestiti dal gruppo.

Il profitto illecito di detta attività ha portato nelle casse dell’organizzazione criminale più di un milione di euro. Le carte interessate dalle frodi sono centinaia.

4) **Nel settore del contrasto alla pirateria informatica**ragguardevoli successi sono stati ottenuti nell’anno in corso dalla Specialità.

A livello nazionale, con l’Operazione Eclissi, il Servizio Polizia Postale ha messo a segno la più vasta operazione di polizia mai condotta nel settore del contrasto al fenomeno delle IPTV illegali. L’Operazione coordinata a livello nazionale dalla Procura della Repubblica di Roma, e a livello internazionale dalle Agenzie europee Eurojust ed Europol ha puntato a disarticolare direttamente la complessa infrastruttura tecnologica operante a livello internazionale, responsabile della diffusione via Internet, attraverso numerosi siti, del segnale illegalmente captato di numerose emittenti televisive a pagamento (Sky; DAZN; Mediaset; Netflix etc.).

Un’indagine tecnico informatica estremamente accurata sulla diffusione dei segnali in streaming effettuato dal Servizio Polizia Postale e delle Comunicazioni ha consentito di individuare le sorgenti estere dalle quali partiva il segnale **“pirata**”.

Potentissimi Server allocati all'estero consentivano la diffusione capillare in tutta Europa del segnale, al punto che le risultanze operative hanno coinvolto le Autorità giudiziarie e le Polizie di Francia; Paesi Bassi; Germania; Bulgaria e Grecia.

Significativi i numeri complessivi relativi sia alle persone coinvolte, circa 5.000.000 di utenti solo in Italia; sia alle **Iptv bloccate 30**, per un volume di affari stimato di oltre 2 milioni di euro al mese, che hanno portato all'individuazione di circa 200 tra conti PayPal, postepay, conti correnti bancari e wallet bit coin, tuttora oggetto di indagine. Inoltre sono stati sequestrati oltre 200 Server e 80 domini e sono state effettuate 20 perquisizioni in tutta Europa presso sedi di società e provider.

A livello locale, una seconda operazioneè stata portata a termine dalla Polizia Postale in Palermo, giungendo alla identificazione dei gestori della nota IPTV pirata "ZSAT", e disarticolando l'infrastruttura informatica che permetteva la riproduzione abusiva, attraverso internet, dell'intero palinsesto Sky.

Al termine di articolate indagini poste in essere dalla Polizia Postale e delle Comunicazioni di Palermo e dalla Procura del capoluogo siciliano, il cerchio si è stretto intorno ad un cittadino palermitano di 35 anni, la cui abitazione è stata individuata e sottoposta ad attenta perquisizione.

Nella stanza da letto dell'indagato, è stata puntualmente rinvenuta la "Sorgente" dell'IPTV pirata ZSAT, composta da 57 decoder di Sky Italia, collegati ad apparati per la ritrasmissione sulla rete internet, per un giro di clienti finali stimato in circa 11.000 persone in tutta Italia.

Proprio a riprova dell'entità del giro di affari illecito, presso la sola abitazione dell'indagato gli uomini della sezione financial cybercrime della polizia postale hanno rinvenuto e sequestrato, nascosti negli scarichi dei bagni e nella spazzatura, ben 186.900 euro in contanti ed una macchina professionale conta-banconote, lingotti d'oro, e due "wallet" hardware (portafogli virtuali) contenenti cryptomoneta in diverse valute, il cui valore complessivo, certamente elevato, verrà meglio stimato a seguito degli ulteriori accertamenti tecnici.

Quello dell'**IPTV illegale**è un mondo criminale complesso ed assai insidioso, gestito dalla criminalità organizzata nazionale ed estera, della cui dimensione e pericolosità non sempre chi le utilizza è avveduto e la cui dimensione criminale effettiva è dettata soprattutto dall'utilizzo dei proventi verso diversificate modalità criminali direttamente lesive degli interessi dei cittadini.

Nel sentire comune si ritiene che in fondo fruire di un sistema pirata non è un crimine, al massimo si sottraggono pochi soldi ad un colosso della comunicazione. Ma se si guarda il fenomeno nella sua complessità, e non solo nel singolo utilizzo, ci si rende conto che nella realtà un intero sistema produttivo può essere messo in crisi. Le più recenti stime parlano infatti di danni per più di **800 milioni di euro.**

ATTIVITA' DI PREVENZIONE

Parallelamente all'incremento dell'uso di strumenti telematici, sono cresciute le aspettative di sicurezza da parte del cittadino.

La Polizia Postale e delle Comunicazioni è impegnata, ormai da diversi anni, in campagne di sensibilizzazione e prevenzione sui rischi e pericoli connessi all'utilizzo della rete internet, rivolte soprattutto alle giovani generazioni.

Nello specifico si evidenzia la settima edizione della campagna itinerante della Polizia Postale e delle Comunicazioni "***Una Vita da Social***", grazie alla quale sino ad oggi sono stati incontrati oltre **2 milioni di studenti**, **220.000 genitori, 125.000 insegnanti** per un totale di **17.000 Istituti scolastici**

e **300** città italiane.

Un progetto dinamico, innovativo e decisamente al passo con i tempi, che si avvicina alle nuove generazioni evidenziando sia le opportunità del web che i rischi di cadere nelle tante trappole dei predatori della rete, confezionando un vero e proprio “manuale d’uso”, finalizzato ad evitare il dilagante fenomeno del cyberbullismo e tutte quelle forme di uso distorto della rete in generale e dei social network.

A disposizione degli utenti è presente la pagina **facebook e twitter**di “Una vita da social”, gestita direttamente dalla Polizia Postale e delle Comunicazioni, dove vengono pubblicati gli appuntamenti, le attività, i contributi e dove i giovani internauti possono “*postare*” direttamente le loro impressioni ad ogni appuntamento.

Grande consenso ha riscosso la campagna **#cuoriconnessi**, che ha coinvolto migliaia di studenti, attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online.

Inoltre nel corso dell’anno sono stati realizzati incontri educativi su tutto il territorio nazionale raggiungendo oltre **300 mila studenti** e circa **3000 Istituti scolastici**per i quali è stata messa a disposizione anche un’email dedicata: progettoscuola.poliziapostale@interno.it.

COMMISSARIATO DI PS ONLINE

Il portale del Commissariato di P.S. online è divenuto il punto di riferimento specializzato per chi cerca informazioni, consigli, suggerimenti di carattere generale, o vuole scaricare modulistica e presentare denunce.

Uno strumento agevole che consente al cittadino, da casa, dal posto di lavoro o da qualsiasi luogo si desideri, di entrare nel portale ed usufruire dei medesimi servizi di segnalazione, informazione e collaborazione che la Polizia Postale e delle Comunicazioni quotidianamente ed ininterrottamente offre agli utenti del web.

Di particolare importanza le denunce e le segnalazioni giunte anche sul sito del Commissariato di P.S. on-line per i reati di cyberbullismo, perpetrati soprattutto in ambito scolastico da parte di studenti nei confronti di compagni e perpetrati attraverso i social media, con atti denigratori e diffamatori nei confronti delle giovani vittime. Alcune attività sono sfociate nell’emissione da parte dei Questori di provvedimenti di ammonimento anche al fine di responsabilizzare minori autori del reato.

Attività del Commissariato di PS online

Richieste di informazioni evase

22.853

Segnalazioni ricevute dai cittadini

20.622

Denunce presentate dagli utenti

10.409

Attività di contrasto nell’ambito della Regione Calabria

Reati segnalati all’A.G. su denuncia o di iniziativa

729

di cui per truffe, frodi ed altri reati informatici

437

Perquisizioni personali e locali eseguite

61

Persone arrestate su ordinanza di custodia dell’A.G.

8

di cui per truffa – estorsione – reati contro il patrimonio

7

di cui per delitto di stalking art.612bis c.p.

1

Persone arrestate in flagranza di reato

1

di cui per detenzione di materiale pedopornografico

1

Persone denunciate in stato di libertà

74

di cui per reati di frode-truffa - reati informatici e contro il patrimonio

35