

Polizia di Stato

Polizia Postale: resoconto attività 2017.

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 2017 è stato costantemente indirizzato alla prevenzione e al contrasto della criminalità informatica in generale, con particolare riferimento ai reati che, anche a fronte della Direttiva del Ministro dell'Interno del 15 Agosto 2017, sono di precipua competenza di questa Specialità. Nell'ambito della **pedopornografia online** sono stati operati **55** arresti e **595** denunce; tra le operazioni più significative, coordinate dal Servizio Polizia Postale e delle Comunicazioni, si segnala l'operazione Sweep Web del Compartimento Polizia Postale e delle Comunicazioni di Firenze che ha condotto all'esecuzione di **45** perquisizioni e **3** arresti per pornografia minorile l'operazione Black Shadow, condotta dal Compartimento Polizia Postale e delle Comunicazioni di Trento, nell'ambito della quale sono state eseguite **37** perquisizioni e **10** arresti per detenzione e divulgazione di materiale pedopornografico. Dalle complesse operazioni di prevenzione, è scaturita una assidua attività di monitoraggio della rete che ha visto coinvolti ben **28560** siti internet, di cui **2077** inseriti in black list. Si conferma la rilevanza del fenomeno dell'adescamento di minori online che ha registrato **437** casi trattati che hanno portato alla denuncia di **158** soggetti e all'arresto di **19**. A tal proposito, significativa è stata l'attività denominata Bad Queen condotta dal Compartimento Polizia Postale di Trieste che ha portato al deferimento all'A.G. i **7** soggetti. Senza dimenticare le indagini avviate a seguito delle segnalazioni dei genitori come l'operazione "12 Apostoli" del Compartimento Polizia Postale di Catania, che ha arrestato **4** persone costituenti una associazione a delinquere finalizzata alla violenza sessuale aggravata ai danni di minori. Di rilievo è l'attività di collaborazione con organismi internazionali: sono stati elaborati circa **176** Report NCMEC dai quali sono scaturite importanti attività di indagine. Un sensibile aumento, rispetto al 2016, è ravvisabile in materia di reati informatici contro la persona (ad es. diffamazione, cyberstalking, trattamento illecito di dati personali, sostituzione di persona) per i quali sono state denunciate **917** persone e arrestate **8**. 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 2016, si è quasi quintuplicato sino a raggiungere **28522**. 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 da una costante attività di monitoraggio. In tale ambito, il Centro ha ulteriormente gestito monitoraggi della rete che hanno riguardato strutture sensibili di rilievo nazionale. Inoltre in particolare la Sala Operativa del Centro ha gestito: **1006** attacchi informatici nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale; **80** richieste di cooperazione nell'ambito del circuito "High Tech Crime Emergency". Tra le attività investigative condotte, in tale ambito, si segnalano **68** indagini avviate nel **2017** per un totale di **33** persone denunciate e l'arresto di **2**. Tra le attività più significative, si segnalano l'operazione "EyePyramid" a seguito della quale è stato fermato il sodalizio composto dai fratelli Occhionero, entrambi arrestati, che si dedicava allo spionaggio informatico politico-istituzionale ed industriale e l'operazione "Andromeda" a seguito della quale è stata smantellata una rete botnet, ovvero un insieme di computer infettati da virus informatici e utilizzati dagli hacker per compiere svariati reati in tutto il mondo. 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 2017 sono state sottoscritte 7 nuove convenzioni con il Gruppo Atlantia (con le società Aeroporti di Roma, Autostrade per l'Italia e Telepass), Lottomatica, Piaggio Aerospace, INAIL e A2A, oltre al rinnovo della convenzione in essere con Enel. Si rappresenta, altresì, che analoghe forme di collaborazione 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. Con riferimento al **financial cybercrime**, le sempre più evolute tecniche di **hackeraggio**, attraverso l'utilizzo di **malware** inoculati mediante tecniche di phishing, ampliano a dismisura i soggetti attaccati, soprattutto nell'ambito dei rapporti commerciali. Infatti lo scopo delle organizzazioni criminali è quello di intromettersi nei rapporti commerciali tra aziende dirottando le somme verso conti correnti nella disponibilità dei malviventi. Il BEC (business e-mail compromise) fraud o CEO (Chief Executive 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 frodate, 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 2017, la Specialità ha potuto bloccare alla fonte su una movimentazione di **22.052.527 €** ben **20.839.576 €** e di recuperare **862.000 €** della residuale parte relativa ai bonifici già disposti. 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, di rilievo è la recente operazione internazionale denominata "Emma3", coordinata dal Servizio Polizia Postale con la collaborazione di **21 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 di identificare **37 money mules** di cui **32 arrestati** e **5 denunciati**, nonché di bloccare oltre **150.000 €**. Il contrasto al fenomeno dei "money mules" nel corso dell'anno ha consentito di recuperare complessivamente circa **370.000 €** di **denunciare 122** individui e di **arrestarne 39**. Altra significativa attività di polizia giudiziaria l'operazione "Criptolocker" condotta dal Compartimento Polizia Postale e delle Comunicazioni di Catania che ha portato a individuare una associazione a delinquere di **7 persone, 4 delle quali arrestate**, con base operativa nel napoletano, che estorcevano denaro a imprenditori e professionisti in tutta Italia bloccando tutti i dati presenti all'interno dei pc delle vittime, criptandoli, ovvero colpendo le transazioni commerciali con attacchi cosiddetti *man in the middle*. Nel settore del **cyberterrorismo** gli investigatori della Polizia Postale e delle Comunicazioni hanno concorso con altri organi di Polizia e di intelligence alla prevenzione e al contrasto dei fenomeni di eversione e terrorismo, sia a livello nazionale che internazionale, posti in essere attraverso l'utilizzo di strumenti informatici e di comunicazione telematica. In tal senso spicca l'operazione antiterrorismo denominata "Da'Wa" condotta dai Compartimenti di Perugia e Milano che ha portato all'arresto di 4 persone, tre tunisini ed un marocchino, che facevano proselitismo sul web, e ha consentito di emettere tre provvedimenti di espulsione nei confronti di altrettanti individui. Nell'ultimo anno, la strategia mediatica messa in campo dalle organizzazioni terroristiche di matrice religiosa islamista ha indotto la Specialità a effettuare una costante attività di osservazione e analisi dei contenuti presenti in rete, coinvolgendo anche ulteriori strutture territoriali rispetto a quelle individuate nel 2016 al fine di individuare forme di proselitismo e segnali precoci di radicalizzazione. L'attività, funzionale a contrastare il proselitismo e prevenire fenomeni di radicalizzazione, ha portato a monitorare circa **17000** spazi web e alla rimozione di diversi contenuti. Con riferimento all'attività di monitoraggio del web per il contrasto al terrorismo di matrice islamica, giova evidenziare che gran parte dei contenuti illeciti pubblicati su internet vengono rimossi direttamente dai gestori delle principali piattaforme web i quali, grazie anche alla richiesta di maggiore collaborazione elaborata in numerose sedi istituzionali nell'ambito di progetti internazionali (es. EU Internet Forum) ai quali ha preso parte anche questa Specialità, stanno garantendo un'azione più incisiva per ridurre la proiezione esterna e virtuale del Califfato. Ancora, si rappresenta, che il Servizio di Polizia Postale e delle Comunicazioni costituisce **punto di contatto nazionale** per l'IRU (Internet Referral Unit), Unità di Riferimento Internet in ambito Europol sviluppata sulla base del progetto *Check the Web*, con l'intento di condividere con altri Paesi informazioni di intelligence e per rispondere alla necessità di agire tempestivamente quando si presentino contenuti pericolosi che riguardano la nostra od altre Nazioni, condividendo notizie di interesse generale. L'IRU, infatti, effettua una approfondita analisi dei contenuti emersi in rete che possano essere di interesse per la sicurezza nazionale, condividendoli con i Paesi UE e con gli altri Paesi interessati. 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 che lo scorso 1° Dicembre 2017, in occasione del "Maker Faire-Fiera dell'Innovazione" è partita la 5° Edizione di "**Una Vita da Social**", campagna itinerante della Polizia Postale e delle Comunicazioni, grazie alla quale sino ad oggi sono stati incontrati oltre **1 milione e 300 mila studenti, 147.000 genitori, 82.500 insegnanti** per un totale di **10.750 Istituti scolastici** e **190 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**, iniziativa che attraverso la proiezione di un docufilm e le testimonianze dirette dei minori vittime di prevaricazioni, vessazioni e violenze online, vuole offrire uno spunto di riflessione per avviare importanti considerazioni sul peso delle parole, sul loro valore e sulla loro potenza, ma anche sulle responsabilità degli adulti. Inoltre nel corso dell'anno sono stati realizzati incontri educativi su tutto il territorio nazionale raggiungendo oltre **250 mila studenti** e circa **2500 Istituti scolastici** per i quali è stata messa a disposizione anche un'email dedicata: progettoscuola.poliziapostale@interno.it. 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 desidera, 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.

