Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale di giustizia e polizia DFGP
Ufficio federale di polizia fedpol

Marzo 2015

Rapporto annuale 2014

Servizio di coordinazione per la lotta contro la criminalità su Internet SCOCI

KOBIK SCOCI CYCO

Koordinationsstelle zur Bekämpfung der Internetkriminalität
Service de coordination de la lutte contre la criminalité sur Internet
Servizio di coordinazione per la lotta contro la criminalità su Internet
Cybercrime Coordination Unit Switzerland

Ufficio federale di polizia fedpol

Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI)
Nussbaumstrasse 29
3003 Berna

www.kobik.ch
www.cybercrime.ch

Publicazione : 26 marzo 2015

Fonti delle illustrationi: SCOCI, Thinkstock

Prefazione

del consigliere di Stato Christoph Neuhaus,
presidente del comitato direttivo dello SCOCI

Panta rei, tutto scorre – come di consueto, lo SCOCI guarda avanti e si adegua alle nuove circostanze. Infatti è costantemente chiamato ad affrontare nuove sfide, maturare esperienze, sottoporsi ad autocritica e potenziare l'offerta.

In primavera le autorità tedesche hanno informato lo SCOCI in merito a un caso di usurpazione di identità su larga scala. I criminali avevano tentato di accedere ad account di posta elettronica servendosi degli indirizzi e-mail e delle rispettive password al fine di abusare degli account per l'invio di messaggi di spam. La reazione dello SCOCI è stata rapida e pragmatica. I provider e più di 38 000 cittadini già il giorno seguente sono stati informati personalmente dell'accaduto. Le reazioni sono state positive e il Servizio nazionale di coordinazione per la lotta contro la criminalità su Internet è stato in grado di dimostrare la sua capacità di reagire tempestivamente agli imprevisti.

Lo SCOCI coopera in modo proattivo con Interpol, Europol, l'FBI, l'HSI e molte altre autorità estere. Quale rappresentante della Svizzera, lo SCOCI partecipa a gruppi di lavoro internazionali insieme ai seguenti partner: i pubblici ministeri svizzeri, le polizie cantonali, i rappresentanti del settore finanziario, i fornitori di servizi Internet oppure la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, SWITCH Internet Domains e diverse ONG. Altri partecipanti sono la Prevenzione svizzera della criminalità, il Servizio delle attività informative della Confederazione, il DFAE nonché altri servizi federali e cantonali. Affinché la Svizzera possa contare sul sostegno necessario anche in tempi difficili, occorre – come sosteneva già l'ex consigliere federale Ogi – curare personalmente i contatti e le amicizie a livello internazionale.

La cooperazione internazionale consiste anche nello smantellare reti bot illegali costituite da computer infetti collegati tra loro per compiere atti fraudolenti, come pure nel coordinare operazioni nazionali che conducono all'arresto di hacker. Anche l'adesione a comitati o alleanze internazionali che intendono combattere la pedocriminalità su Internet come la Global Alliance against Child Sexual Abuse Online è altrettanto importante. Ad essere fondamentale è tuttavia la fiducia che lo SCOCI è in grado di suscitare grazie all'elevata qualità del suo lavoro. Questa fiducia gli permette infatti di continuare ad essere un partner apprezzato e affermato nella lotta alla cibercriminalità.

Nemmeno in futuro lo SCOCI dovrà temere di non avere sufficiente lavoro o di svolgere un'attività ordinaria priva di sfide. Le cyber-rapine in banche con un bottino miliardario, il sequestro di quantità record di materiale pedopornografico o i danni milionari causati alle piccole e medie imprese svizzere da attacchi di ingegneria sociale sono solo alcuni esempi che mostrano il carico di lavoro che lo SCOCI – finanziato per due terzi dai Cantoni e per un terzo dalla Confederazione – è chiamato ad affrontare insieme ai suoi dieci collaboratori e ai sei collaboratori di fedpol assegnatigli a titolo di sostegno. Entro la fine del 2016 lo SCOCI inoltre sottoporrà al Consiglio federale il piano di attuazione della misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi. In tale contesto proseguono i lavori per la gestione di una panoramica svizzera dei casi e il coordinamento di affari di portata intercantonale.

Lo SCOCI è ambito, non passa quasi giorno senza che si parli di un caso nuovo, sempre più eclatante, di cibercriminalità. Chissà, forse la sfida più grande per lo SCOCI è quella di trasmettere agli organi decisionali una cognizione generale ed estesa della portata della criminalità informatica. In ogni caso servono buone condizioni quadro e investimenti nel settore della sicurezza, anche se questo può comportare costi aggiuntivi.

Indice

1 L’essenziale in breve

- Nel 2014 sono pervenute allo SCOCI complessivamente 10 214 segnalazioni tramite l’apposito modulo online, ovvero il 10,9 per cento in più rispetto all’anno precedente.
- Il 66,9 per cento delle segnalazioni ha riguardato reati contro il patrimonio. Questa categoria di reati ha fatto registrare un ulteriore incremento rispetto ai reati contro l’integrità sessuale, confermando la tendenza già delineatasi negli anni precedenti.
- In totale, 50 segnalazioni sono state trasmesse, in virtù della loro rilevanza penale, a autorità e organizzazioni nazionali o estere.
- Nell’anno in rassegna, le ricerche attive condotte nelle reti *peer-to-peer* hanno permesso allo SCOCI in 86 casi di identificare le connessioni a Internet coinvolte attivamente nello scambio di materiale pedopornografico.
- Le indagini preliminari sotto copertura ai sensi della legge sulla polizia del Cantone di Svitto e le inchieste mascherate secondo il Codice di procedura penale (CPP) svolte dallo SCOCI nel 2014 hanno condotto alla trasmissione di 29 denunce al Cantone competente. Per ragioni di competenza, altri 281 casi sono stati trasmessi ad autorità di perseguimento penale estere per l’ulteriore trattamento.
- Oltre un migliaio di segnalazioni relative a siti Internet contenenti materiale penalmente rilevante è stato trasmesso ad autorità estere tramite Interpol / Europol oppure organizzazioni attive nel settore della criminalità su Internet (p. es. Inhope).
- I lavori di attuazione della misura 6 della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) sono in corso.

2 Lo SCOCI, punto di contatto nazionale

Il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI) funge da centro di contatto nazionale per le persone che intendono segnalare la presenza di contenuti sospetti su Internet. Dopo un primo esame e dopo aver messo al sicuro i dati, lo SCOCI trasmette le segnalazioni di rilevanza penale pervenute tramite l'apposito modulo online alle competenti autorità di perseguimento penale nazionali o estere. Lo SCOCI cerca per quanto possibile di rispondere direttamente alle domande dei cittadini o di indirizzare le persone coinvolte ai competenti servizi specializzati o alle autorità locali di perseguimento penale.

2.1 Segnalazioni pervenute

Nel periodo compreso tra il 1° gennaio 2014 e il 31 dicembre 2014, allo SCOCI è pervenuto un totale di 10 214 segnalazioni di sospetto e domande tramite il modulo online disponibile su www.cybercrime.ch, pari a un aumento del 10,9 per cento rispetto all'anno precedente (9208 segnalazioni).

Il numero delle segnalazioni pervenute non permette di giungere a conclusioni valide in merito alla dimensione effettiva della criminalità su Internet o all'evoluzione dei contenuti illegali diffusi in rete. I dati seguenti rispecchiano infatti soltanto il modo in cui la società percepisce i contenuti e le attività illegali su Internet nonché la predisposizione della popolazione a collaborare attivamente con la polizia e le altre autorità segnalando tali contenuti.

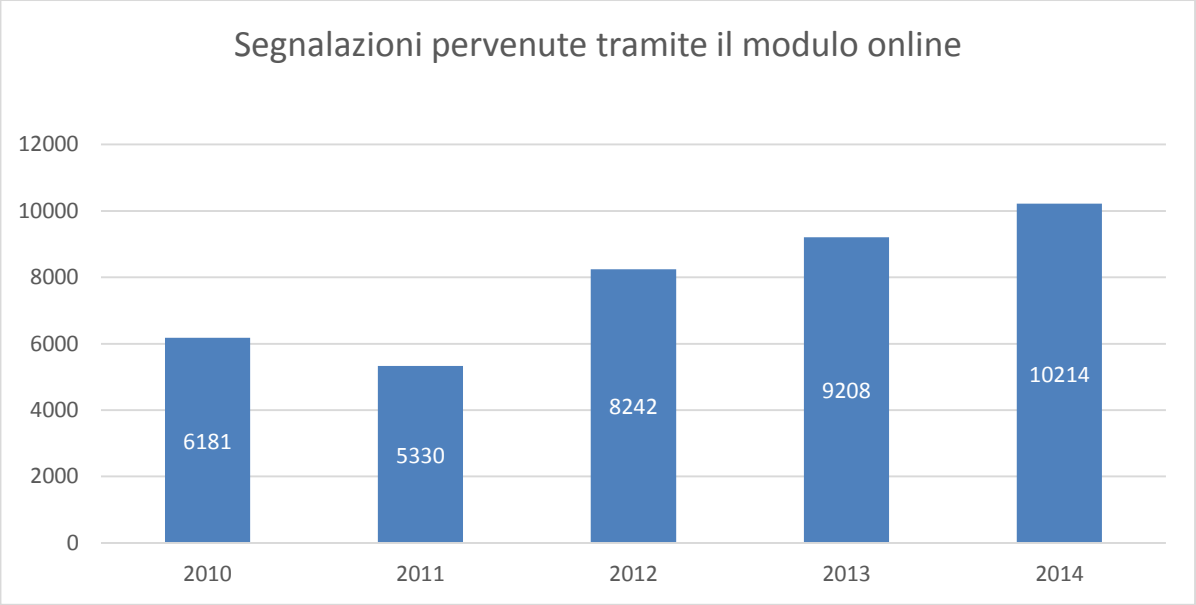

Grafico 1: segnalazioni pervenute tramite www.cybercrime.ch – dati annuali

In media lo SCOCI ha ricevuto mensilmente 851 segnalazioni. Le oscillazioni rilevate già negli ultimi due anni sono state osservate anche nel 2014, con un picco massimo nel mese di maggio (1024 segnalazioni) e una flessione alla fine di settembre (837 segnalazioni) e all'inizio di ottobre (680 segnalazioni). Come nell'anno precedente, nel mese di maggio è stato registrato un aumento delle segnalazioni dei casi phishing e dei tentativi di truffa, mentre nei mesi di settembre e ottobre ne è stata rilevata una diminuzione. Proprio in seguito all'aumento delle segnalazioni pervenute, nel mese di maggio lo SCOCI ha pubblicato sui social media e sul

suo sito Internet quattro avvisi concernenti i fenomeni oggetto delle segnalazioni. Una ragione di tale aumento potrebbe risiedere nella fluttuazione del volume dei messaggi di spam e di phishing attestata dai maggiori produttori di programmi antivirus proprio in concomitanza con le vacanze estive negli Stati Uniti (da fine maggio a fine agosto). Tuttavia, i dati a sua disposizione non permettono allo SCOCI di valutare le effettive ripercussioni di tali fenomeni sul volume delle segnalazioni pervenute.

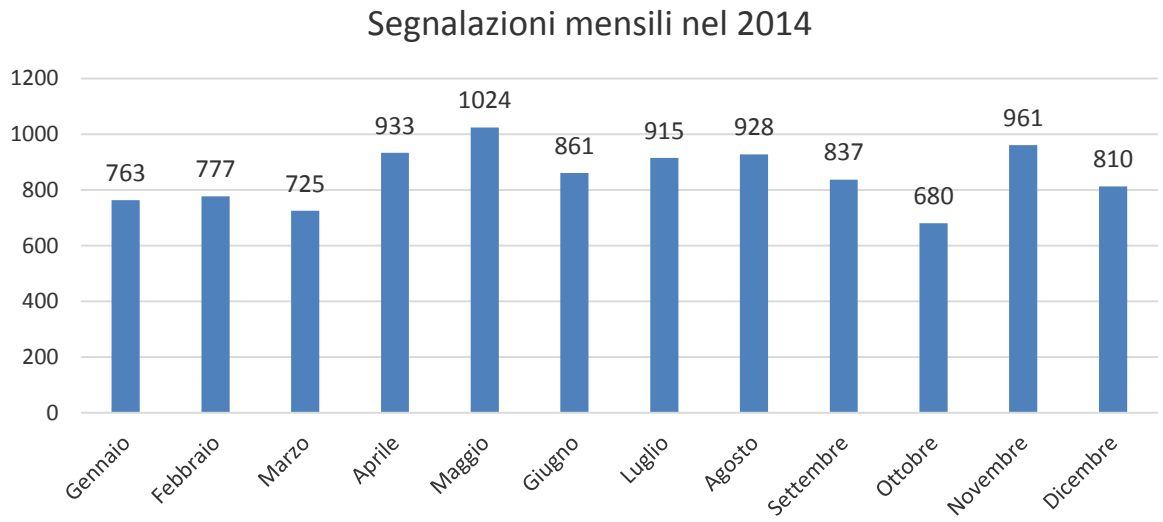

Grafico 2: segnalazioni pervenute tramite www.cybercrime.ch – dati mensili (totale: 10 214)

2.2 Contenuto delle segnalazioni

Le forme di criminalità segnalate allo SCOCI possono essere suddivise in due ambiti interconnessi. Per criminalità su Internet in senso stretto s'intendono i reati perpetrati utilizzando le tecnologie di Internet o sfruttando i punti deboli di esse. Ne fanno parte ad esempio i fenomeni quali l'hacking, i *Distributed Denial of Service* (gli attacchi DDoS) o la creazione e la diffusione di software nocivi (*malware*). Tali reati sono diventati possibili soltanto con l'avvento di Internet e sono diretti contro le sue tecnologie. La criminalità su Internet in senso lato sfrutta invece le possibilità offerte da Internet, quali la posta elettronica o i server per lo scambio di dati, per commettere reati. Rientrano ad esempio in tale categoria i metodi di truffa utilizzati su piattaforme di piccoli annunci o la diffusione di materiale pornografico illegale.

Nel complesso, circa l'87,7 per cento delle segnalazioni ricevute presentava una rilevanza penale, di cui l'88,6 per cento riguarda fattispecie del Codice penale (CP)[1]. Le segnalazioni restanti (11,4 %; cfr. cap. 2.2.3, grafico 9) riguardavano in particolare violazioni della legge federale contro la concorrenza sleale (LCSl)[2], della legge sul diritto d'autore (LDA)[3], della legge sulla protezione dei marchi (LPM)[4], della legge sugli stupefacenti (LStup)[5] nonché della legge sul riciclaggio di denaro (LRD)[6].

[1] Codice penale svizzero del 21 dicembre 1937; RS 311.0

[2] Legge federale del 19 dicembre 1986 contro la concorrenza sleale; RS 241

[3] Legge federale del 9 ottobre 1992 sul diritto d'autore e sui diritti di protezione affini; RS 231.1

[4] Legge federale del 28 agosto 1992 sulla protezione dei marchi e delle indicazioni di provenienza; RS 232.11

[5] Legge federale del 3 ottobre 1951 sugli stupefacenti e sulle sostanze psicotrope; RS 812.121

[6] Legge federale del 10 ottobre 1997 relativa alla lotta contro il riciclaggio di denaro e il finanziamento del terrorismo

In circa il 12 per cento dei casi, dopo aver esaminato i fatti, lo SCOCI non ha constatato contenuti penalmente rilevanti. Tale percentuale racchiude anche le domande inviate allo SCOCI che non concernevano direttamente un reato.

Per le segnalazioni riguardanti fattispecie non perseguibili d'ufficio ma soltanto a querela di parte, lo SCOCI ha indirizzato l'autore della segnalazione alle competenti forze cantonali di polizia.

Rispetto all'anno precedente, la quota delle segnalazioni riguardanti reati contro il patrimonio è aumentata nuovamente. Complessivamente, il 66,9 per cento delle segnalazioni pervenute (6837) riguardava questo titolo del Codice penale (art. 137–172ter CP). Con il 7,4 per cento delle segnalazioni (758), seguono in seconda posizione i reati contro l'integrità sessuale (art. 187–212 CP) che registrano dunque un netto calo, pari al 58,8 per cento rispetto all'anno precedente (da 1842 a 758). A tale proposito occorre sottolineare che con l'entrata in vigore il 1° luglio 2014 della revisione del Codice penale, il possesso e la diffusione di pornografia dura con escrementi umani non è più punibile per legge. Si veda a tale proposito il capitolo 2.2.2.

nel settore finanziario; RS 955.0

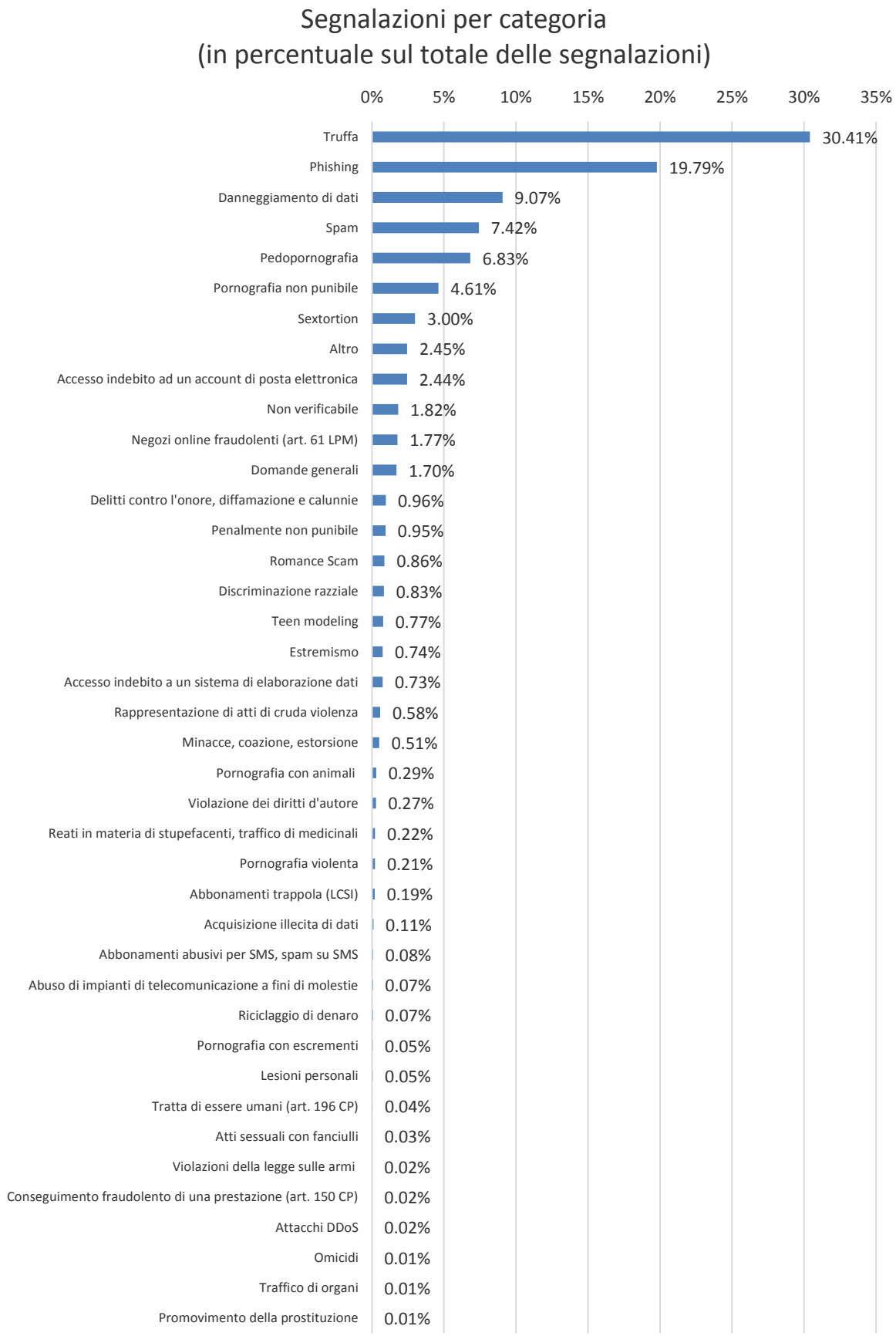

Grafico 3: Segnalazioni pervenute nel 2014 suddivise per categoria (totale: 10 214)

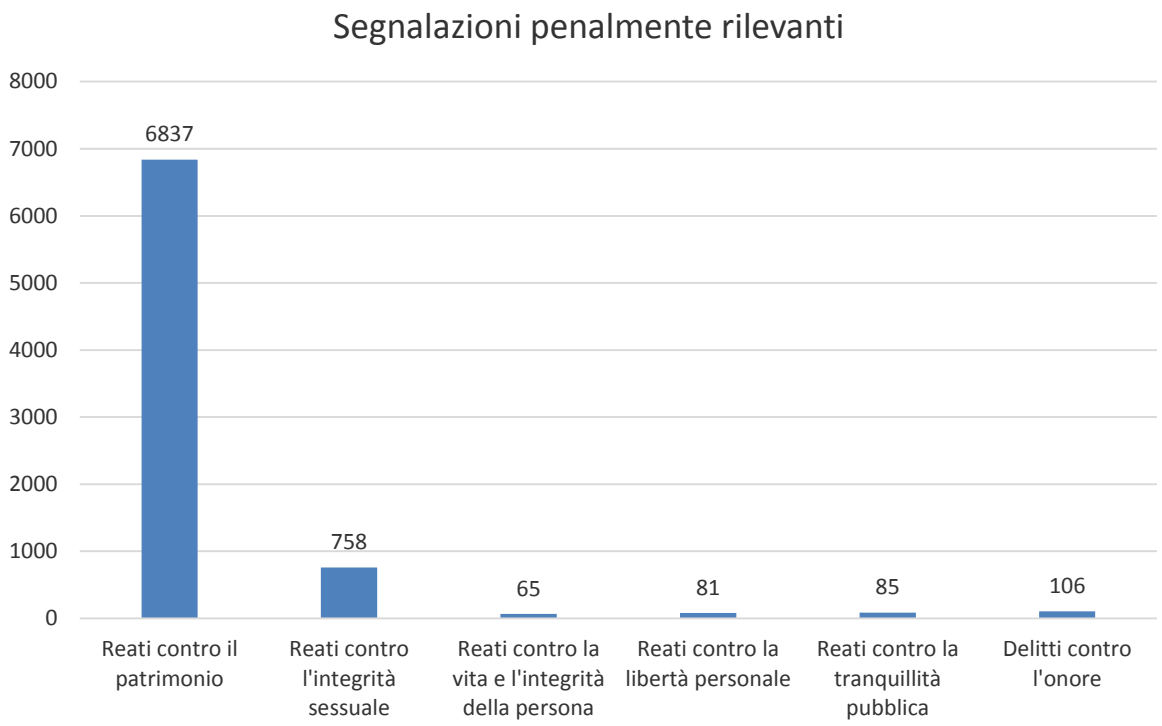

Grafico 4: segnalazioni penalmente rilevanti pervenute nel 2014 (totale: 7932)

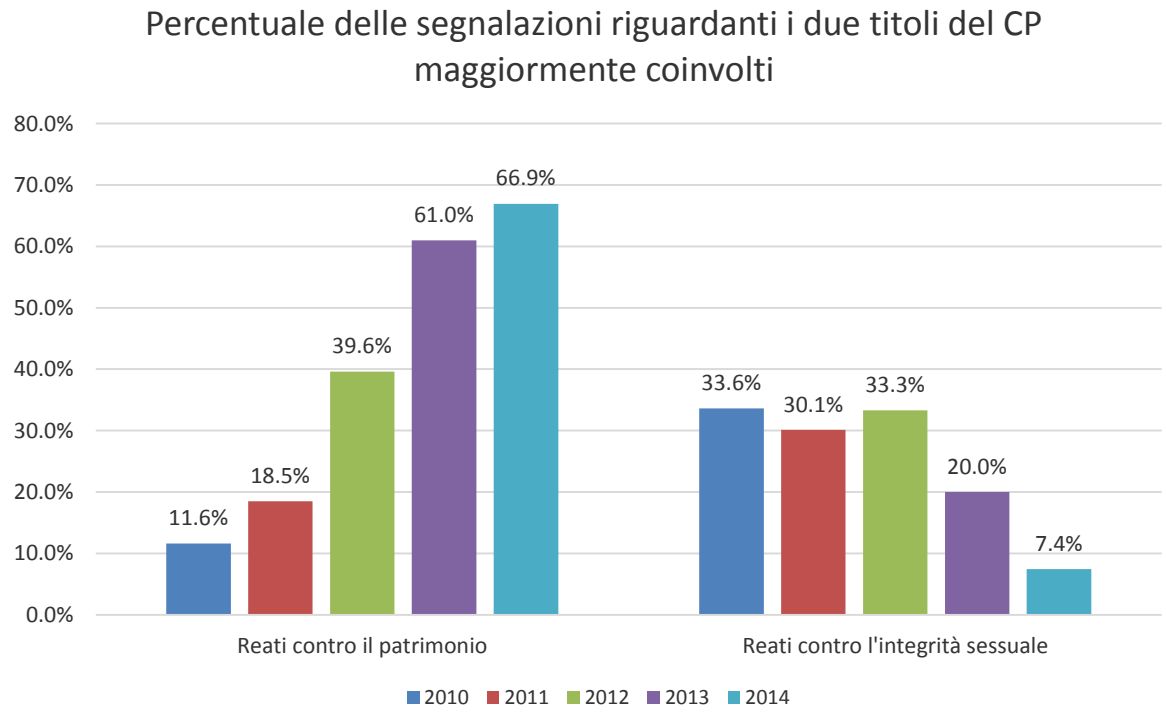

Grafico 5: percentuale delle segnalazioni sui reati contemplati dai titoli 2 e 5 del CP nel periodo 2010-2014

2.2.1 Reati contro il patrimonio

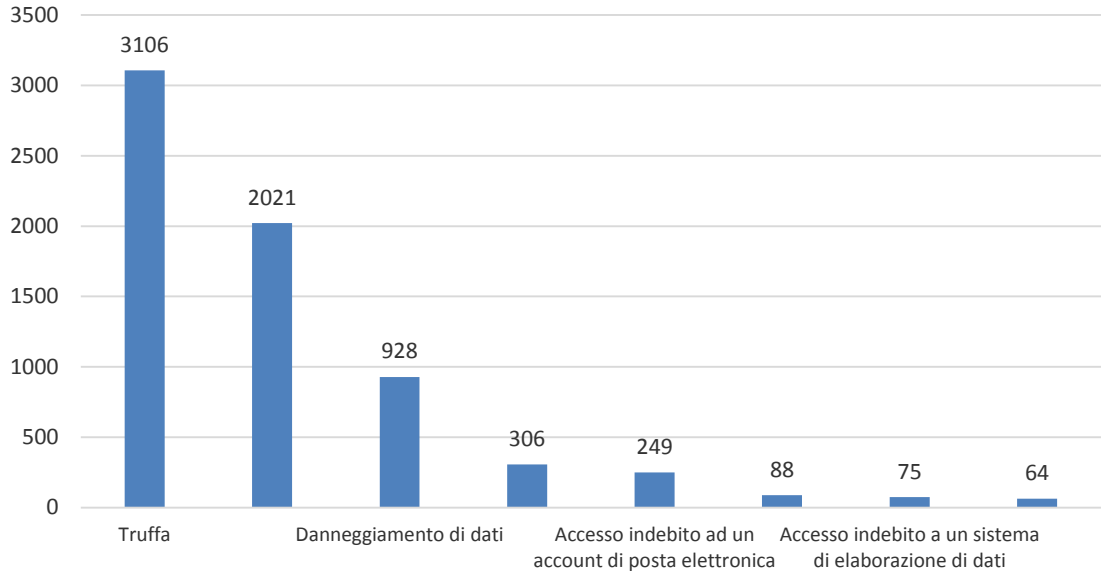

Grafico 6: segnalazioni concernenti i reati contro il patrimonio pervenute nel 2014 (totale: 6837)

Il 66,9 per cento delle segnalazioni (6837) riguarda reati contro il patrimonio. L'aumento registrato sembra corrispondere ai risultati delle analisi di fonti indipendenti quali ad esempio le relazioni trimestrali delle aziende produttrici di software antivirus o dei ricercatori nell'ambito della sicurezza su Internet. Da tali analisi si evince infatti che il volume totale di spam e di attacchi di phishing, così come il numero di nuove infezioni causate da malware e simili, stia aumentando costantemente su scala mondiale. L'elenco dei fatti segnalati descritti qui di seguito non è completo, tuttavia esso rappresenta la maggior parte delle segnalazioni pervenute allo SCOCI.

2.2.1.1 Tentativi di truffa (criminalità su Internet in senso lato)

Con il 30,4 per cento (3106) delle segnalazioni pervenute, i tentativi di truffa rappresentano la quota maggiore del volume totale di segnalazioni. Rispetto all'anno precedente, nell'ambito delle criminalità su Internet in senso lato non sono state accertate grosse differenze nei modi operandi già noti alle autorità.

Anche nell'anno in rassegna, la maggior parte dei tentativi di truffa riguardavano falsi annunci su piattaforme di piccoli annunci e di aste online. Nel mirino dei truffatori vi sono i potenziali acquirenti: le vittime vengono attirate da prodotti, generalmente molto ambiti (smartphone di marca, determinate categorie di auto, ecc.), offerti a prezzi particolarmente favorevoli. L'obiettivo dei criminali è di indurre, grazie a questi prezzi imbattibili, i potenziali clienti a pagare un acconto senza però in seguito avere realmente intenzione di inviare il prodotto acquistato.

Altrettanto frequenti sono le segnalazioni di tentativi di truffa tramite falsi annunci immobiliari. Per commettere questo tipo di truffa, i criminali sfruttano la marcata penuria di alloggi nelle più grandi città svizzera come Zurigo o Basilea, pubblicando inserzioni in cui offrono beni immobiliari a prezzi convenienti. Alle vittime viene promesso di potersi trasferire immediatamente nell'appartamento o di ricevere per posta le chiavi per visionarlo, a condizione di versare in anticipo fino a tre mesi di affitto a titolo di garanzia. Al più tardi al momento della visita dell'appartamento, la vittima scopre di essere stata raggirata.

Non sono soltanto i potenziali acquirenti a essere nel mirino dei truffatori, bensì anche i venditori e gli inserzionisti. Può accadere ad esempio che i truffatori rispondano ad annunci per articoli di elettronica e cerchino di convincere il venditore a spedire la merce all'estero, dichiarando di essere disposti a pagare un prezzo più alto rispetto a quello richiesto. Spesso i criminali cercano di far credere che alcuni articoli di elettronica disponibili su piattaforme di piccoli annunci in Svizzera non siano reperibili all'estero. Essi dichiarano di agire a nome di una terza persona non domiciliata in Svizzera e che pertanto non può concludere l'affare. Se la potenziale vittima decide di procedere alla vendita, viene invitata a spedire la merce; generalmente però la somma pattuita non le sarà mai corrisposta. In un'altra variante, il criminale cerca di convincere il venditore a ricevere il pagamento tramite un servizio di pagamento online. In seguito l'autore invia al venditore delle false conferme di pagamento per la merce acquistata; gli importi dichiarati spesso superano il prezzo effettivamente richiesto. La vittima riceve ulteriori messaggi di posta elettronica inviati servizio di pagamento online fittizio in cui le viene chiesto di pagare dei presunti dazi doganali, il costo del nolo marittimo, ecc. Il truffatore rimane in contatto con la vittima ribadendole che si sta assumendo tutti i costi dissipando così ogni dubbio del venditore. In realtà, tutti i messaggi di posta elettronica del servizio di pagamento e le richieste provengono dal truffatore stesso, e tutto il denaro versato dal venditore finisce nelle tasche del criminale, e l'articolo che la vittima crede di aver venduto risulta irrimediabilmente perduto.

Anche le piccole e medie imprese (PMI) diventano sempre più spesso vittime di truffe. In tali casi i criminali cercano di carpire in tutti i modi informazioni sui metodi di pagamenti in uso presso le potenziali vittime. In un primo momento i truffatori si informano sulle persone responsabili all'interno dell'azienda di tenere regolarmente i contatti con banche o fiduciari. In seguito cercano di ottenere informazioni sui metodi di pagamento utilizzati e sui pagamenti previsti accedendo tramite tecniche di phishing ai dati di accesso alla posta elettronica. I criminali utilizzano successivamente le informazioni raccolte per inviare e autorizzare dei trasferimenti di denaro inviando alle banche e/o alle fiduciarie delle vittime dei falsi ordini di pagamento per posta elettronica. Questa tipologia di truffa può essere altamente redditizia: il denaro così ottenuto nei casi segnalati spazia da alcune centinaia a decine di migliaia di franchi. Sulla base delle comunicazioni delle autorità cantonali di polizia (cfr. cap. 4), si stima che in Svizzera il pregiudizio finanziario totale ammonti già a diversi milioni di franchi.

2.2.1.2 *Sextortion* (criminalità su Internet in senso lato)

Le prime segnalazioni riguardanti il fenomeno di *sextortion* (parola composta da *sex* ed *extortion*, dall'inglese estorsione) sono state inviate allo SCOCI già nel 2013. In questa tipologia di truffa, le vittime, perlopiù uomini, vengono contattati da truffatori, presumibilmente di sesso femminile, su siti di incontri o sui social media. Dopo un primo scambio di messaggi, la truffatrice propone alla vittima di continuare la conversazione su una piattaforma che permette le videochiamate. A questo punto, la vittima può osservare un'avvenente donna spogliarsi e che la induce a compiere degli atti sessuali verranno registrati di nascosto. Il criminale in seguito tenta di estorcere denaro alla vittima minacciando di pubblicare le registrazioni compromettenti se non viene pagata la somma richiesta, normalmente di poche centinaia di franchi. Nei casi segnalati, nonostante i malcapitati abbiano effettivamente pagato il riscatto, i truffatori non si sono esentati dal pubblicare i video compromettenti. Per giunta, le vittime hanno continuato a ricevere minacce e richieste di riscatto con importi sempre più elevati.

2.2.1.3 Phishing (criminalità su Internet in senso lato/stretto)

Con un totale di 2021 segnalazioni (19,8 %), il numero dei tentativi di phishing ha fatto registrare un lieve calo (- 8,5 %) rispetto all'anno precedente (2208 segnalazioni). Con l'invio di messaggi di posta elettronica su larga scala, gli attacchi di phishing mirano ad attirare un gran

numero di persone su siti web il cui aspetto è molto simile a quello di noti servizi Internet. Le potenziali vittime vengono indotte a inserire i propri dati di accesso (nome utente, password). I truffatori non puntano unicamente a ottenere i dati di accesso ai servizi di e-banking o di pagamento online, bensì anche i dati di accesso alle piattaforme di aste o di acquisti online, ai servizi di cloud server, a siti per scaricare musica o a negozi virtuali online di applicazioni per smartphone.

I siti di phishing segnalati nell'anno in rassegna erano localizzati perlopiù su server che gestiscono siti web appartenenti a terzi. I criminali sfruttavano ad esempio le lacune nel sistema di sicurezza dei sistemi di gestione dei contenuti CMS (*Content Management System*) per posizionare le pagine di phishing sui suddetti server. Anche le e-mail di phishing in alcuni casi sono state inviate in modo simile, ovvero tramite mail server utilizzati abusivamente o reti bot.

2.2.1.4 *Police ransomware* (criminalità su Internet in senso stretto)

Il cosiddetto *Police ransomware* (contrazione dei termini inglesi *ransom*, ossia riscatto, e *malware*, software dannoso) è un tipo di software dannoso che impedisce qualsiasi attività futura del computer avvisando l'utente che il blocco può essere rimosso soltanto pagando un riscatto di poche centinaia di franchi tramite un servizio anonimo di pagamenti online. La pressione esercitata dalla richiesta di pagamento del riscatto è accresciuta dal fatto che nel messaggio di blocco visualizzato sullo schermo figura l'emblema ufficiale di un'autorità di polizia o di altre istituzioni. L'infezione del computer è causata dall'apertura inavvertita di un allegato di un messaggio di posta elettronica contaminato oppure visitando un sito Internet infettato appositamente dai truffatori (*drive by download*). Gli attacchi con questo tipo di software non sono mirati: l'obiettivo dei truffatori è quello di infettare il numero più elevato possibile di computer al fine di massimizzare il profitto. A differenza dei software dannosi descritti qui di seguito (*crypto ransomware*), per un esperto è relativamente semplice rimuovere l'infezione e recuperare i dati che erano momentaneamente indisponibile.

2.2.1.5 *Crypto ransomware* (criminalità su Internet in senso stretto)

Già nella seconda metà del 2013 sono aumentate le segnalazioni sui cosiddetti *trojan crittografici* (*crypto ransomware*, combinazione delle parole inglesi *cryptography* ovvero crittografia e *ransomware*, ovvero software dannoso a scopo di ricatto). Analogamente ai *police ransomware*, questa tipologia di virus si diffonde tramite gli allegati di posta elettronica e i siti Internet creati ad hoc. Se il computer dell'utente viene infettato, il software inizia a cifrare e rendere inutilizzabili i file ivi contenuti, come ad esempio i documenti di Microsoft Office o le cartelle contenenti video o file musicali. Nel peggiore dei casi, neanche gli esperti sono in grado di ripristinare i dati, o vi riescono solo profondendo notevoli sforzi. In seguito all'infezione l'utente viene avvisato che i propri dati sono stati criptati e viene costretto a pagare un riscatto sotto forma di denaro virtuale per decrittarli. Tuttavia, il pagamento della somma richiesta non garantisce l'effettiva decrittazione dei dati.

2.2.1.6 *E-banking trojan* e *keylogger* (criminalità su Internet in senso stretto)

Nell'anno in rassegna sono stati segnalati numerosi messaggi di posta elettronica ai quali erano stati allegati software dannosi per e-banking (*e-banking trojan*). I truffatori cercano di indurre i destinatari dei messaggi ad aprire gli allegati facendo loro credere che contengano ad esempio una fattura insoluta di un negozio online oppure una lista di conversazioni di telefonia mobile con l'estero. Aprendo l'allegato la vittima installa il malware sul proprio computer. Una volta installato, il software dannoso è in grado di entrare nelle sessioni aperte di e-banking e di modificare i contenuti visualizzati dal browser. All'utente sembra che siano in corso delle

operazioni di manutenzione, mentre in realtà il truffatore svolge delle vere e proprie transazioni bancarie. Inoltre, esistono varie tipologie di malware in grado di registrare le digitazioni sulla tastiera e il traffico di rete, consentendo così al criminale di trafugare i dati di accesso (nomi utente e password).

2.2.2 Reati contro l'integrità sessuale

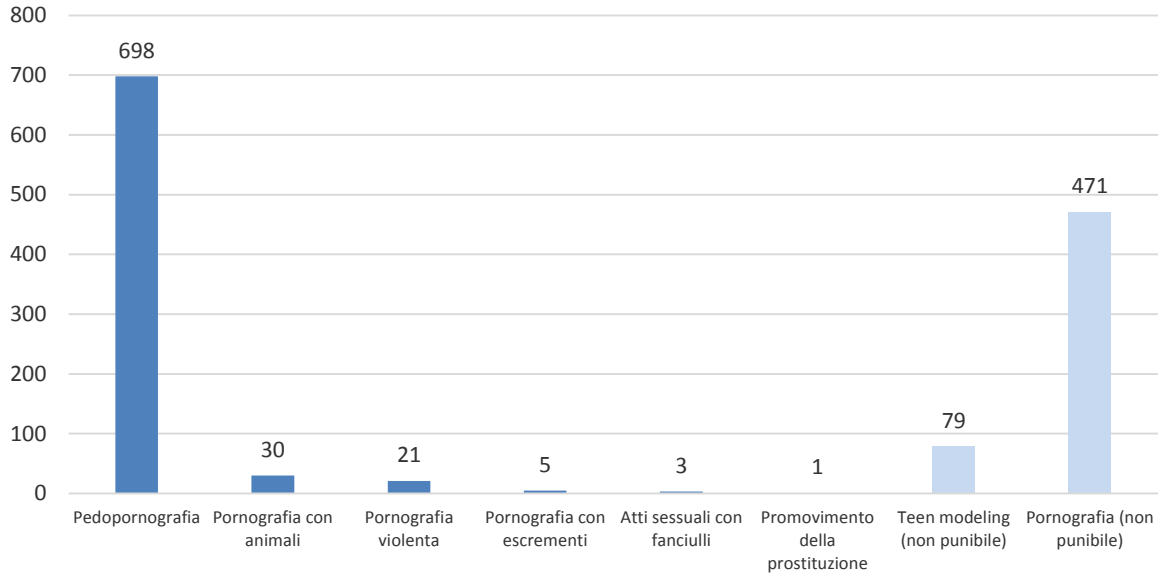

Grafico 7: Segnalazioni concernenti i reati contro l'integrità sessuale nel 2014 (totale dei reati punibili: 758)

Nell'anno in rassegna il numero delle segnalazioni concernenti i reati contro l'integrità sessuale è diminuito in maniera considerevole, ovvero quasi del 58,8 per cento passando da 1842 a 758.

Il numero delle segnalazioni relative a siti contenenti materiale pedopornografico ha fatto registrare nuovamente una netta flessione rispetto al 2013, passando da 1414 a 698 segnalazioni (- 50,6 %). Occorre inoltre osservare che dal 1° luglio 2014 è entrata in vigore una modifica di legge che abroga il divieto di produrre e mettere in circolazione rappresentazioni vertenti su atti sessuali con escrementi. Di conseguenza, le segnalazioni vertenti su questo tipo di rappresentazioni pervenute dopo il 30 giugno 2014, non essendo più penalmente rilevanti, sono state classificate come segnalazioni su contenuti non punibili.

Lo SCOCI ha inoltre ricevuto un totale di 79 segnalazioni di sospetto riguardanti i cosiddetti siti Internet di *teen modeling*. Le immagini di queste pagine web raffigurano minorenni in pose sensuali o che indossano un abbigliamento non adeguato alla loro età, ovvero erotico o osé. Questo tipo di rappresentazioni non è considerato pornografico ai sensi del Codice penale e non è quindi penalmente rilevante. Sebbene tali raffigurazioni siano prive di carattere penale, gli utenti le percepiscono come rappresentazioni pedopornografiche segnalandole allo SCOCI.

In altri 471 casi gli autori delle segnalazioni hanno richiamato l'attenzione dello SCOCI su contenuti per i quali, dopo un esame approfondito, non è stata riscontrata alcuna rilevanza penale, ma che sono stati tuttavia segnalati perché considerati come pornografia vietata. Tali casi concernevano ad esempio siti Internet contenenti immagini di atti sessuali con escrementi segnalati dal 1° luglio 2014 oppure siti Internet le cui raffigurazioni sono state percepite dagli utenti come penalmente riprovevoli, senza che esse presentino tuttavia alcuna rilevanza penale (cfr. paragrafo precedente). Pertanto, tali segnalazioni non sono state inserite nella statistica dei reati contro l'integrità sessuale.

Lo SCOCI ritiene che la flessione delle segnalazioni riguardanti i reati contro l'integrità sessuale sia dovuta in parte alla maggiore efficienza da parte dello SCOCI nella stesura dell'elenco dei siti da bloccare e anche all'ottima collaborazione con i fornitori di servizi di telecomunicazione (FST) e con Interpol. Lo SCOCI ha contribuito in modo decisivo all'elaborazione della lista «Worst-of» di Interpol (cfr. cap. 6). Grazie alla collaborazione tra Interpol e molti motori di ricerca, come Google e Microsoft, molti siti a contenuto pedopornografico non sono più indicizzati portando così sempre meno utenti a entrare in contatto con questo genere di materiale. La cooperazione proattiva con Interpol nell'allestimento della lista «Worst-of», ma anche come pure con gli FST svizzeri, consente quindi allo SCOCI di fornire un contributo essenziale alla riduzione della reperibilità su Internet di materiale vietato e in tal modo di diminuire l'ulteriore vittimizzazione di coloro che sono raffigurati nelle rappresentazioni di abusi sessuali.

Dall'altro lato, il calo delle segnalazioni potrebbe ricollegarsi direttamente alla tendenza già constatata sin dal 2012 di scambiare contenuti pornografici vietati in luoghi di Internet non pubblicamente visibili, come ad esempio le reti The Onion Router (TOR) o Invisible Internet Project (I2P), oppure utilizzando le reti private *peer-to-peer* (cfr. cap. 4.2).

2.2.3 Ulteriori reati

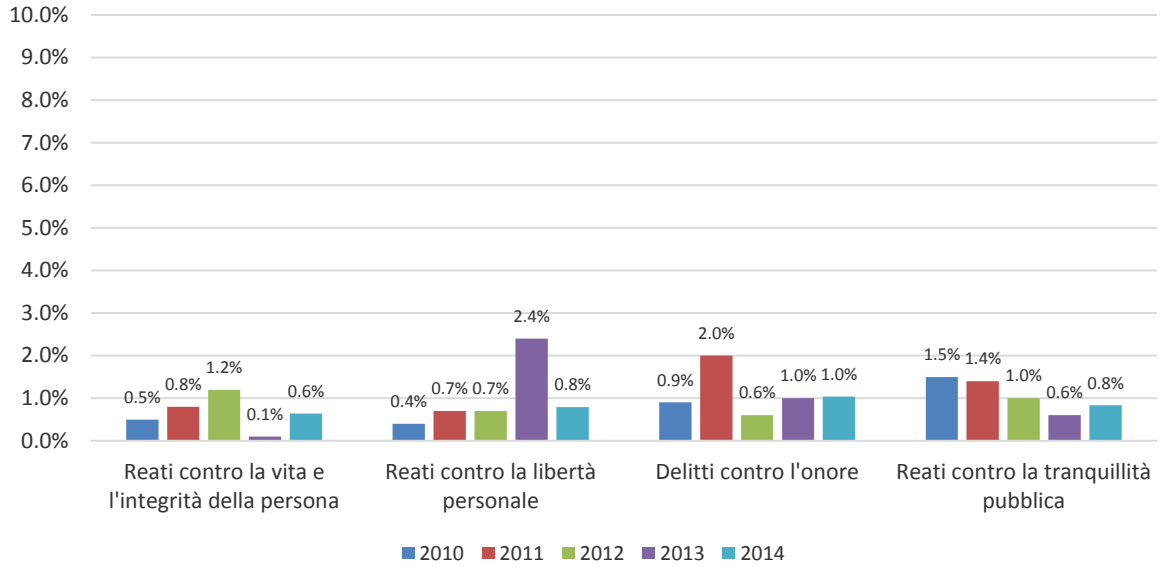

Grafico 8: percentuale delle segnalazioni concernenti reati previsti in altri titoli del CP (2010 – 2014)

Circa il 3,3 per cento di tutte le segnalazioni pervenute riguarda reati contro la vita e l'integrità della persona, la libertà personale, la tranquillità pubblica e l'onore. Complessivamente, 85 segnalazioni concernevano reati contro la tranquillità pubblica. La maggior parte dei casi segnalati concerneva affermazioni estremiste e discriminatorie sui social media. Nonostante la le percentuali relative a tali delitti siano rimaste pressoché invariate, il numero assoluto di annunci è aumentato.

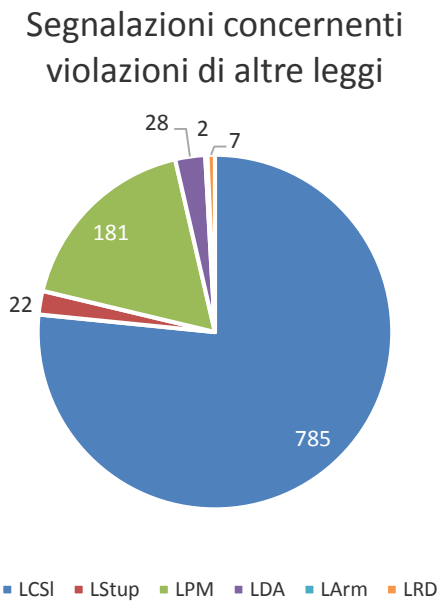

Grafico 9: ripartizione delle segnalazioni concernenti violazioni di altre leggi (il 10 % delle segnalazioni pervenute complessivamente)

Nel 10,0 per cento dei casi segnalati è stata riscontrata un'infrazione ad altre leggi, in particolare alla LCSI, che reprime i messaggi pubblicitari di posta elettronica indesiderati (spam).

Nell'anno in rassegna sono state inviate 181 segnalazioni riguardanti possibili negozi online fraudolenti e la vendita di contraffazioni su dei siti Internet che ricalcano l'aspetto di quelli dei produttori di articoli di marca. Nella maggior parte dei casi, le segnalazioni riguardano negozi online che si spacciano per siti di discount di articoli di lusso e di marca (articoli sportivi, occhiali da sole, borsette, ecc.). I clienti che si sono serviti di questi siti per ordinare merce venduta a prezzi notevolmente ribassati, sia non hanno ricevuto affatto la merce richiesta sia sono state recapitate loro delle contraffazioni scadenti. In 76 casi, i negozi online fraudolenti erano stati registrati con un dominio .ch.

Eliminare simili contenuti al di fuori di un procedimento penale comporta un notevole investimento di tempo. In caso di sospetto, lo SCOCI richiede al centro di registrazione dei nomi di dominio SWITCH un recapito postale in Svizzera del titolare del nome di dominio. Se dopo un periodo di 30 giorni, il titolare non adempie alla richiesta, le condizioni generali di SWITCH permettono di richiedere la cancellazione del nome di dominio.

2.2.4 Sintesi

Nel 2014 il numero di segnalazioni riguardanti reati contro il patrimonio è aumentato ulteriormente, confermando dunque la tendenza già osservata negli anni precedenti. Al contempo, il numero di segnalazioni concernenti i reati contro l'integrità sessuale ha subito, come in passato, una flessione. Il numero complessivo delle segnalazioni concernenti le restanti fattispecie del Codice penale e di altre leggi è rimasto su valori costanti.

In generale si può affermare che i fenomeni osservati nel 2014 erano già noti alle autorità, infatti corrispondono, con alcune variazioni, ai modi operandi evidenziati negli anni precedenti. Tuttavia, si è osservato un miglioramento della qualità dell'agire dei criminali. Si attesta infatti una cura sempre maggiore nella grammatica e nell'ortografia dei messaggi di phishing o degli annunci su Internet. Analogamente, anche l'aspetto degli annunci, dei siti di phishing e dei messaggi di posta elettronica diventa sempre più professionale. Per gli utenti è dunque sempre più difficile distinguere il sito Internet affidabile da quello fittizio.

2.3 Risultato delle attività dello SCOCI

Sulla base delle segnalazioni inviate tramite l'apposito modulo online, lo SCOCI svolge diverse attività e adotta una serie di misure al fine di cancellare o rimuovere i contenuti penalmente rilevanti oppure trasmette le segnalazioni alle autorità di perseguimento penale competenti:

- tutte le 10 214 segnalazioni pervenute sono state analizzate e valutate sotto il profilo della loro eventuale rilevanza penale;
- lo SCOCI ha risposto individualmente a 3218 segnalazioni su 10 214;
- 50 segnalazioni sono state direttamente trasmesse, in virtù della loro rilevanza penale, al Cantone o all'autorità competente;
- più di un migliaio di segnalazioni relative a siti Internet contenenti materiale penalmente rilevante è stato trasmesso alle autorità estere tramite Interpol/Europol oppure organizzazioni attive nella lotta contro la criminalità su Internet (p. es. Inhope);
- numerose segnalazioni sono state trasmesse all'interno di fedpol al commissariato Criminalità generale, organizzata e finanziaria e al commissariato Pedocriminalità/pornografia nonché all'Ufficio di comunicazione in materia di riciclaggio di denaro (MROS);
- i fenomeni oggetto di frequenti segnalazioni hanno portato alla pubblicazione di 27 avvisi sul sito dello SCOCI www.cybercrime.ch, e dalla fine dello scorso anno, anche sulle reti sociali Facebook e Twitter. Lo SCOCI trasmette gli avvisi anche alle organizzazioni partner, alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI, alla Prevenzione svizzera della criminalità nonché ai media. In tal modo è possibile mettere in guardia il pubblico dai pericoli attuali.

2.4 Casistica

Nel 2014 è stata segnalata allo SCOCI la presenza su un sito pornografico di un utente che pubblicava video di frequentatori di uno stabilimento balneare svizzero. I video pubblicati, per lo più di donne, erano stati registrati chiaramente all'insaputa delle vittime. Le immagini ritraevano soprattutto il seno e il sedere delle clienti. Inoltre, i titoli e le descrizioni contenevano affermazioni sessiste e offensive. Dopo che una delle vittime aveva segnalato i fatti ai media, la polizia cantonale competente ha ricevuto numerose denunce per reato contro l'onore. Grazie al sostegno dello SCOCI e alla collaborazione dei gestori della piattaforma, la polizia cantonale è riuscita a identificare e ad arrestare il colpevole.

Grazie alle segnalazioni dei cittadini, lo SCOCI è in grado di redigere e pubblicare sul suo sito Internet e sui social media degli avvertimenti alla popolazione. Per esempio, in aprile diversi utilizzatori di una rete sociale hanno contattato lo SCOCI segnalando degli annunci per partecipare a un dubbioso concorso per vincere un'automobile. Secondo l'annuncio, il concorso era organizzato dalle filiali in Francia e in Svizzera dell'azienda produttrice. L'unica informazione richiesta per la partecipazione era il numero di telefono. In realtà dietro il falso annuncio si nascondeva una trappola: inserendo il numero di telefono cellulare sulla pagina del concorso, l'utente sottoscriveva involontariamente un abbonamento di telefonia mobile. Circa un'ora dall'invio della segnalazione da parte di un cittadino tramite il modulo online, lo SCOCI aveva già potuto pubblicato un avviso sulle reti sociali; quest'ultimo è stato in seguito ripreso e diffuso da diversi media nazionali e internazionali nonché dalla Prevenzione svizzera della criminalità.

3 Ricerche attive da parte dello SCOCI

Ogni anno il comitato direttivo dello SCOCI definisce i settori della criminalità su Internet su cui incentrare le ricerche attive. Come negli anni precedenti, anche nel 2014 tali ricerche erano focalizzate sulla lotta alla pedocriminalità su Internet. Tuttavia, visto la notevole crescita dei reati contro il patrimonio osservata sin dal 2012 è stata ribadita la necessità per lo SCOCI di indagare anche su questa categoria di reati. Questa decisione ha un impatto in particolare sull'attività di coordinamento dello SCOCI (cfr. cap. 4), che è finalizzata perlopiù a garantire lo scambio d'informazioni nell'ambito di operazioni tra autorità svizzere ed estere.

Grazie alle ricerche attive, nel 2014 sono state allestite e trasmesse alle autorità svizzere ed estere complessivamente 396 denunce, pari a una lieve flessione del 6,4 per cento rispetto all'anno precedente.

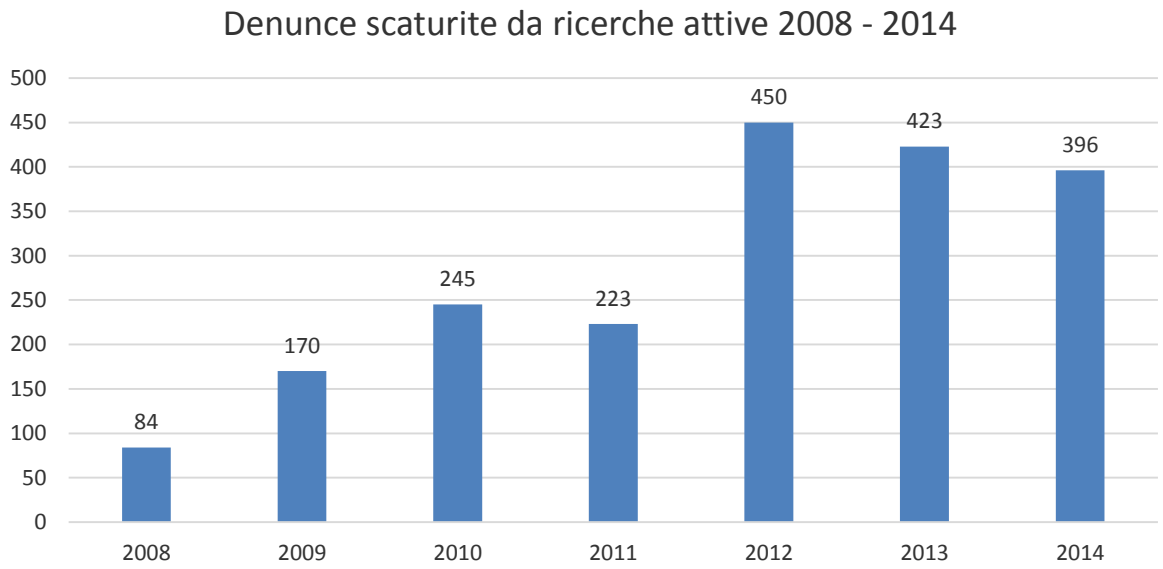

Grafico 10: denunce trasmesse nel quadro di ricerche attive (2008 – 2014)

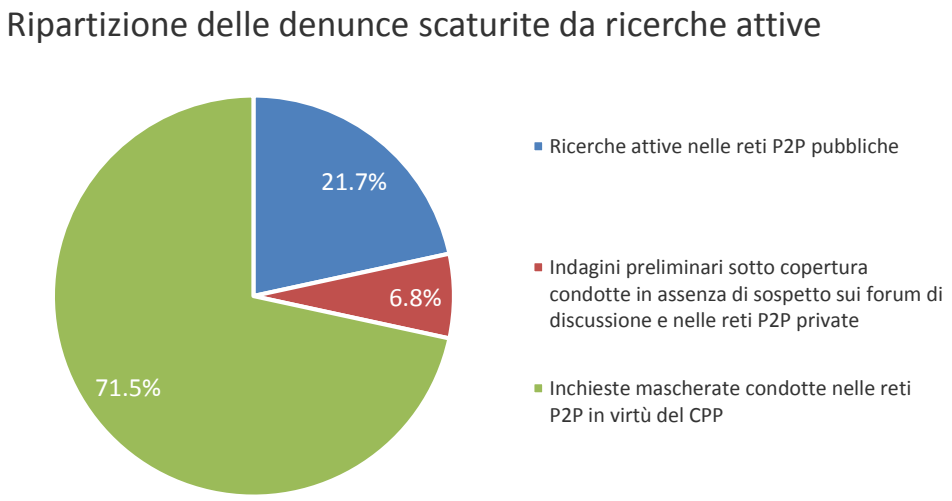

Grafico 11: denunce suddivise in base al tipo di monitoraggio effettuato (totale: 396)

3.1 Ricerche attive nelle reti *peer-to-peer* (P2P)

Su 396 denunce, 86 sono scaturite da ricerche attive condotte dallo SCOCI in reti *peer-to-peer* pubbliche. Rispetto all'anno precedente, il numero di casi ha fatto nuovamente registrare un lieve calo. Tale dato è attribuibile alla diminuzione del numero di utenti attivi nelle reti *peer-to-peer* sottoposte a monitoraggio e al progressivo spostamento delle attività dei cibercriminali verso parti di Internet non pubblicamente visibili come le reti *peer-to-peer* private e il Darknet[7].

Lo scopo delle denunce consiste nell'identificare gli utenti che condividono attivamente e regolarmente materiale pedopornografico ai sensi dell'articolo 197 capoversi 4 e 5 CP. Sebbene lo SCOCI focalizzi le proprie ricerche su utenti domiciliati in Svizzera, nell'anno in rassegna sono stati riscontrati anche reati commessi da una persona domiciliata all'estero (USA). In questi casi lo SCOCI provvede a inoltrare i dati raccolti agli uffici Interpol esteri competenti.

3.2 Indagini preliminari sotto copertura svolte in assenza di sospetti

L'accordo sulla collaborazione in materia di indagini preliminari di polizia svolte su Internet al fine di combattere la pedocriminalità (monitoraggio delle chat) concluso tra lo SCOCI, il Dipartimento della sicurezza del Cantone di Svitto e fedpol, disciplina le modalità secondo le quali i collaboratori dello SCOCI possono svolgere indagini preliminari sotto copertura per contrastare la pedocriminalità in rete[8]. In virtù di tale accordo, i collaboratori dello SCOCI conducono indagini preliminari sotto copertura esclusivamente su incarico e sotto l'egida della polizia cantonale di Svitto. In questo modo s'intende garantire che nel settore della pedocriminalità su Internet le indagini preventive sotto copertura possano continuare a essere svolte, oltre che dai Cantoni, anche da un servizio centrale nazionale e che gli sforzi compiuti dai singoli Cantoni possano essere coordinati.

Le indagini preliminari svolte sotto copertura dallo SCOCI hanno permesso nel 2014 di allestire e trasmettere 26 denunce ai Cantoni competenti e una denuncia alle autorità estere. Due di queste denunce sono scaturite da indagini condotte in alcune chat svizzere destinate in modo specifico ai minori. In un terzo caso è stata sporta denuncia dopo che il pedocriminale, durante una videochat, aveva spontaneamente attivato la propria webcam coinvolgendo così nei suoi atti sessuali l'agente sotto copertura, che si era precedentemente spacciato per una minorenne. Nei tre casi illustrati, la fattispecie denunciata è di tentati atti sessuali con fanciulli (art. 187 CP). Il basso numero di indagini condotte dallo SCOCI nelle chat per minori è riconducibile al fatto che la maggior parte dei Cantoni dispongono ormai delle basi legali necessarie per agire autonomamente in questo tipo di chat. Lo SCOCI mette a disposizione dei corpi di polizia cantonali una piattaforma centrale per la pianificazione nazionale degli interventi e lo scambio d'informazioni evitando così che due Cantoni sorveglino contemporaneamente la stessa chat. La piattaforma rappresenta dunque uno strumento nazionale finalizzato a una sorta di «pattugliamento» costante, gestito autonomamente dai singoli Cantoni. L'intensità di tale attività di pattugliamento dipende dalle possibilità e dalle risorse di cui i Cantoni dispongono per condurre indagini preventive sotto copertura.

Lo SCOCI ha destinato la maggior parte delle proprie risorse al monitoraggio e alle relative

[7] In principio il termine indicava una rete peer-to-peer virtuale sulla quale gli utenti potevano scambiare file con determinate persone di fiducia. Oggigiorno i termini darknet, web nascosto o deep web designano quella parte del world wide web a cui non è possibile accedervi da un normale motore di ricerca.

[8] Intervento ai sensi del § 9d dell'Ordinanza del Cantone di Svitto del 22 marzo 2000 sulla polizia cantonale (PolV; SRSZ 520.110).

indagini sotto copertura nelle reti di condivisione P2P private, la cui natura richiede una conduzion delle indagini centralizzata, nonché agli interventi nel Darknet. Nello specifico, si tratta di ambienti particolari che non permettono di determinare sin da subito la provenienza delle vittime e degli autori dei reati e conseguentemente di stabilire il foro del reato. Sotto un profilo etico-morale è comunque necessario che tali indagini siano condotte, a titolo di misura di emergenza, almeno fino all'identificazione e alla localizzazione delle vittime e/o degli autori e alla trasmissione delle informazioni alle autorità competenti. Sulla base di queste considerazioni, lo SCOCI esegue pertanto tali indagini, per conto dei Cantoni, a livello centralizzato.

Nei restanti 24 casi, le indagini preliminari sotto copertura che hanno portato a una denuncia sono state condotte per l'appunto in reti *peer-to-peer* private. Le reti di questo tipo si differenziano dalle reti *peer-to-peer* classiche per il fatto che i file vengono condivisi direttamente tra gli utenti attraverso un collegamento diretto cifrato, invisibile al pubblico. La presa di contatto con tali utenti presuppone pertanto il ricorso a collaboratori incaricati di svolgere indagini preliminari sotto copertura. In questo tipo di indagini, la maggior parte delle denunce ha riguardato il possesso e la diffusione di materiale pornografico illegale ai sensi degli articoli 197 capoversi 4 e 5 CP rispettivamente degli articoli 197 numeri 3 e 3^{bis} CP prima dell'entrata in vigore della revisione del CP il 1° luglio 2014.

3.3 Inchieste mascherate ai sensi del CPP

Al pari dell'anno precedente, anche nel 2014 lo SCOCI è stato incaricato da alcuni ministeri pubblici cantonali di condurre inchieste mascherate ai sensi del Codice di procedura penale svizzero (CPP). Le inchieste in questione, fondate sugli articoli 285*a* e seguenti CPP, si sono limitate esclusivamente alle reti *peer-to-peer* private. Tali incarichi sono stati affidati nel quadro di procedimenti penali che, a loro volta, erano stati avviati sulla base delle indagini sotto copertura condotte dallo SCOCI in assenza di sospetti conformemente alla legge di polizia del Cantone di Svitto e nel corso dei quali erano scaturiti nuovi casi sospetti. Le inchieste condotte dallo SCOCI hanno portato complessivamente a 283 denunce.

Come accennato in precedenza, i software utilizzati dalle comunità *peer-to-peer* private consentono di creare collegamenti diretti tra due computer per lo scambio di file, indipendentemente dal luogo in cui si trovano gli utenti. Questa particolarità tecnica rende difficile restringere il campo delle ricerche ai soli autori svizzeri. Nel corso delle inchieste condotte, lo SCOCI ha identificato tre autori svizzeri; le restanti 280 denunce sono state trasmesse, corredate delle prove a carico degli autori, alle autorità di perseguimento penale estere competenti nel quadro dello scambio internazionale di informazioni in materia di polizia. Nel trattare sistematicamente i sospetti a prescindere dalla provenienza degli autori dei reati o delle vittime, lo SCOCI adempie, per conto dei Cantoni, all'obbligo, previsto dalla Global Alliance (cfr. capitolo 6.7.3), di combattere a livello globale, in modo congiunto e solidale, il fenomeno degli abusi di minori su Internet. Tale soluzione rappresenta uno sgravio per i Cantoni, in quanto li esenta da impiegare risorse per trattare casi destinati comunque a concludersi con una denuncia all'estero degli autori del reato.

3.4 Riscontri dei Cantoni

Per disporre di una panoramica generale delle misure adottate dai Cantoni, lo SCOCI invita questi ultimi a fornirgli informazioni sugli sviluppi dei casi che sono stati loro segnalati (misure di polizia adottate e/o esito di eventuali procedimenti giudiziari).

Di seguito sono riportati i riscontri pervenuti dai Cantoni nell'anno in rassegna. La stragrande maggioranza dei casi denunciati è scaturita da ricerche attive condotte già nel 2013. Infatti, i riscontri sono trasmessi, in larga parte, solo dopo la conclusione del rispettivo procedimento o il passaggio in giudicato della sentenza.

3.4.1 Riscontri da parte delle autorità cantonali di polizia

Per la prima volta nella storia dello SCOCI i riscontri pervenuti hanno permesso di constatare che ogni segnalazione di sospetto trasmessa dal Servizio di coordinazione è stata seguita da una perquisizione domiciliare.

Tuttavia non è ancora possibile affermare che il 100 per cento delle denunce sia sfociato o è destinato a sfociare in una perquisizione domiciliare. Il fatto che non siano ancora pervenuti tutti i riscontri per il 2013/14 rende infatti impossibile determinare con certezza il numero esatto di perquisizioni complessivamente effettuate. Ciononostante la quota elevata di perquisizioni dimostra che i corpi di polizia si occupano attivamente delle denunce trasmesse dallo SCOCI, conferendo loro un'alta priorità.

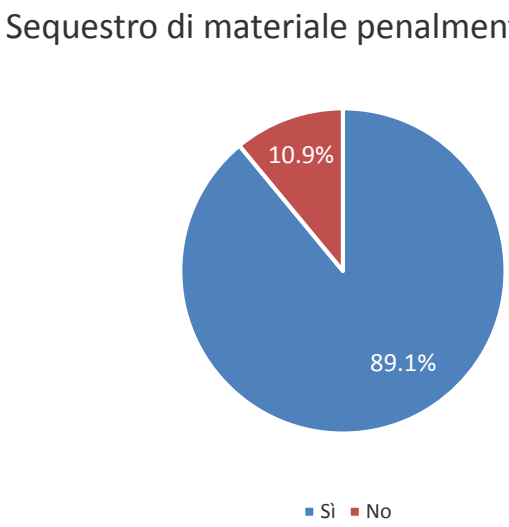

Grafico 12: percentuale delle perquisizioni domiciliari andate a buon fine nel 2014 (sequestro di materiale penalmente rilevante a seguito di una denuncia trasmessa dallo SCOCI)

Nell'89,1 per cento dei casi le perquisizioni domiciliari effettuate in seguito alle denunce trasmesse dallo SCOCI hanno portato al sequestro di materiale illegale. Negli altri casi, le cause del mancato sequestro di materiale sono molteplici. Per esempio, negli ultimi anni è stato dimostrato che le reti wireless pubbliche e non protette rendono impossibile l'identificazione precisa degli autori. Inoltre, il ricorso a supporti di memorizzazione sempre più compatti permette ai criminali di nascondere con crescente facilità il materiale probatorio. Si riscontra infine un maggiore ricorso a supporti cifrati, i quali complicano il sequestro delle prove relative al possesso e allo scambio di materiale illegale.

Nel 92,9 per cento dei casi, il materiale di rilevanza penale sequestrato era di carattere pedopornografico. Non si tratta di un dato sorprendente, soprattutto se si considera che le ricerche attive nelle reti *peer-to-peer*, private o pubbliche, sono incentrate su questo tipo di reati e che la maggior parte delle denunce deriva proprio da queste ricerche. Occorre comunque rilevare che nel 59,1 per cento delle perquisizioni domiciliari effettuate sono state accertate anche altre forme di pornografia illegale (art. 197 CP).

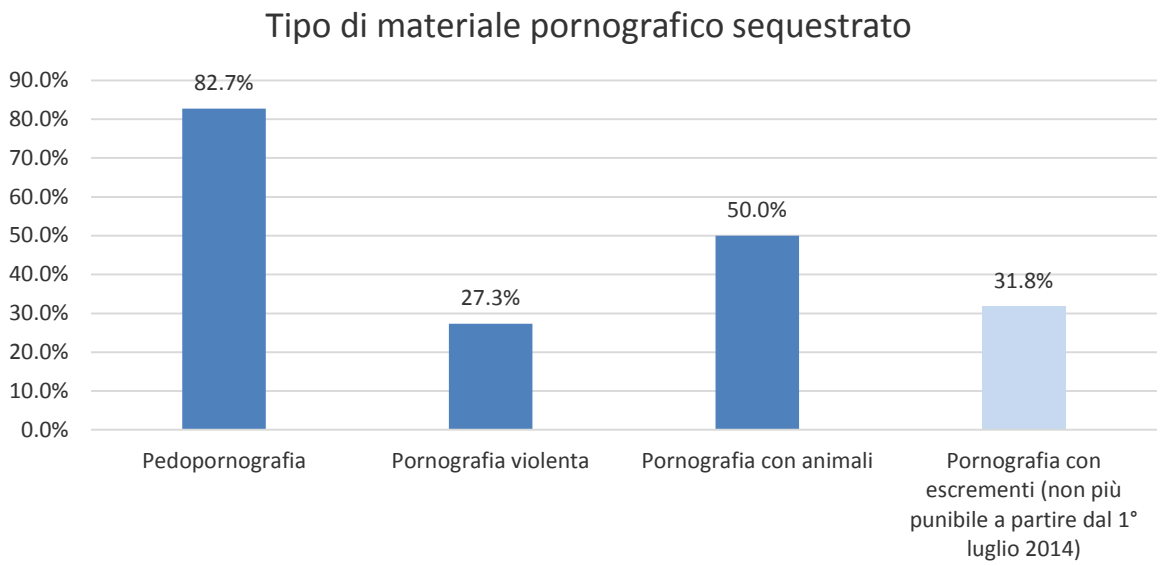

Grafico 13: tipo di materiale pornografico illegale sequestrato nel 2014 durante le perquisizioni domiciliari

Dai riscontri forniti dalle autorità cantonali di polizia emerge che le perquisizioni domiciliari andate a buon fine hanno portato nel 57,1 per cento dei casi al sequestro di filmati, nel 59,2 per cento dei casi al sequestro di materiale fotografico e nel 6,1 per cento dei casi al sequestro di altro materiale probatorio. Nel complesso, le perquisizioni domiciliari hanno portato al sequestro di circa 700 000 filmati e immagini penalmente rilevanti.

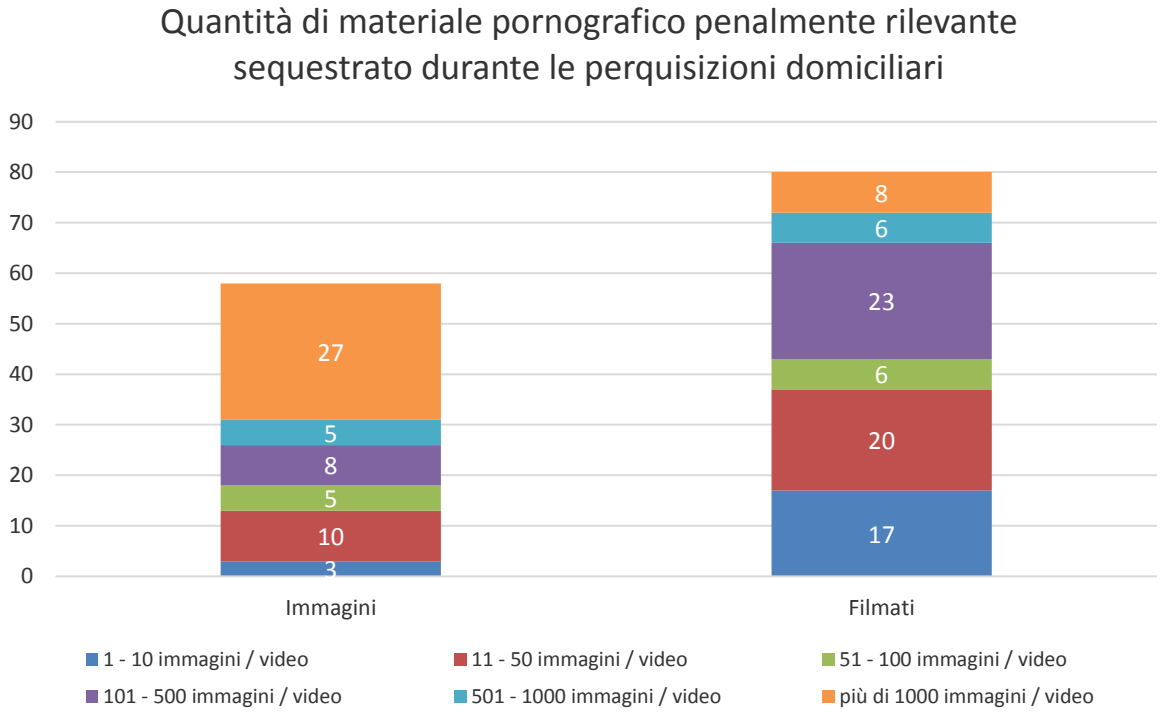

Grafico 14: quantità di materiale pornografico sequestrato nel 2014 nel corso di perquisizioni domiciliari. Il grafico riporta il numero di sequestri effettuati, suddivisi in base alla quantità di immagini o filmati penalmente rilevanti che sono stati rinvenuti (evidenziati da un colore diverso).

3.4.2 Riscontri delle autorità giudiziarie cantonali

Nell'89,5 per cento dei casi in cui le autorità giudiziarie cantonali hanno fornito un riscontro allo SCOCI, i procedimenti penali si sono conclusi con una condanna.

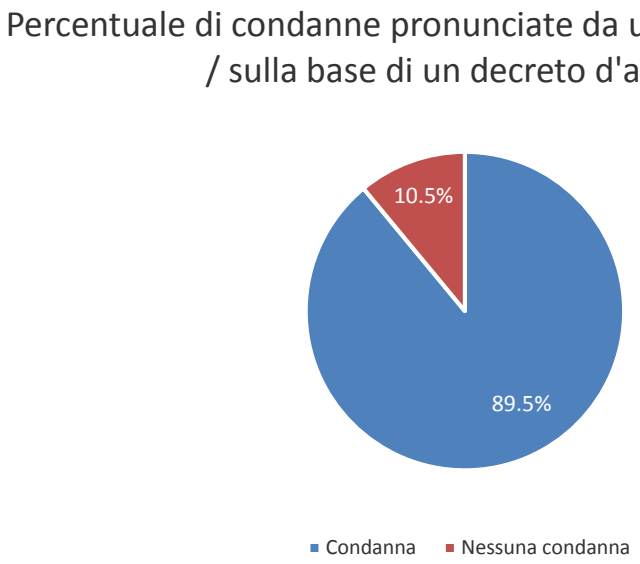

Grafico 15: condanne pronunciate nel 2014 da un tribunale penale o sulla base di un decreto d'accusa

La maggior parte delle condanne è stata pronunciata per possesso di pornografia dura ai sensi del reato di pornografia sancito dall'articolo 197 CP, in particolare in virtù delle fattispecie descritte ai numeri 3 e 3bis di tale disposizione (fino al 30 giugno 2014) ovvero ai capoversi 4 e 5 (a partire dall'entrata in vigore della revisione del CP il 1° luglio 2014).

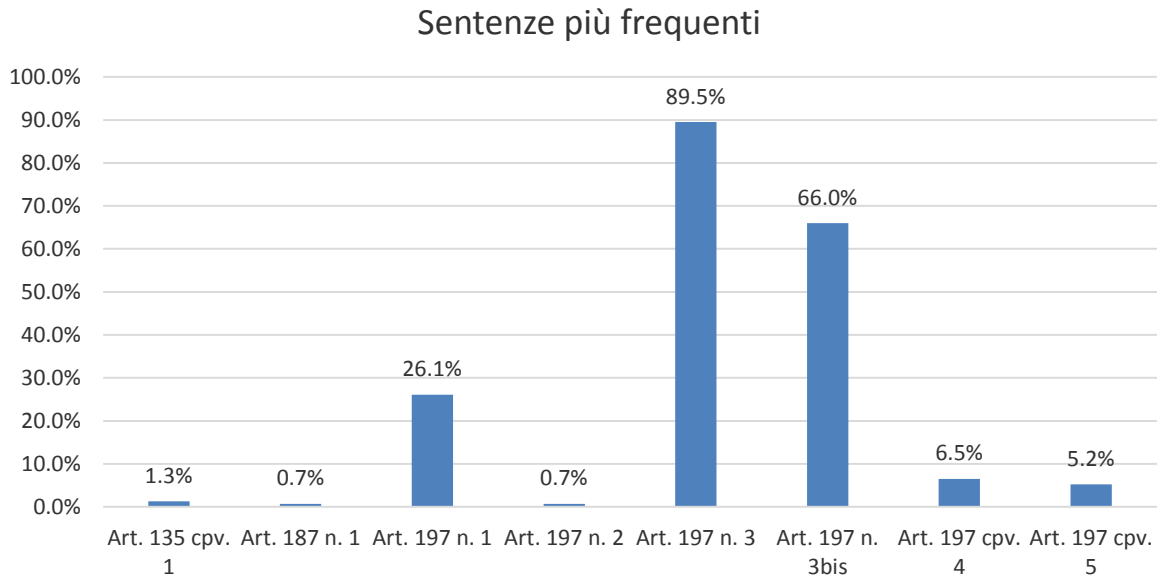

Grafico 16: sentenze più frequenti nel 2014. Il grafico indica la percentuale di sentenze pronunciate in virtù delle disposizioni del Codice penale.

Nel 92,2 per cento delle condanne comunicate nell'anno in rassegna è stata inflitta una pena pecuniaria (aliquota giornaliera), cumulata con una multa nel 74,5 per cento dei casi. Nel 94,3 per cento delle condanne la pena pecuniaria è stata pronunciata con la condizionale. Nel 5,2 per cento dei casi la condanna prevedeva un lavoro di pubblica utilità, una terapia, la privazione della libertà (detenzione) o una pena pecuniaria senza condizionale.

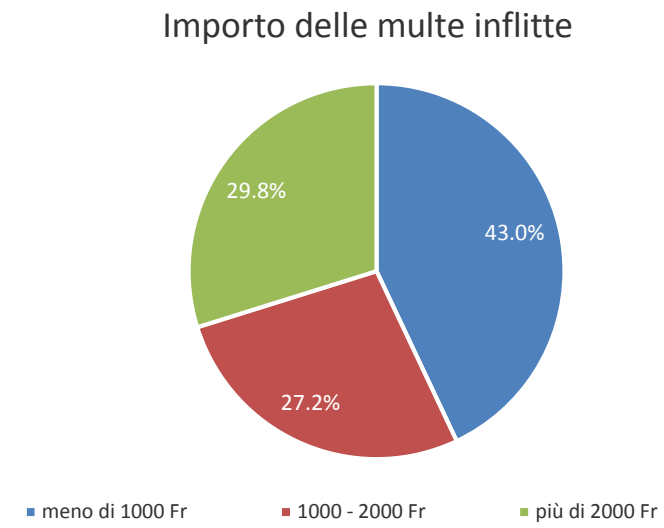

Grafico 17: incidenza degli importi delle multe inflitte nel 2014

All'incirca nel 43,0 per cento dei casi l'importo della multa è inferiore ai 1000 franchi, nel 27,2 per cento dei casi è compreso tra 1000 e 2000 franchi e soltanto nel 29,8 per cento delle multe esso supera i 2000 franchi.

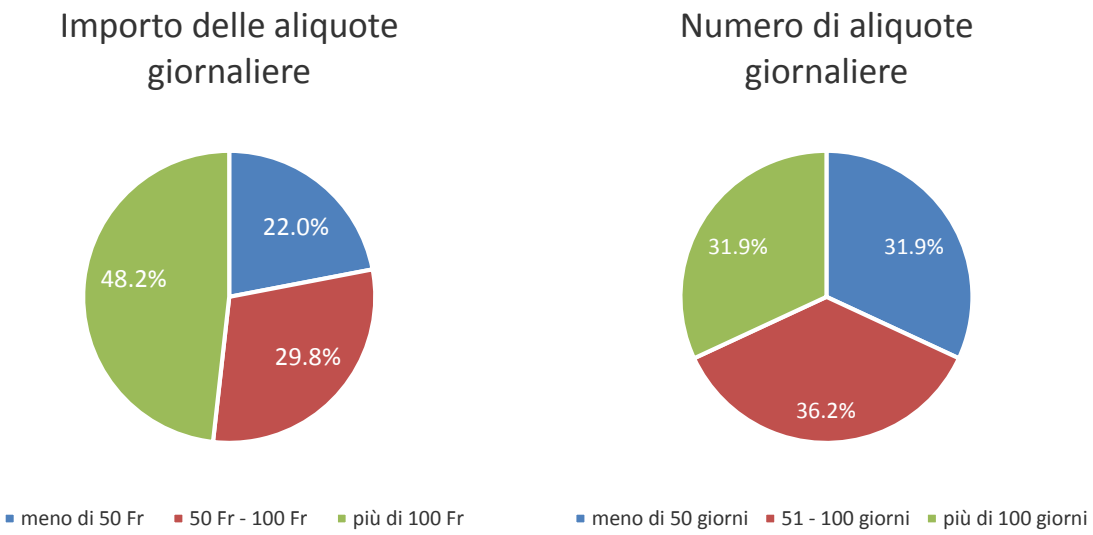

Grafico 18: importo e numero di aliquote giornaliere stabilite nel quadro delle condanne pronunciate nel 2014

Il 31,9 per cento delle pene pecuniarie non supera le 50 aliquote giornaliere, nel 36,2 per cento dei casi la loro entità è compresa tra 51 e 100 aliquote e, infine, nel 31,9 per cento dei casi supera le 100 aliquote giornaliere.

Di norma le persone condannate devono inoltre assumersi le spese procedurali che in molti casi superano ampiamente il valore della multa vera e propria.

4 Casistica

Nel corso delle indagini preliminari sotto copertura condotte dallo SCOCI all'interno di reti private di condivisione di file è stato possibile identificare un utente in Austria. Quest'ultimo aveva fornito all'agente sotto copertura dello SCOCI accesso alla sua ampia raccolta di materiale pedopornografico. Le successive attività d'indagine avevano permesso di risalire a una connessione Internet in Austria, utilizzata dall'autore del reato per collegarsi alla piattaforma di condivisione. In seguito alla trasmissione del caso ai colleghi austriaci, l'ufficio anticrimine della Stiria (Landeskriminalamt Steiermark) ha potuto avviare indagini nei confronti di altre 51 persone sospette residenti in Svezia, Paesi Bassi, Belgio, Danimarca, Brasile e Iran.

In un altro caso, nel corso di una perquisizione domiciliare scaturita da una denuncia dello SCOCI, la polizia cantonale ha potuto sequestrare del materiale pedopornografico. Poiché l'indiziato era il coniuge di una madre diurna, il comune ha deciso di informarne con un comunicato stampa la cittadinanza. Dal 2012 la famiglia diurna aveva già avuto in custodia tre bambini. Fortunatamente dalle indagini condotte dalle autorità cantonali non sono emersi indizi di violenze subite da minori.

4 Scambio di informazioni di polizia giudiziaria

4.1 Segnalazioni ricevute e trasmesse

Da quando nel 2009 è stato integrato nella Polizia giudiziaria federale, lo SCOCI ha assunto la funzione di coordinamento dello scambio internazionale di informazioni di polizia giudiziaria nell'ambito della criminalità su Internet. In qualità di centro di competenza e di coordinamento, lo SCOCI fornisce sostegno ai Cantoni nelle loro indagini. Con l'entrata in vigore nel nostro Paese della Convenzione sulla cibercriminalità (*Budapest Convention on Cybercrime, Council of Europe*, CCC) il 1° gennaio 2012, a livello internazionale la Svizzera è considerata sempre di più un partner attivo nella lotta contro la criminalità su Internet. Per adempiere tali compiti, lo SCOCI dispone di un'ampia rete di contatti in Svizzera e all'estero, sia nel settore pubblico che in quello privato. Lo SCOCI funge inoltre, per conto dei Cantoni, da punto di contatto con le organizzazioni internazionali Interpol ed Europol per le questioni concernenti la cibercriminalità. Uno dei suoi partner più importanti in tale ambito è l'European Cybercrime Center (EC3) di Europol.

Allo SCOCI sono pervenute complessivamente 1314 segnalazioni di polizia giudiziaria attraverso diversi canali, ossia il 77,8 per cento in più rispetto all'anno precedente. La stessa tendenza è stata riscontrata sul fronte delle segnalazioni trasmesse che hanno fatto registrare un aumento del 35,8 per cento con un totale di 1285 segnalazioni. Tali segnalazioni comprendono lo scambio di informazioni con le autorità svizzere ed estere.

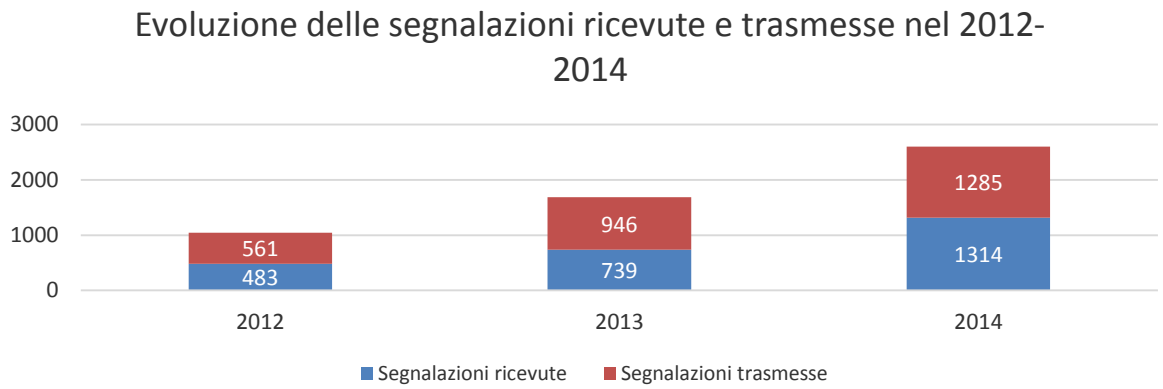

Grafico 19: sviluppo del numero di segnalazioni nell'ambito dello scambio di informazioni di polizia giudiziaria nel 2012-2014

La Convenzione sulla cibercriminalità prevede la possibilità per i Paesi firmatari di chiedere la conservazione rapida di dati informatici in relazione ai quali intendono presentare una domanda di assistenza giudiziaria (art. 29 segg.). A tale proposito, lo SCOCI ha trasmesso alle autorità estere 15 domande pervenute dai Cantoni. Le autorità estere hanno presentato a loro volta 11 domande.

4.2 Coordinamento delle procedure sul piano nazionale e internazionale

Sulla base delle segnalazioni ricevute e trasmesse nell'ambito dello scambio internazionale di informazioni di polizia giudiziaria, lo SCOCI adotta costantemente misure di coordinamento.

Nel 2014 tali misure sono state necessari in 146 casi. Il tipo di sostegno fornito varia a seconda della situazione concreta. Lo SCOCI assume il ruolo di punto di contatto centrale tra le autorità estere di polizia, in particolare nell'ambito di procedure investigative internazionali, e fornisce consulenza alle autorità giudiziarie e di polizia svizzere. In altri casi, soprattutto in quelli di competenza cantonale, lo SCOCI sostiene i servizi richiedenti fornendo loro analisi, pareri tecnici e perizie legali oppure impiegando agenti sotto copertura.

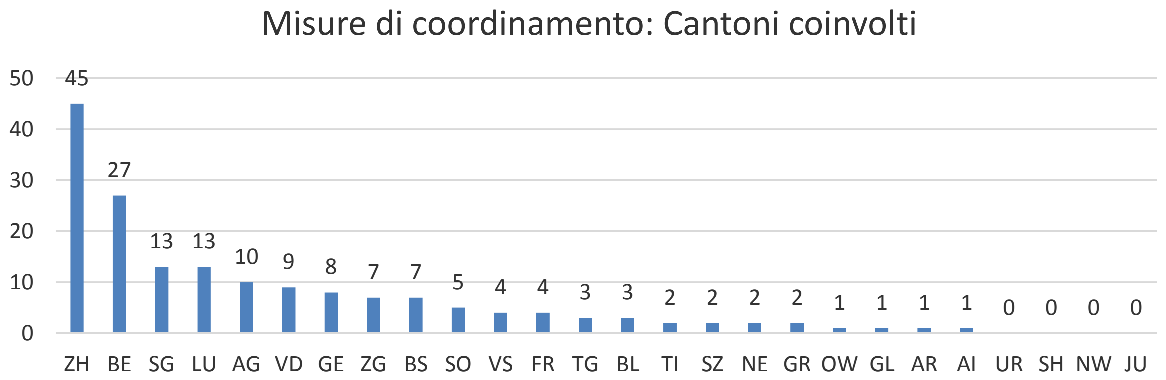

Grafico 20: Cantoni coinvolti dalle misure di coordinamento nel 2014. Poiché una misura di coordinamento può interessare più Cantoni, il totale delle misure riportate nel grafico non corrisponde al numero summenzionato.

L'obiettivo delle misure adottate dallo SCOCI è di garantire che le risorse a disposizione dei servizi cantonali di polizia vengano impiegate in maniera ottimale nonché di evitare le sovrapposizioni nelle procedure d'indagine nazionali. In tale ambito, in due casi il Servizio ha organizzato delle sedute di coordinamento con i rappresentanti delle unità inquirenti delle polizie cantonali impegnate nei medesimi casi.

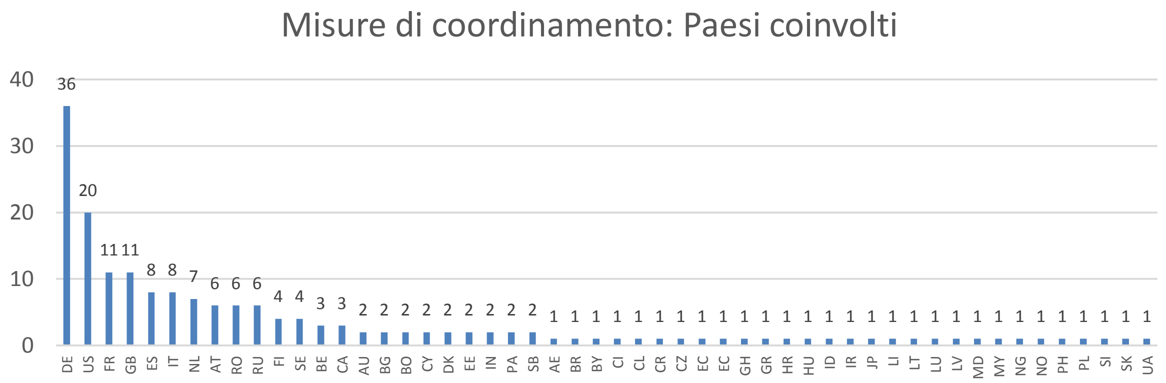

Grafico 21: Paesi coinvolti dalle misure di coordinamento nel 2014. Poiché una misura di coordinamento può interessare più Paesi, il totale delle misure riportate nel grafico non corrisponde al numero summenzionato.

Il perseguimento penale di una banda criminale che agisce dall'estero richiede un dispiego notevole di risorse e ampie conoscenze tecniche. Perseguire un singolo reato nell'ambito di un caso complesso, quale un attacco a seguito di un malware, spesso è un'operazione destinata a fallire per mancanza di tracce concrete. L'esperienza maturata nell'ambito di un caso complesso in cui un software dannoso è stato utilizzato a scapito di clienti di banche svizzere, dimostra l'importanza e gli oneri di una gestione del caso a livello nazionale (cfr. misura 6 Strategia nazionale per la protezione della Svizzera contro i cyber-rischi). È di fondamentale importanza tenere una panoramica centralizzata dei casi per individuare i legami tra l'attacco

vero e proprio con il malware, la sua diffusione tramite e-mail o siti Internet creati appositamente nonché il pagamento e il successivo trasferimento del denaro rubato. Le indagini possono fornire indicazioni utili solamente se le denunce in relazione al fenomeno vengono registrate e analizzate sistematicamente. Inoltre, poiché tali casi raramente riguardano soltanto la Svizzera, bensì tutta l'area francofona o germanofona, è dunque imprescindibile ed efficiente dal punto di vista delle risorse impiegate cooperare a livello internazionale e attuare uno scambio di informazioni con i vari partner, come ad esempio con l'European Cybercrime Center EC3 di Europol.

4.3 Casistica

Nel mese di maggio un'operazione di polizia coordinata a livello internazionale dall'FBI in 16 Paesi, ha condotto all'arresto di circa 100 diffusori del malware «Blackshades». Prima di tale operazione, lo SCOCI aveva avviato delle indagini preliminari in merito a possibili diffusori svizzeri del malware basandosi sulle indicazioni trasmesse dall'FBI nell'ambito dello scambio internazionale di informazioni di polizia giudiziaria. Sulla base di tali indagini preliminari e in seguito a una seduta di coordinamento indetta dallo SCOCI con i ministeri pubblici e le autorità di polizia coinvolti, 11 Cantoni hanno avviato procedimenti penali nei confronti dei presunti acquirenti per importazione di software dannoso ai sensi dell'articolo 144bis numero 2 del Codice penale. Dopo ulteriori indagini, in una seconda seduta di coordinamento le autorità cantonali di perseguimento penale hanno presentato i primi risultati e discusso la procedura da adottare il giorno previsto per l'operazione internazionale di polizia. Nel corso dell'operazione le autorità cantonali hanno effettuato contemporaneamente 16 perquisizioni domiciliari e i successivi interrogatori. L'età media delle persone arrestate era di 24 anni, il più giovane aveva appena 16 anni. Grazie alle procve raccolte nel corso delle perquisizioni domiciliari e agli interrogatori, sono state già pronunciate le prime sentenze.

In un altro caso lo SCOCI ha ricevuto una domanda in virtù degli articoli 29 e 30 della Convenzione sulla cibercriminalità. Nel corso di un'indagine effettuata dall'autorità richiedente è stato accertato l'abuso di un servizio online svizzero allo scopo di inviare tramite posta elettronica messaggi ricattatori. Nella domanda, l'autorità estera aveva chiesto la conservazione rapida di informazioni che avrebbero potuto essere utili all'identificazione dell'autore de messaggi minatori. Il servizio online coinvolto era gestito da un privato (in un primo momento sconosciuto) tramite un sito Internet facente capo a un hosting provider svizzero. Siccome il domicilio del privato e il luogo in cui erano localizzati i dati erano ubicati in due Cantoni differenti, è stato necessario il coordinamento delle misure di polizia e giudiziarie. In collaborazione con i corpi di polizia coinvolti, i ministeri pubblici cantonali e l'ambito direzionale Assistenza giudiziaria internazionale dell'Ufficio federale di giustizia, è stato possibile identificare tempestivamente il gestore del servizio online e accedere ai dati richiesti. Grazie alla trasmissione in formato digitale della copia preliminare della domanda di assistenza giudiziaria da parte dell'autorità richiedente, già il giorno successivo è stato possibile trasmettere rapidamente i dati richiesti in applicazione dell'articolo 30 della Convenzione sulla cibercriminalità.

5 Progetti

5.1 SNPC

Il 27 giugno 2012 il Consiglio federale ha approvato la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC). Tale strategia, e in particolare la misura 6, riconosce la lotta della criminalità su Internet come un fattore essenziale per la protezione delle infrastrutture critiche. In virtù delle proprie competenze, il DFGP è stato incaricato dell'attuazione di questa misura. A tal fine, è chiamato a elaborare, d'intesa con i Cantoni, un documento programmatico che fornisca una panoramica aggiornata della criminalità su Internet in Svizzera e permetta dunque di coordinare con più efficienza gli affari di portata intercantonale. Le informazioni ottenute in materia di perseguimento penale dovranno confluire in una rappresentazione globale della situazione destinata a MELANI.

Il documento programmatico dovrà essere presentato al Consiglio federale entro la fine del 2016. Oltre alla misura descritta, esso chiarirà le questioni relative ai punti di contatto con gli altri attori coinvolti nell'ambito della riduzione dei rischi informatici, al coordinamento con i lavori per la rappresentazione della situazione nonché alle risorse e agli adeguamenti giuridici necessari a livello federale e cantonale.

I lavori in vista dell'attuazione della misura 6 dell'SNPC sono stati avviati con successo. All'inizio di maggio 2014, lo SCOCI ha lanciato un sondaggio nazionale presso tutte le autorità di perseguimento penale della Confederazione e dei Cantoni. I riscontri pervenuti hanno permesso di determinare la situazione attuale come pure i punti deboli e le esigenze delle autorità impegnate nella lotta alla criminalità su Internet che sono quindi confluiti nel documento programmatico.

Poiché i lavori relativi al progetto si sono rivelati, a causa della complessità dell'incarico, più impegnativi del previsto, è stato necessario rinviare la consultazione presso i Cantoni al primo trimestre del 2015.

La versione definitiva del documento dovrebbe essere disponibile a partire da settembre 2015. Successivamente il progetto sarà presentato al Consiglio federale.

6 Gruppi di lavoro, cooperazione e contatti

6.1 Raccolta nazionale di file e valori hash

Lo SCOCI gestisce insieme ai Cantoni una raccolta di valori hash di immagini classificate in modo univoco come pornografia illegale. Lo scopo di questa raccolta è di ridurre lo stress psichico e la mole di lavoro per gli inquirenti che si occupano dei casi di diffusione di materiale pedopornografico. A tale scopo, le immagini i cui valori hash sono già stati registrati nella Raccolta nazionale vengono classificate automaticamente. La Raccolta nazionale di file e valori hash è entrata nella fase operativa nell'ottobre del 2012 e da allora è a disposizione dei servizi specializzati dei corpi di polizia cantonali e municipali.

Con l'entrata in vigore il 1° luglio 2014 della modifica dell'articolo 197 del Codice penale è stato abrogato il divieto relativo alla pornografia con escrementi. Ciò ha richiesto un adeguamento della Raccolta nazionale e la cancellazione dei valori hash delle immagini ivi registrate riconducibili a tale categoria.

Sono messi a disposizione dei Cantoni soltanto i valori hash le cui immagini corrispondenti sono già state valutate tre volte in modo univoco come pornografia illegale. L'attività di classificazione richiede del tempo. Inoltre ai fini dello scambio internazionale è indispensabile, oltre a una classificazione uniforme, anche uno standard di qualità affidabile. Lo scopo di questo controllo di qualità è quello di garantire che i valori hash di materiale classificato in modo univoco come illegale possano essere utilizzati nell'ambito di un processo.

Alla fine del 2014 lo SCOCI aveva ricevuto complessivamente circa quattro milioni di immagini, i cui valori hash sono stati successivamente registrati nella Raccolta nazionale. La categorizzazione del materiale visivo si rivela dispendiosa in termini di tempo e può essere garantita soltanto grazie al sostegno dei Cantoni. Finora sono 138 000 le immagini valutate tre volte in modo univoco come illegali e registrate dunque nella Raccolta nazionale.

Lo SCOCI mette inoltre a disposizione dei Cantoni per lo svolgimento di indagini forensi tre milioni di valori hash provenienti dall'estero. Nello specifico, si tratta di valori che sono stati calcolati dalle autorità estere di perseguimento penale e trasmessi allo SCOCI. Tuttavia, essendo sprovvisti del corrispondente materiale visivo, essi non possono essere sottoposti a un controllo qualitativo. Per tale ragione, a differenza dei valori registrati nella Raccolta nazionale, questo tipo di dati possono essere definiti semplicemente come valori hash sospetti. Lo SCOCI mette inoltre a disposizione liste bianche contenenti 78 milioni di valori hash relativi a contenuti penalmente irrilevanti (p. es. le icone dei sistemi operativi o delle applicazioni). Dette liste permettono di ridurre automaticamente il numero di file che gli analisti forensi sono chiamati a elaborare. Lo SCOCI acquisisce regolarmente questo tipo di liste e le mette a disposizione insieme alle cosiddette liste nere.

Attualmente lo SCOCI sta elaborando in collaborazione con i Cantoni un piano per ampliare la raccolta di dati ai fini di un'identificazione sistematica delle vittime e di un confronto con la banca dati ICSE[9] di Interpol. Tali attività sono strettamente connesse con gli obiettivi della Global Alliance (cfr. cap. 6.7.3), il cui adempimento prevede tra l'altro per la Svizzera di elaborare insieme ai Cantoni entro il 2016 un piano nazionale di identificazione delle vittime.

La gestione di una banca dati nazionale di immagini non solo permette di diffondere i valori hash e di utilizzarli per l'analisi forense del materiale sequestrato, ma fornisce anche spunti

[9] ICSE – International Child Sexual Exploitation image data base

investigativi per l'identificazione degli autori dei reati e delle vittime. Non disponendo di informazioni precise sul luogo del reato, al momento dell'apertura delle indagini le autorità inquirenti non sono comunque in grado di sapere se gli abusi commessi rientrano nella propria area geografica di competenza. A tale proposito, va comunque notato che l'approccio consistente nel condurre indagini orientate all'identificazione delle vittime basandosi sulle immagini sequestrate e sulla cooperazione transfrontaliera, è riconosciuto come più che promettente a livello internazionale. Inoltre, appare opportuno, sul piano etico-morale, destinare le risorse disponibili all'identificazione di minori che, al momento del sequestro o dell'esame delle immagini, si presume possano essere ancora vittime di abusi sessuali; tale principio resta valido anche nel caso in cui dovesse emergere che gli abusi sono stati commessi al di fuori della propria area geografica di competenza. Le vittime possono pertanto contare sul fatto che le autorità di perseguimento penale agiranno, indipendentemente dalla loro competenza territoriale, per prevenire gli abusi e assicurare i colpevoli alla giustizia. La soluzione consiste dunque nell'assumere un impegno comune ai fini del contrasto di questo fenomeno globale e di sfruttare quanto più il proprio margine di manovra.

Nell'ambito dell'identificazione delle vittime in Svizzera s'intravede ancora un potenziale di sviluppo. Con la Raccolta nazionale di file e valori hash sono state gettate le basi per un approccio sistematico nell'identificazione delle vittime. Tuttavia, le numerose piattaforme online quali i forum, le reti *peer-to-peer* per la condivisone di file, i social media e le reti anonime di interazione interpersonale continuano purtroppo a essere utilizzate abusivamente dai pedocriminali.

Con la creazione della Raccolta nazionale, la Svizzera ha compiuto un primo passo importante nel combattere la produzione, il commercio e la diffusione di immagini illegali nonché nel contrastare gli abusi sessuali ai danni di minori su Internet e il fenomeno della rivittimizzazione cui restano esposti. Con la propria partecipazione alla conferenza della Global Alliance against child sexual abuse online (Alleanza globale contro l'abuso sessuale di minori online), tenutasi il 6 dicembre 2012, la consigliera federale Simonetta Sommaruga ha confermato la volontà della Svizzera di sostenere la lotta a questo fenomeno a livello nazionale e internazionale.

6.2 Gruppi di lavoro nazionali

Nel 2014 lo SCOCI ha fatto parte di diversi gruppi di lavoro nazionali.

Insieme al commissariato Pedocriminalità/pornografia della Polizia giudiziaria federale, lo SCOCI è membro e promotore del gruppo di lavoro «Kindsmissbrauch» (abusi sui fanciulli), cui partecipano anche le autorità di perseguimento penale della Confederazione e dei Cantoni, Prevenzione svizzera della criminalità e organizzazioni di pubblica utilità operanti nel settore della protezione dell'infanzia.

Come negli anni precedenti, lo SCOCI ha partecipato anche nel 2014 ai lavori del programma nazionale «Giovani e media», sia in seno all'organo di gestione strategica, incaricato dell'elaborazione del programma, sia nel gruppo di progetto esecutivo «Monitoraggio della regolamentazione ed evoluzione dei media». Il programma si prefigge di aiutare bambini e giovani a utilizzare i nuovi media in modo sicuro, responsabile e adeguato alla loro età.

6.3 Collaborazione con i servizi della Confederazione

Alla criminalità su Internet sono applicabili quasi tutti i titoli del Codice penale. Tale aspetto trova conferma nella collaborazione multiforme portata avanti dallo SCOCI con diversi servizi all'interno dell'Amministrazione federale. In seno a fedpol, il Servizio collabora intensamente soprattutto con i commissariati Pedocriminalità/pornografia, Indagini Tecnologie dell'informazione e Inchieste mascherate della Polizia giudiziaria federale. Inoltre è in stretto contatto con la divisione principale di fedpol Cooperazione internazionale di polizia (CIP). Analogamente all'anno precedente, sono stati intensificati i contatti con vari servizi federali, quali la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), l'ambito direzionale Assistenza giudiziaria internazionale dell'Ufficio federale di giustizia (UFG), l'Autorità federale di vigilanza sui mercati finanziari (FINMA), l'Istituto federale della proprietà intellettuale (IPI), la Commissione federale delle case da gioco (CFCG), il Dipartimento federale degli affari esteri (DFAE) e la Rete integrata Svizzera per la sicurezza (RSS).

6.4 Scambio di esperienze con i Cantoni

Nell'anno in rassegna lo SCOCI ha intrattenuto diversi contatti con rappresentanti di vari corpi di polizia e pubblici ministeri cantonali. Gran parte di questi contatti sono stati allacciati nell'ambito di casi operativi in corso. Grazie a questi contatti, i Cantoni hanno potuto approfittare delle conoscenze specialistiche e della rete di contatti internazionale di cui dispongono i collaboratori dello SCOCI. Allo stesso modo, lo SCOCI ha potuto trarre vantaggio dalla conoscenza delle realtà locali, delle procedure consolidate tra forze di polizia e ministeri pubblici e delle conoscenze in materia forense presenti nei Cantoni.

Grazie all'attività di coordinamento svolta dallo SCOCI e all'efficiente collaborazione con i Cantoni, in diversi casi (cfr. cap. 5.3) è stato possibile impedire la distruzione delle prove da parte dei sospettati o avviare un procedimento penale sulla base di fatti segnalati dall'estero.

6.5 Collaborazione con organizzazioni non governative (ONG) e associazioni

Da diversi anni lo SCOCI collabora strettamente con l'ONG Action Innocence Genève (AIG) nella lotta contro la pedopornografia. Grazie al sostegno offerto da AIG, negli ultimi anni è stato possibile proseguire e approfondire il progetto per il monitoraggio delle reti *peer-to-peer*.

Lo SCOCI lavora inoltre a stretto contatto con l'associazione Stop Piracy allo scopo di segnalare alle competenti autorità di polizia e ai provider i negozi online fraudolenti che mettono in vendita prodotti di marca contraffatti.

Allo stesso modo, lo SCOCI mira a collaborare con l'associazione Swiss Internet Security Alliance (SISA) che raggruppa provider ed esperti in materia di sicurezza delle informazioni e ha come scopo quello di rendere il web svizzero un luogo libero dai malware.

6.6 Collaborazione con i provider svizzeri di accesso a Internet (ISP)

Dal 2007 è in vigore un accordo tra lo SCOCI e i principali provider svizzeri concernente il blocco di siti Internet contenenti materiale pedopornografico. Il blocco interessa esclusivamente i siti esteri che offrono il download di materiale raffigurante atti sessuali con fanciulli ai

sensi dell'articolo 197 capoversi 4 e 5 CP. I provider bloccano l'accesso a questi siti in virtù delle proprie condizioni generali di contratto e della loro etica aziendale e deviano gli utenti verso una cosiddetta *stop page*. A tal fine, lo SCOCI gestisce e mette a disposizione dei provider una lista costantemente aggiornata in cui sono riportati tra i 700 e i 1000 siti Internet.

Nell'ambito di questo progetto lo SCOCI collabora strettamente con Interpol. La lista allestita in Svizzera alimenta con un consistente apporto la lista «Worst-Of» di Interpol, sulla quale figurano i siti Internet che propongono materiale pedopornografico. Lo SCOCI si impegna ogni giorno nella ricerca di nuovi siti Internet contenenti materiale pedopornografico e integra costantemente la lista di Interpol, che è gestita in collaborazione con diversi Paesi.

6.7 Cooperazione internazionale

6.7.1 Europol

Dal 2011 lo SCOCI partecipa a diversi gruppi di lavoro nell'ambito dell'European Cybercrime Center (EC3). Il centro per la lotta contro la criminalità su Internet EC3, con sede all'Aia, fornisce sostegno operativo agli Stati membri dell'UE e agli Stati terzi e mette a disposizione le proprie conoscenze specialistiche e le proprie attività di analisi ai fini della conduzione di indagini comuni a livello europeo. Lo SCOCI intrattiene stretti contatti con l'EC3 e nell'anno in rassegna ha partecipato regolarmente a riunioni strategiche e operative organizzate da quest'ultimo. In tale contesto l'EC3 dà priorità alla lotta a fenomeni quali la criminalità su Internet in senso stretto, alle frodi sistematiche con le carte di credito e alla diffusione organizzata e a scopo di lucro di materiale pedopornografico.

Lo SCOCI partecipa al Focal Point (FP) CYBORG dell'EC3, specializzato nella lotta alla criminalità transfrontaliera su Internet in senso stretto e in particolare ai fenomeni di phishing, DDoS, botnet, hacking, ecc. Inoltre, insieme al commissariato Pedocriminalità/pornografia della Polizia giudiziaria federale, lo SCOCI è membro del FP TWINS incentrato sulla lotta contro la pedocriminalità su Internet.

6.7.2 Adesione della Svizzera alla Virtual Global Taskforce (VGT)

Il rapido sviluppo di Internet offre costantemente ai pedocriminali nuove possibilità per anticipare sempre di un passo le autorità di perseguimento penale e per commettere abusi su minori. La VGT è un'alleanza internazionale tra autorità di perseguimento penale, organizzazioni non governative ed economia privata finalizzata alla lotta agli abusi (sessuali) di minori su Internet e a fornire una risposta diretta al rapido sviluppo del web.

Grazie a queste sinergie, la VGT contribuisce a rendere Internet uno spazio più sicuro, consentendo di individuare e localizzare in tempi più brevi gli abusi, di aiutare i minori in difficoltà e di assicurare il perseguimento penale efficace dei pedocriminali.

Dal 2012 la Svizzera aderisce alla Global Alliance against child sexual abuse online (Alleanza globale contro l'abuso sessuale di minori online), fornendo così il proprio contributo nella lotta congiunta a tale fenomeno. Tra gli obiettivi che la Svizzera si era prefissata nell'ambito della cooperazione con la Global Alliance vi era l'adesione alla VGT. Nell'anno in rassegna è stato possibile realizzare tale obiettivo.

Immagine 1: Bruxelles, 13 maggio 2014: Thomas Walther, capo del commissariato SCOCI, sottoscrive la dichiarazione d'adesione della Svizzera alla Virtual Global Taskforce in presenza di Anthony L. Gardner, ambasciatore degli Stati Uniti presso l'Unione europea (a sinistra nella foto), di Roberto Balzaretti, ambasciatore svizzero presso l'UE (a destra) e di Ian Quinn, presidente della VGT (il secondo da sinistra).

Oltre alla Svizzera, hanno aderito alla VGT anche l'Australia, il Canada, la Colombia, la Corea, gli Emirati Arabi Uniti, l'Italia, la Nuova Zelanda, i Paesi Bassi, il Regno Unito, gli Stati Uniti d'America, Europol e Interpol.

Tra i membri del settore privato si annoverano: End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes network (ECPAT International), International Association of Internet Hotlines (INHOPE), National Center for Missing & Exploited Children (NCMEC), International Centre for Missing and Exploited Children (ICMEC), PayPal, Microsoft Digital Crimes Unit, World Vision, Blackberry, The Code, Kids Internet Safety Alliance (KINSA), NetClean, International Justice Mission e Telstra.

Maggiori informazioni concernenti la VGT sono disponibili sul sito www.virtualglobaltaskforce.com.

6.7.3 Global Alliance against Child Sexual Abuse Online

Su invito del commissario europeo Cecilia Malmström e del procuratore generale statunitense Eric Holder Jr., il 30 settembre 2014 i rappresentanti e gli esperti di oltre 40 Paesi hanno partecipato a Washington DC alla seconda conferenza ministeriale della Global Alliance against Child Abuse Online.

In occasione della conferenza ministeriale, i relatori rappresentanti del settore del perseguimento penale, dell'economia privata e delle organizzazioni non governative hanno presentato i successi ottenuti nei quattro ambiti principali d'interesse della Global Alliance (identificazione

delle vittime, identificazione e perseguimento degli autori del reato, sensibilizzazione, prevenzione del fenomeno della rivittimizzazione). Durante il suo discorso inaugurale, il procuratore generale statunitense Eric Holder Jr. ha affermato di essere orgoglioso dei successi e dei progressi raggiunti sin qui della Global Alliance. Dal 2012 sono già 54 i Paesi che vi hanno aderito e che combattono attivamente il fenomeno globale degli abusi di minori su Internet. Holder ha comunque affermato che non è il caso di cullarsi sugli allori, in quanto i rischi legati agli abusi di minori sono addirittura aumentati. In particolare, occorre dedicare la giusta attenzione alla pedopornografia su Internet, che continua a propagarsi incontrastata, contribuendo così a una perenne vittimizzazione dei minori vittime degli abusi. Holder è comunque consapevole che l'Alleanza da sola non è in grado di risolvere il problema della pedopornografia online, e va dunque considerata come uno strumento di supporto alle strutture e agli accordi già esistenti a livello internazionale.

La Global Alliance fissa gli obiettivi politici e operativi, lasciando tuttavia ai singoli Paesi la libertà di decidere come intendono attuarli e raggiungerli. Nel 2014 la Svizzera è stata in grado di raggiungere, o addirittura, superare i vari obiettivi che si era prefissata. Ciò le ha permesso di riscuotere un ampio apprezzamento a livello internazionale per l'impegno profuso nella lotta alla cibercriminalità. Il nostro Paese è stato ad esempio menzionato ed encomiato durante diversi eventi ed è riuscito nell'arco degli ultimi due anni a raggiungere un ruolo internazionale di primo piano nella lotta agli abusi di minori online.

Su iniziativa del premier britannico David Cameron e in sintonia con gli obiettivi della Global Alliance, tra il 10 e l'11 dicembre 2014 si è tenuto a Londra il vertice #WePROTECT Children Online Global Summit. Diversamente dalla Global Alliance, l'attenzione del #WePROTECT non è rivolta alle autorità di perseguimento penale, ma ai partecipanti dell'economia privata. Nel corso del summit, le aziende leader operanti nel settore delle tecnologie, oltre a dichiararsi disponibili a fornire il proprio contributo alla causa, hanno anche firmato insieme ai rappresentanti delle autorità di perseguimento penale e alle organizzazioni private uno «Statement of Action»[10].

6.7.4 FBI & Homeland Security

Alla luce del fatto che la maggior parte dei provider ha sede negli Stati Uniti e che questi ultimi ambiscono a una cooperazione intensa con Europol e i suoi Stati membri in materia di cibercriminalità, lo SCOCI lavora a stretto contatto con l'ufficio dell'attaché legale dell'FBI a Berna. Oltre allo scambio d'informazioni di polizia giudiziaria, lo SCOCI intrattiene uno scambio informale in merito alle migliori pratiche in materia di preservazione di dati presso i maggiori provider statunitensi. Allo stesso modo, le richieste degli Stati Uniti concernenti la preservazione di dati dei provider svizzeri sono trasmesse direttamente tramite l'attaché alla Centrale operativa di fedpol e trattate dallo SCOCI.

Lo SCOCI collabora infine strettamente con l'attaché dell'U.S. Immigration and Customs Enforcement (ICE) a Roma, collocato in seno al dipartimento Homeland Security. L'attaché garantisce in particolare i contatti con la divisione Cybercrime (appartenente allo stesso ICE), il cui direttore riveste attualmente la carica di presidente della VGT.

[10] Il documento può essere consultato in inglese sul sito: https://www.gov.uk/government/publications/weprotect-summit, ultima consultazione il 18 marzo 2015

7 Presenza nei mass media, attività didattica e conferenze

7.1 Presenza nei mass media

Nel 2014, le attività dello SCOCI hanno trovato ampia risonanza nei media. I collaboratori dello SCOCI hanno risposto a circa un centinaio di richieste da parte dei media.

Meritano une menzione particolare anche gli avvisi pubblicati dallo SCOCI per segnalare i pericoli legati a fenomeni criminali su Internet, in parte portati all'attenzione anche dei mass media e di altre organizzazioni partner come MELANI e Prevenzione svizzera della criminalità. Tali avvisi sono allestiti principalmente quando lo SCOCI osserva una certa frequenza di segnalazioni concernenti lo stesso fenomeno. Un ulteriore motivo per pubblicare un avviso può essere costituito inoltre da festività imminenti. Durante questi periodi si è infatti osservato che determinati fenomeni criminali sono più ricorrenti. Nel 2014 per esempio, lo SCOCI ha pubblicato un avviso concernente la diffusione di malware allegati a e-mail, con presunte fatture insolute inviate da negozi online, fornitori di servizi di telecomunicazione, ecc. o ancora un avviso riguardante l'aumento dei tentativi di truffa e dei finti negozi online nel periodo prenatalizio.

Molte case editrici svizzere hanno creato apposite redazioni online incaricate di approfondire e divulgare i temi legati a Internet. Inoltre negli ultimi anni, diverse personalità pubbliche sono diventate vittime di cibercriminali. Da notare infine che i profili dello SCOCI presenti sui social media, in particolare su Twitter, vengono consultati attivamente dalle redazioni online svizzere e internazionali. Queste ultime diffondono gli avvisi dello SCOCI utilizzando i propri canali e facendo spesso riferimento al modulo di comunicazione dello SCOCI.

7.2 Social media

Dal 2013 lo SCOCI ha aperto un proprio profilo sulle reti sociali Facebook (www.facebook.com/ScociSvizzera) e Twitter (@KOBIK_Schweiz). Questi strumenti fungono da rapido canale di diffusione degli avvisi da parte dello SCOCI per allertare la popolazione svizzera sulle tipologie di truffa maggiormente segnalate o sui possibili attacchi con software nocivi. I riscontri ricevuti finora sono assolutamente positivi.

Dopo circa un anno, le pagine dello SCOCI in tedesco, in francese e in italiano di Facebook contava già 3576 «Mi piace» e il profilo multilingue su Twitter 487 *follower*.

7.3 Attività didattica e conferenze

Nell'anno in rassegna i collaboratori dello SCOCI hanno partecipato a numerose conferenze, convegni internazionali e corsi di formazione. Hanno colto l'occasione, oltre che per perfezionare ulteriormente le proprie conoscenze, per curare i contatti e scambiare informazioni con partner ed esperti nell'ambito della criminalità su Internet, della protezione dell'infanzia e dell'identificazione delle vittime.

I collaboratori dello SCOCI hanno inoltre partecipato a diversi eventi in qualità di istruttori, tra

i quali un corso della durata di due giorni organizzato dalla Svizzera e condotto da due collaboratori dello SCOCI per l'Accademia di polizia dell'Europa centrale MEPA in materia di Open Source Intelligence su Internet. I collaboratori dello SCOCI hanno inoltre partecipato a più di un centinaio di altri eventi in qualità di esperti, istruttori e specialisti.

Il 13 novembre 2014 si è tenuto il terzo «Forum Cybercrime ministeri pubblici - SCOCI», una giornata incentrata sulla collaborazione tra i pubblici ministeri e lo SCOCI in materia di cibercriminalità. Esperti a livello internazionale hanno fornito ai partecipanti una panoramica concreta della lotta internazionale contro la criminalità su Internet. È stato inoltre presentato il laboratorio mobile utilizzato da Interpol per identificare le vittime di rappresentazioni pedopornografiche e, in tale ambito, è stata offerta l'opportunità di svolgere esercitazioni pratiche. Durante la successiva tavola rotonda è stata discussa la revisione della LSCPT[11]. Al forum hanno partecipato un centinaio di persone.

Il giorno successivo, ovvero il 14 novembre 2014, si è svolta a Berna la giornata dell'identificazione delle vittime, organizzata dallo SCOCI con la partecipazione di Interpol, destinata ai collaboratori dei corpi di polizia cantonali e delle città. Tale giornata è il risultato diretto dell'adesione della Svizzera alla Global Alliance against Child Sexual Abuse Online (cfr. cap. 6.7.3) e delle misure e degli obblighi ad essa connessi. Tali misure prevedono tra l'altro sforzi maggiori per identificare le vittime della pedopornografia e garantire loro la giusta protezione, assistenza e sostegno. A tale scopo è stato necessario accertare se è possibile ricorrere a sinergie tra la classificazione delle immagini nella Raccolta nazionale di file e valori hash e l'identificazione delle vittime in collaborazione con la banca dati ICSE messa a disposizione da Interpol. In un secondo tempo verrà elaborato, insieme ai Cantoni, un piano di cooperazione e di identificazione delle vittime nell'ottica di una ripartizione dei compiti entro la fine del 2016.

In relazione alla Raccolta nazionale, lo SCOCI ha organizzato nel corso di tutto l'anno formazioni sulla categorizzazione di materiale fotografico e video per inquirenti di diversi corpi di polizia svizzeri e rappresentanti di imprese private incaricate dai ministeri pubblici cantonali di effettuare le analisi forensi del materiale sequestrato e di procedere alla categorizzazione. Tali formazioni hanno lo scopo di assicurare che le raffigurazioni di pornografia vietata vengano categorizzate nella Raccolta nazionale seguendo i medesimi criteri a livello nazionale garantendone così la massima qualità. Durante il corso, della durata di due mezze giornate, i partecipanti vengono introdotti anche nell'ambito giuridico e hanno la possibilità di categorizzare materiale fotografico e di discutere i casi più controversi con i formatori.

[11] Legge federale del 6 ottobre 2000 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni; RS 780.1

8 Interventi politici a livello federale

Mozione 14.3022: Pornografia infantile. Vietare le immagini di bambini nudi – Rickli Natalie Simone, 3 marzo 2014

Interpellanza 14.3204: Consenso del gruppo di lavoro AGUR 12. Ulteriori passi – Gutzwiller Felix, 20 marzo 2014

Interpellanza 14.3250: Violenza giovanile. Cosa fare? – Grin Jean-Pierre, 21 marzo 2014

Mozione 14.3288: Rendere l'usurpazione d'identità un reato penale a sé stante – Comte Raphaël, 21 marzo 2014

Mozione 14.3367: Combattere il sexting – Amherd Viola, 8 maggio 2014

Postulato 14.3655: Definire la nostra identità digitale e identificare le soluzioni per proteggerla – Derder Fathi, 20 giugno 2014

Mozione 14.3665: Integrare l'articolo 260bis CP (art. 187 CP, "Atti sessuali con fanciulli") – Commissione degli affari giuridici CN, 14 agosto 2014

Mozione 14.3666: Articolo 198 CP. Reato perseguibile d'ufficio in determinati casi – Commissione degli affari giuridici CN, 14 agosto 2014

Interpellanza 14.3888: Lotta internazionale alla propaganda dell'odio su Internet – Naef Martin, 25 settembre 2014

Mozione 14.3905: Garantire l'identificazione degli autori di messaggi d'odio su Internet – Schwaab Jean Christophe, 25 settembre 2014

Postulato 14.3908: Internet. Tolleranza zero nei confronti dell'intolleranza – Tornare Manuel, 25 settembre 2014

Postulato 14.3962: Migliorare l'assistenza amministrativa internazionale in caso di reati contro minori commessi in Internet – Müller-Altermatt Stefan, 26 settembre 2014

Postulato 14.3963: La legislazione sulla protezione dei dati protegge anche i pedofili? – Müller-Altermatt Stefan, 26 settembre 2014

Interpellanza 14.3969: Competenze mediali contro le campagne di odio, 26 settembre 2014

Interrogazione 14.5175: Prendre en compte les cyberrisques liés à la plate-forme Tumblr – Schmid-Federer Barbara, 12 marzo 2014 (non disponibile in italiano)

9 Sviluppi futuri

Il numero delle segnalazioni registrate dallo SCOCI dipende dalla propensione della popolazione a segnalare contenuti sospetti su Internet. Tali comunicazioni consentono allo SCOCI di avere una migliore panoramica della cibercriminalità in Svizzera. Tuttavia, non è che la punta dell'iceberg poiché la maggior parte delle attività illegali su Internet spesso sono sconosciute al pubblico svizzero. Le pagine seguenti si basano su informazioni liberamente accessibili, nonché sulle conoscenze acquisite dallo SCOCI nel corso dei suoi undici anni di attività.

Attacchi di phishing e miglioramento delle tecniche di truffa

Dalla comparsa delle prime tipologie di truffa tramite posta elettronica, i cibercriminali hanno affinato le loro tecniche dando prova di grande duttilità. Oggi i truffatori sono in grado di utilizzare con grande facilità strumenti informatici per rendere difficile la propria identificazione, come ad esempio la rete TOR, i servizi VPN e i *bulletproof hosting provider.*

Anche in futuro la Svizzera, proprio per la sua ricchezza e l'elevato tasso di penetrazione di Internet, continuerà a essere un bersaglio privilegiato degli attacchi di phishing, ovvero la categoria degli attacchi che sembrano provenire da un istituto o persona nota e con i quali si intrattiene una relazione. Negli attacchi di *spear phishing* vengono creati siti di phishing molto professionali e identici ai siti ufficiali; spesso questi siti sono riconoscibili come tali soltanto da persone esperte. Per evitare di essere identificati dai sistemi antivirus e firewall, i cibercriminali salvano le pagine su conti piratati e non, ad esempio su un *cloud server* (*Dropbox*, *Google Drive*, ecc). In alternativa, i cibercriminali iniettano un codice dannoso all'interno di un sito affidabile al fine di reindirizzare i visitatori sul loro sito di phishing. A tale proposito, si prevede aumento de i casi di uso abusivo dei nuovi domini di primo livello (p. es. *support, .email,* ecc.) e di certificati di sicurezza scaduti o rubati[12].

L'onnipresenza di Internet e la propensione a una condivisione indiscriminata delle proprie informazioni (status sulle reti sociali, indicazioni di località, di relazioni sentimentali, ecc.) è una vera e propria manna per i cibercriminali. Questi ultimi accumulano grandi quantità di dati e di informazioni che si riveleranno utili alla preparazione di truffe vieppiù sofisticate a scapito di cittadini, ma anche di piccole, medie e grandi imprese. Alla luce di tali considerazioni, si prevede un aumento dei tentativi di usurpazione d'identità associato a una crescita dei casi di truffa.

L'economia sotterranea del Darknet

La crescente velocità di Internet, la diffusione e la popolarità di alcune tecniche di anonimizzazione incoraggiano i cibercriminali a utilizzare maggiormente i servizi del Darknet. L'operazione Onymous[13], condotta lo scorso 6 novembre da Europol e dall'FBI in cooperazione con 16 Paesi europei tra i quali la Svizzera, ha mostrato l'elevato tasso di penetrazione di tali servizi tra la popolazione. La maggior parte del commercio e del traffico illeciti migra verso il Darknet dove è possibile acquistare, in maniera più o meno anonima, malware, dati di carte di credito oppure noleggiare reti bot per commettere attacchi DDoS[14]. Inoltre, alcune piattaforme del web nascosto si affermano come luogo di scambio di materiale pedopornografico, di acquisto o vendita di prodotti stupefacenti o di qualsiasi altro bene vietato. Tali attività sono agevolate

[12] http://www.csoonline.com/article/2687132/social-engineering/recently-introduced-tlds-create-new-opportunities-for-criminals.html, ultima consultazione il 18 marzo 2015

[13] https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network, ultima consultazione il 18 marzo 2015

[14] Trend Micro, *Deepweb and Cybercrime*, 2013, pag. 9 segg.

dalla diffusione di denaro virtuale, come il Bitcoin, o di metodi di pagamento a distanza che permettono trasferimenti di denaro più anonimi e discreti.

Alcune organizzazioni criminali non si limitano più soltanto a vendere le proprie prestazioni, ma offrono ai propri «clienti»[15] dei veri e propri «servizi post-vendita», fornendo un'assistenza 24 ore su 24. Tra le prestazioni offerte vi è ad esempio la possibilità di noleggiare delle reti bot per l'invio di massa di spam o diffondere *trojan,* beneficiando di un supporto tecnico in caso di problemi. I criminali sviluppano così un nuovo business model*,* conosciuto come *Crime-as-a-Service,* in grado di offrire servizi innovativi e a prezzi concorrenziali. Oggigiorno la cibercriminalità non è più riservata agli esperti, ma è alla portata di tutti coloro che possono acquistare i servizi di cui sopra. Tutto lascia intendere che tale tendenza andrà ad accentuarsi ulteriormente nel corso dei prossimi anni.

Malware sui telefoni cellulari

In futuro gli smartphone e altre categorie di tablet rappresenteranno una fetta di mercato sempre più considerevole rispetto ai computer tradizionali[16]. Alcuni utenti preferiscono già ora lo smartphone al computer, in quanto esso, grazie alla sua estrema portabilità, permette di restare sempre connessi. Se l'utente medio ha compreso l'importanza di possedere un antivirus e di aggiornare costantemente i programmi sul proprio computer, lo stesso non si può dire per il grado di sensibilizzazione nei confronti dei rischi e pericoli legati ai dispositivi portatili. I cibercriminali traggono profitto da tali lacune sviluppando un numero sempre crescente di software dannosi per i dispositivi portatili che permettono, ad esempio, di carpire i dati dal cellulare, oppure di inviare, all'insaputa del proprietario, dei messaggi a dei servizi a pagamento. I malware, finora circoscritti al computer, fanno ora dunque la loro comparsa anche sui dispositivi portatili. È il caso ad esempio del *police ransomware* Reveton per il quale, l'anno scorso, è stata per la prima volta identificata una versione appositamente creata per Android[17]. Il mondo del denaro virtuale è altrettanto sconvolto dai primi software nocivi per smartphone di trasformare uno cellulare in un generatore di bitcoins (*bitcoin mining*) senza che il proprietario se ne accorga[18].

In Svizzera tale fenomeno non è ancora diffuso, ma non si può escludere che in futuro tale situazione non possa cambiare.

[15] Europol, *The Internet Organized Crime Threat Assessment* (iOCTA) *report*, 2014, pag. 11

[16] http://www.forbes.com/sites/louiscolumbus/2013/09/12/idc-87-of-connected-devices-by-2017-will-be-tablets-and-smartphones/, ultima consultazione il 18 marzo 2015

[17] http://blog.trendmicro.com/trendlabs-security-intelligence/ransomware-moves-to-mobile/, ultima consultazione il 18 marzo 2015

[18] https://blog.lookout.com/blog/2014/04/24/badlepricon-bitcoin/, ultima consultazione il 18 marzo 2015

Vecchie vulenarabilità, *cloud* e nuovi sistemi di pagamento

Il 2014 ha visto la comparsa di diverse vulnerabilità critiche (p. es. *Heartbleed*[19] e *Shellschock*[20]) e di alcune lacune nei protocolli datati (p. es. POODLE[21]) che permettono ai criminali di accedere ai server di messaggeria per creare e gestire delle reti bot[22]. In futuro occorrerà attendersi a tali tipologie di attacco ed essere in grado di reagire prontamente.

Data l'enorme quantità di informazioni contenute, i servizi *cloud* sono bersagli privilegiati da parte dei criminali. Lo scandalo del pirataggio e del furto di immagini dagli account *iCloud* di alcune star americane[23] mostra le conseguenze drammatiche che una protezione insufficiente di un account può avere. I cibercriminali, attirati dalla grande quantità di informazioni personali, continueranno anche in futuro ad attaccare i *cloud server*. Da parte loro, gli utenti devono essere coscienti di tali minacce e adottare le misure necessarie per mettere al sicuro i propri dati, come ad esempio la verifica in due passaggi e la scelta di password non triviali.

In America, la corsa ai nuovi sistemi di pagamento senza contanti è già iniziata: le società stanno eseguendo importanti investimenti per creare il portafoglio digitale del futuro, come ad esempio *Apple Pay*, *Google Wallet* e *Cashcloud*. Come ogni nuova tecnologia, tali sistemi di pagamento susciteranno l'interesse dei criminali, motivo per cui i consumatori dovranno imparare ad utilizzarli nel modo più sicuro possibile.

The Internet of Things

Cisco stima che il numero dei dispositivi connessi a Internet raggiungerà i 50 miliardi nel 2020[24]. Oltre a computer, tablet e smartphone, Internet connetterà ogni tipo di oggetto, ad esempio docce, cucine, lampade, termostati, automobili, ecc.; gli esperti parlano di *Internet of Things*[25], l'Internet delle cose. C'è da scommettere che pure tale fenomeno susciterà le brame del mondo della cibercriminalità. Anche in questo campo, occorrerà sensibilizzare il pubblico riguardo alle opportunità e ai rischi delle nuove tecnologie nonché a un uso appropriato di queste ultime.

---

[19] http://heartbleed.com, ultima consultazione il 18 marzo 2015

[20] http://www.troyhunt.com/2014/09/everything-you-need-to-know-about.html, ultima consultazione il 18 marzo 2015

[21] https://access.redhat.com/articles/1232123, ultima consultazione il 18 marzo 2015

[22] SWITCHcert, rapporto sulle tendenze attuali nell'ambito della IT-Security e IT-Privacy, novembre 2014, pagg. 1-2

[23] http://time.com/3247717/jennifer-lawrence-hacked-icloud-leaked/ ultima consultazione il 18 marzo 2015

[24] SWITCHcert rapporto sulle tendenze attuali nell'ambito della IT-Security e IT-Privacy, ottobre 2014, pagg. 4-5

[25] http://postscapes.com/internet-of-things-examples/, ultima consultazione il 18 marzo 2015