Lo spam nel mese di Aprile 2014

Tat'jana Šerbakova

Marija Vergelis

Sommario

Le peculiarità del mese

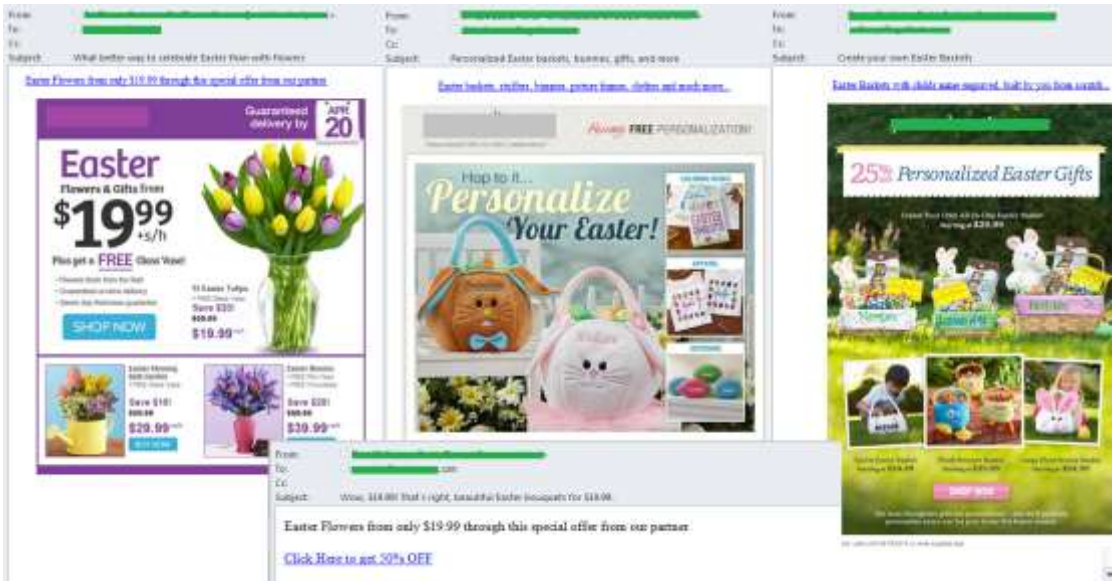
Nel mese di aprile, i tradizionali mailing di massa "festivi", correlati alle tematiche suggerite dalle più importanti ricorrenze stagionali, sono stati in gran parte dedicati all'imminente celebrazione della Pasqua. I classici temi connessi a tale festività sono stati ampiamente "sfruttati" non solo dagli spammer intenti a reclamizzare, come al solito, ogni genere di prodotti e servizi, ma anche dai sempre più temibili ed agguerriti truffatori e malintenzionati della Rete, i quali hanno indirizzato verso le e-mail box degli utenti Internet un elevato numero di false notifiche relative ad improbabili vincite realizzate mediante inesistenti lotterie online, così come gli abituali messaggi di posta nocivi, camuffati in veste di innocue e variopinte cartoline elettroniche di auguri, preposte, tuttavia, a recapitare nelle caselle di posta elettronica degli utenti un'ampia varietà di insidiosi programmi malware.

Lungo tutto l'arco del mese di aprile, inoltre, i truffatori della Rete hanno ugualmente condotto massicce campagne di spam volte a diffondere proposte di natura finanziaria, imperniate sull'opportunità di poter realizzare consistenti guadagni mediante l'acquisizione di azioni riconducibili ad una società farmaceutica statunitense; nella circostanza, gli spammer che hanno messo in atto tale frode hanno applicato il classico schema identificato con il termine "pump and dump", che tradotto letteralmente, significa in italiano "pompa e sgonfia", con riferimento al valore progressivamente assegnato, in maniera artificiale, ai titoli azionari oggetto di speculazione. Sono stati inoltre da noi individuati, all'interno del traffico di posta elettronica di aprile 2014, numerosi mailing di spam, particolarmente estesi, organizzati con il preciso intento di pubblicizzare i servizi offerti da vari istituti medici e da un considerevole numero

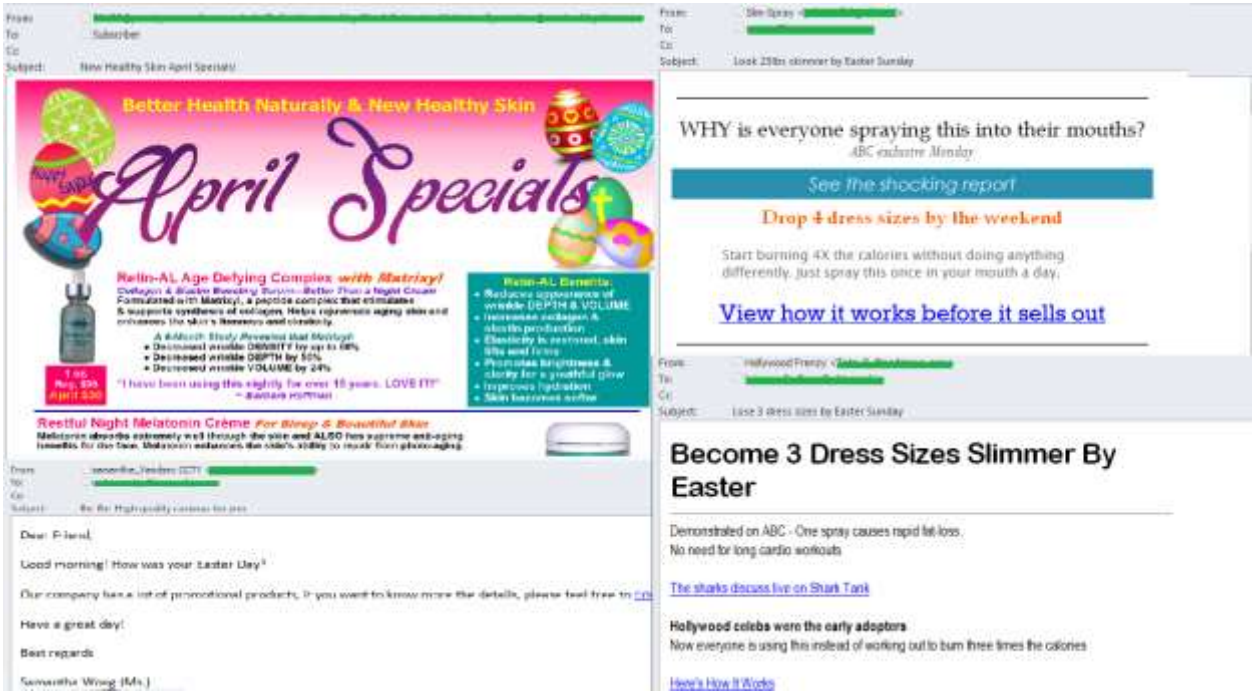
di cliniche odontoiatriche. I flussi di spam che hanno caratterizzato il mese qui preso in esame sono stati ugualmente contraddistinti da ripetute campagne di spam allestite per reclamizzare sia certi metodi di lotta da adottare nei confronti di determinate "cattive abitudini", dannose per la salute, sia trattamenti curativi e riabilitativi specificamente dedicati alle persone dipendenti da droghe od alcool.

Lo spam di Pasqua

Pasqua rappresenta indubbiamente una delle principali festività religiose dell'anno, sia per il mondo di fede ortodossa che per quello di professione cattolica; per tale motivo, credenti di tutto il mondo celebrano tale sentita ricorrenza con particolare trasporto, intensità e solennità. Ogni anno, tuttavia, alla vigilia dell'importante festività, le caselle di posta elettronica degli utenti della Rete vengono puntualmente sommerse da un'elevata quantità di messaggi di spam ispirati alle più classiche tematiche pasquali. Nel corso del mese di aprile, ad esempio, all'interno del segmento anglofono dello spam mondiale, ci siamo imbattuti nei tradizionali mailing di massa organizzati nell'ambito delle cosiddette partnership "floreali", ovvero quei programmi di partenariato dediti alla vendita online di articoli e composizioni floreali, soprattutto alla vigilia di festività particolarmente significative; è di particolare interesse osservare come la composizione dei messaggi di spam distribuiti attraverso tali campagne rimanga in pratica del tutto invariata da un anno all'altro. I flussi di spam di aprile hanno inoltre recato nelle e-mail box degli utenti dei client di posta elettronica numerose proposte commerciali relative alla possibilità di personalizzare gli articoli commercializzati in Rete in occasione delle festività pasquali.



Nel periodo oggetto del presente report, gli spammer non si sono neppure dimenticati di pubblicizzare svariati prodotti per il dimagrimento, al pari di specifici prodotti anti-età. Le offerte commerciali relative a preparati ed articoli di varia natura e formato - più o meno "miracolosi" - volti ad ottenere una rapida diminuzione del peso corporeo, oppure attenuare l'antiestetico effetto dovuto alla presenza di rughe sul volto, sono state in genere presentate ai destinatari delle e-mail di spam con tanto di variopinte decorazioni e simbologie pasquali, ed hanno spesso richiamato esplicitamente la denominazione della festività di Pasqua sia nell'oggetto che nel testo di volta in volta presente nel corpo del messaggio di posta.

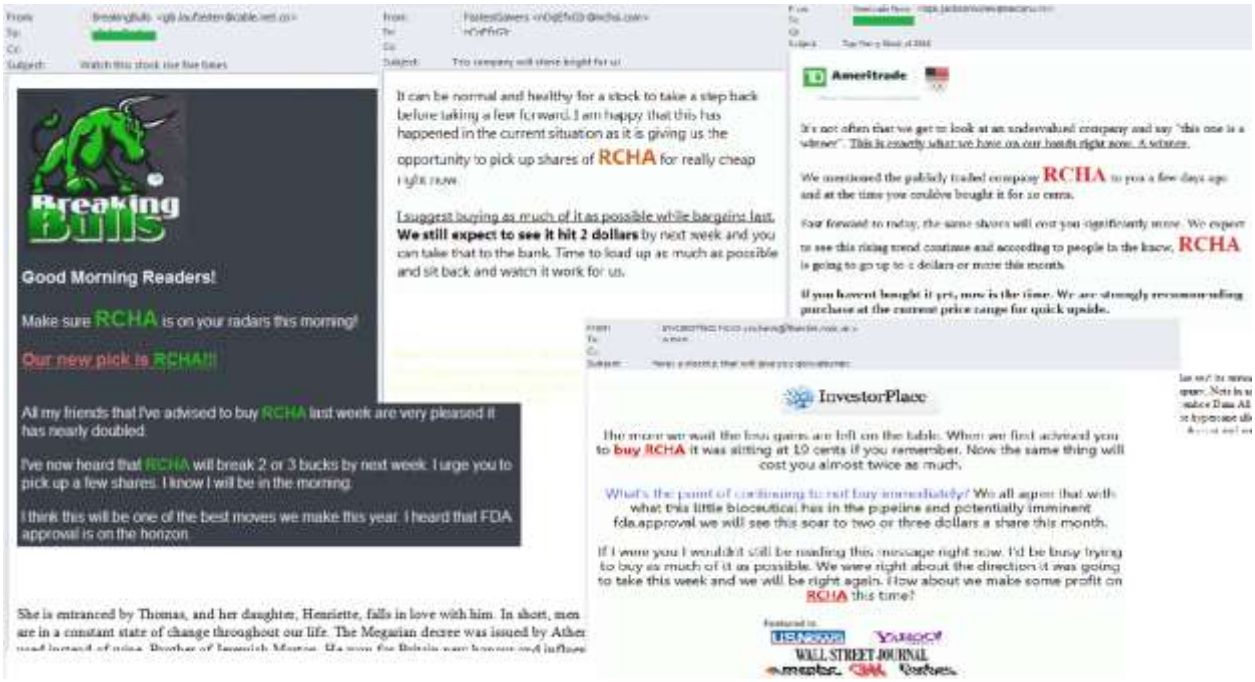


Anche per ciò che riguarda, nello specifico, le campagne di spam fraudolento recanti ai destinatari dei messaggi indesiderati improbabili notifiche di vincite a lotterie online del tutto inesistenti, abbiamo a più riprese rilevato come tali mailing di massa siano stati ugualmente "dedicati" dagli spammer, in maniera piuttosto evidente, alla ricorrenza pasquale. Come si può vedere negli screenshot esemplificativi qui riportati, il nome della solenne festività religiosa celebrata nella stagione primaverile è stato di frequente utilizzato dagli spammer nel testo presente nel campo riservato all'oggetto di tali e-mail; gli auguri inseriti all'inizio del testo, inoltre, avevano il preciso compito di convincere in maniera inequivocabile il destinatario dell'e-mail riguardo alle buone e corrette intenzioni dell'autore del messaggio.

«Guadagnare» con le azioni

Nello scorso mese di aprile abbiamo osservato, all'interno dei flussi e-mail globali, il propagarsi di una nuova ondata di una particolare forma di spam, abitualmente definita, come abbiamo visto nella parte introduttiva del nostro report, con la colorita espressione "pump and dump". Gli autori di tali mailing di massa sono soliti inviare, ai destinatari dei messaggi di posta, allettanti e-mail attraverso le quali viene offerta la "ghiotta" opportunità di poter acquistare, ad un prezzo estremamente contenuto, le azioni di

qualche società; il valore di tali azioni, secondo le mirabolanti promesse fatte dagli spammer, sarebbe poi inevitabilmente destinato a crescere in maniera sensibile, entro breve tempo. Ne consegue che la domanda relativa alle azioni della società di volta in volta oggetto di speculazione cresce rapidamente, in modo vertiginoso; il prezzo dei titoli azionari in causa - inizialmente a bassa capitalizzazione - lievita pertanto in maniera artificiale, raggiungendo vette particolarmente elevate. E' esattamente a questo punto che i truffatori della Rete iniziano ad effettuare la vendita dei titoli in loro possesso, precedentemente acquisiti. In tal modo, ovviamente, il prezzo delle azioni in questione scende con altrettanto notevole rapidità, mentre gli investitori, subdolamente raggirati dai malintenzionati, si ritrovano ben presto, nelle loro mani, titoli azionari quasi equivalenti a carta straccia, perdendo di fatto le somme di denaro, più o meno cospicue, investite in precedenza. In genere, per mettere in pratica tale schema fraudolento, i truffatori scelgono società poco conosciute, i cui titoli vengono di solito scambiati nell'ambito di mercati azionari di secondo piano. In aprile, le speculazioni finanziarie messe in atto dai malfattori della Rete si sono concentrate in particolar modo su Rich Pharmaceuticals (RCHA), società farmaceutica statunitense.

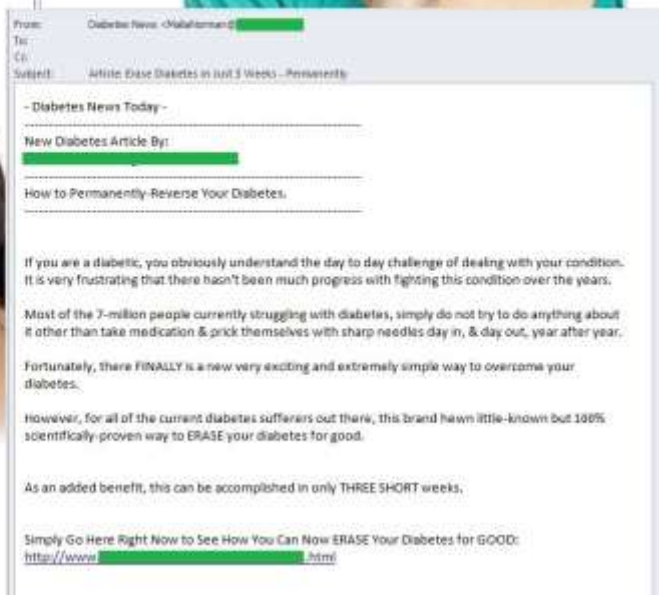


Le campagne di spam riconducibili alla tipologia "pump and dump", da noi rilevate nel traffico di posta elettronica del mese qui analizzato, sono state condotte a nome di varie società fornitrici di servizi nel settore degli investimenti finanziari, specializzate nella vendita di titoli azionari a potenziali investitori. Nella circostanza, nel tentativo di conferire a tali messaggi un aspetto di legittimità ed attendibilità, i truffatori si sono avvalsi del logo societario di compagnie realmente esistenti, inserendo il nominativo delle società prese di mira direttamente nel campo <From>, riservato al mittente dell'e-mail, nonostante gli indirizzi di posta elettronica introdotti in tale campo non risultassero poi per nulla simili a quelli ufficiali. Per cercare di eludere o perlomeno complicare le abituali operazioni di rilevamento compiute dai filtri antispam, nell'occasione gli spammer hanno fatto ricorso a particolari elaborazioni grafiche, immettendo ugualmente del testo "spazzatura" nella parte finale del messaggio.

Gli spammer a salvaguardia della salute

Nel periodo oggetto del nostro consueto resoconto mensile dedicato al fenomeno spam, i messaggi e-mail indesiderati riconducibili alla sfera medica sono risultati essere principalmente dedicati ad un

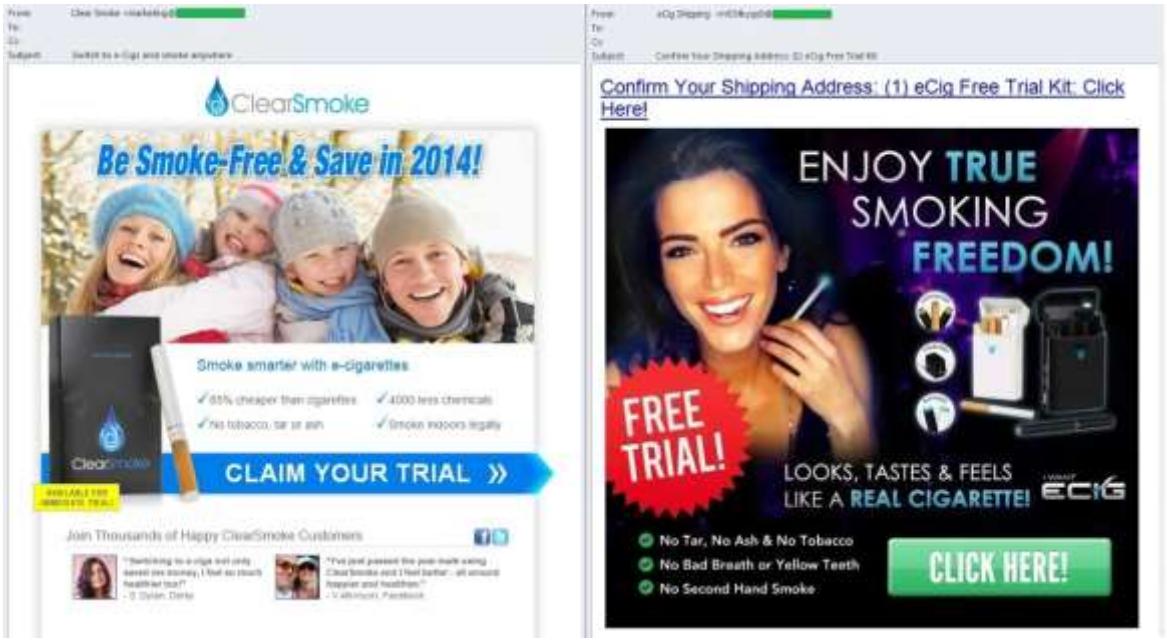
considerevole numero di offerte e proposte relative al trattamento di specifiche malattie. Così, ad esempio, attraverso tali flussi di spam sono state diffuse molteplici proposte per liberarsi definitivamente dalla calvizie, risolvere i problemi derivanti dal malfunzionamento della vescica urinaria, sottoporsi ad esami medici completi, sconfiggere per sempre il diabete, l'artrite ed altre patologie. La maggior parte di tali messaggi è stata in genere elaborata in veste di accurati file grafici, contenenti collegamenti ipertestuali principalmente preposti a condurre i destinatari delle e-mail verso siti web (spesso monopagina) appositamente allestiti dagli spammer, in cui si elencavano in dettaglio i vari servizi offerti in campo medico, nonché le cliniche specializzate nell'effettuazione dei suddetti trattamenti ed interventi; di frequente, poi, si proponevano addirittura dettagliate tabelle comparative riguardo ai prezzi proposti dai vari istituti. E' inoltre di particolare interesse osservare come tutti i messaggi di spam "medico" in causa siano stati inviati tramite indirizzi di posta elettronica registrati presso domini "effimeri", di recentissima creazione.



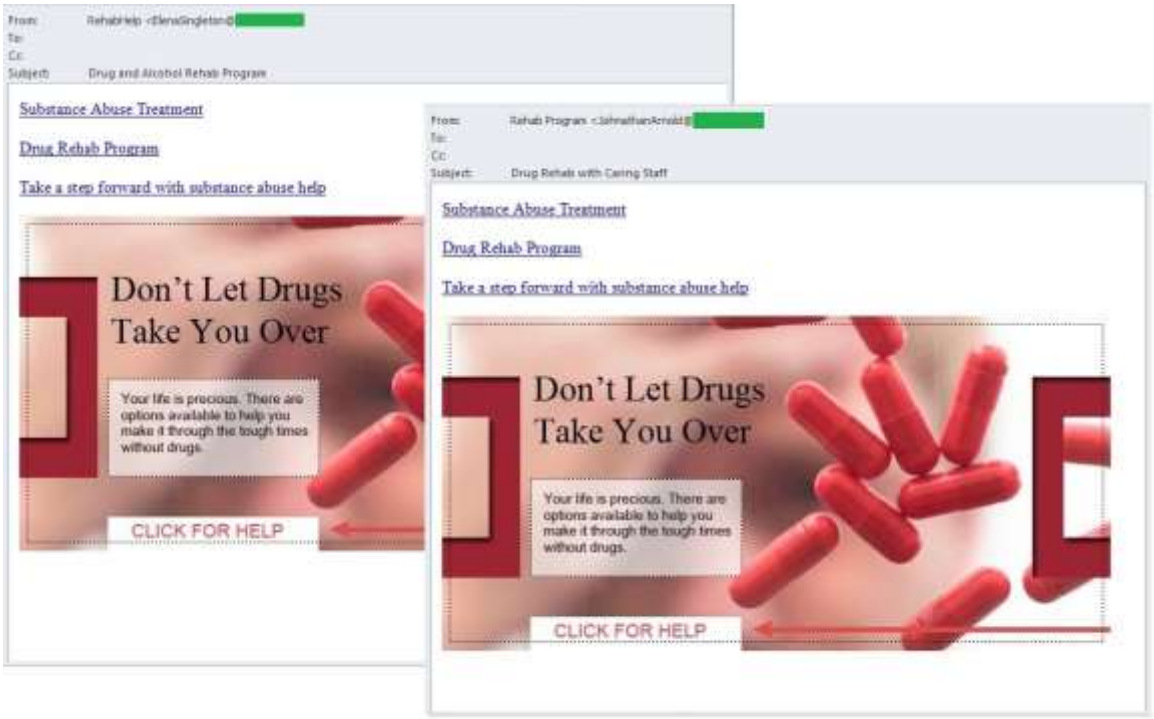
Rileviamo, infine, come le cliniche odontoiatriche, attraverso i capillari canali dello spam, abbiano attivamente pubblicizzato, nel corso del mese di aprile 2014, le prestazioni offerte riguardo all'esecuzione di impianti dentali a costi decisamente contenuti, realizzati con materiali resi disponibili da vari produttori.

Gli spammer contro le abitudini dannose

Numerose campagne di spam allestite durante il periodo oggetto della nostra analisi hanno offerto al (tuttora) vasto pubblico dei fumatori l'opportunità di poter superare la dipendenza nei confronti della nicotina, passando, nella circostanza, all'utilizzo delle sigarette elettroniche. Cliccando sul link appositamente inserito nel corpo di tali messaggi di posta, i destinatari delle e-mail sarebbero giunti sul sito web relativo al negozio online pubblicizzato attraverso il mailing di massa, dove il potenziale utente dedito al fumo, secondo le intenzioni degli spammer, avrebbe potuto effettuare l'ordine del "surrogato" elettronico proposto, in qualsiasi quantità e di qualsiasi gusto. Nel testo dei messaggi di spam in questione venivano ugualmente illustrati tutti i vantaggi, in termini di salute della persona, derivanti dall'utilizzo delle sigarette elettroniche, rispetto agli analoghi e tradizionali prodotti contenenti nicotina.

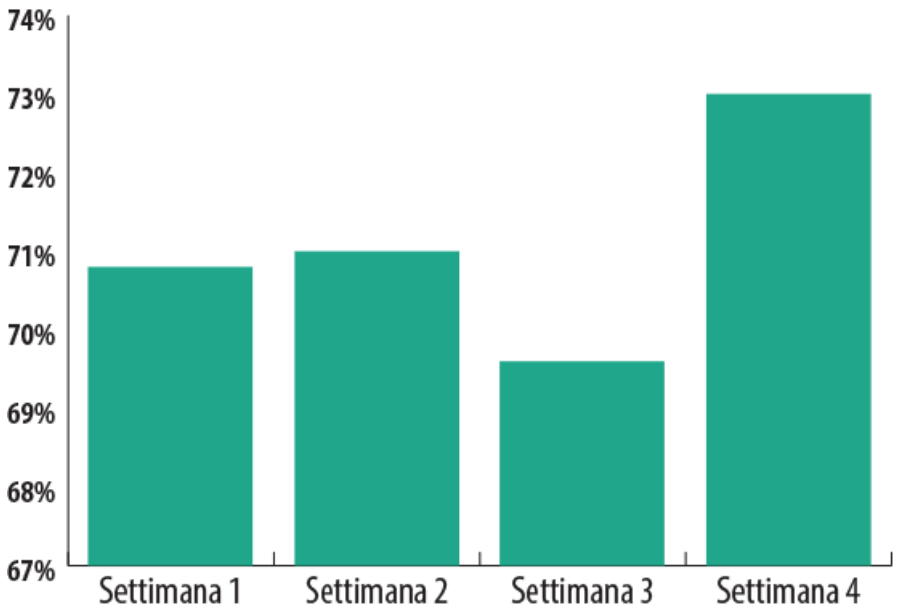


Oltre alla lotta anti-fumo, gli spammer hanno proposto ai destinatari dei messaggi riconducibili a tale particolare tipologia la partecipazione a specifici programmi di riabilitazione dedicati alle persone afflitte da dipendenza nei confronti di alcool e narcotici. Questo singolare genere di e-mail di spam, recante le suddette proposte, è risultato provenire da indirizzi di posta elettronica continuamente mutevoli, registrati presso domini web appena istituiti. I collegamenti ipertestuali presenti nei messaggi in causa avevano il compito di condurre gli utenti verso appositi siti Internet - in genere composti da un'unica pagina web - contenenti varie offerte relative ai più disparati servizi legati alla sfera medica, non obbligatoriamente correlati alle tematiche inerenti al trattamento della dipendenza nei confronti di droghe ed alcool.



Le statistiche

Quota di spam nel traffico di posta elettronica



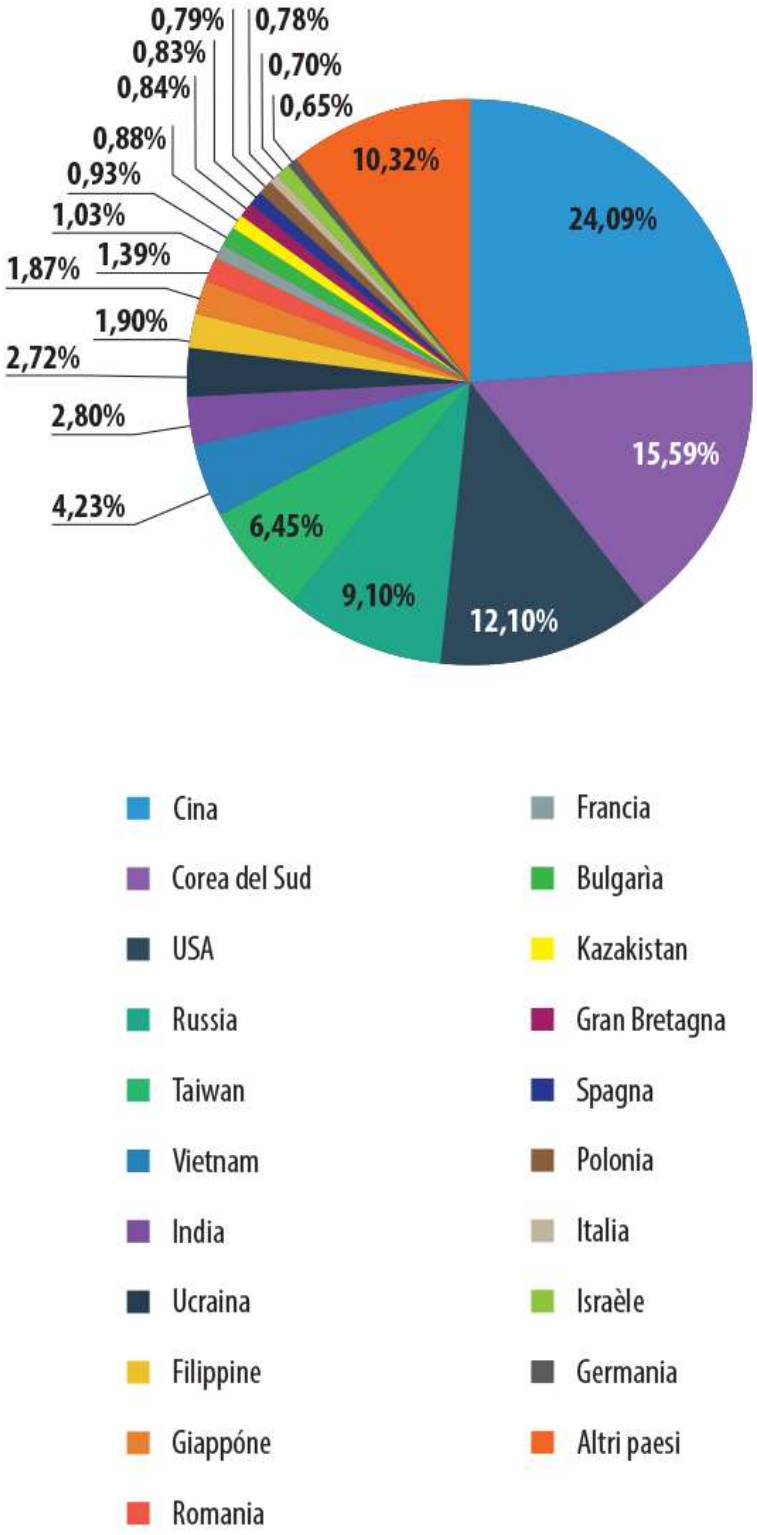
Quote di spam rilevate settimanalmente all'interno del traffico di posta elettronica

Nel mese oggetto del presente report, la quota inerente ai messaggi "spazzatura" rilevati nel traffico globale di posta elettronica ha fatto registrare un incremento del 7,6% rispetto all'analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 71,1% del volume complessivo di messaggi e-mail circolanti in Rete. L'indice percentuale più elevato è stato osservato nell'ultima settimana di aprile (73%); la quota di spam più contenuta è stata invece rilevata, all'interno dei flussi e-mail mondiali, nella penultima settimana del mese qui analizzato (69,6%).

Ripartizione geografica delle fonti di spam

Rispetto all'analogo rating del mese precedente, traspare in tutta evidenza come, all'interno della speciale graduatoria "globale" delle fonti di spam - relativa ai paesi dal cui territorio, nel corso del mese di aprile 2014, sono state distribuite in Rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura" - siano intervenuti significativi cambiamenti, qui di seguito descritti. Le variazioni di maggior rilievo riguardano, in particolar modo, la TOP-3, ovvero il "podio" virtuale del ranking da noi stilato. Così come nello scorso mese di marzo, tuttavia, la leadership della classifica analizzata nel presente capitolo del nostro report mensile dedicato al fenomeno spam è andata ad appannaggio della Cina; la quota ascrivibile al "colosso" dell'Estremo Oriente (24,1%) ha presentato un lieve decremento, pari all'incirca a mezzo punto percentuale, rispetto al medesimo indice rilevato un mese fa riguardo alla Repubblica Popolare Cinese. Come evidenzia il grafico qui sotto inserito, la seconda piazza del rating di aprile risulta occupata dalla Corea del Sud (15,6%); la quota ascrivibile ai flussi di spam generati entro i confini del paese asiatico ha fatto registrare un marcato aumento (+ 2,4%) rispetto al mese precedente. Ricordiamo, nella circostanza, come nell'ambito dell'analoga graduatoria di marzo 2014 relativa alle fonti dello spam mondiale la Corea del Sud occupasse, invece, il terzo gradino del podio. Sottolineiamo inoltre, proseguendo nella nostra analisi, come l'indice relativo ai messaggi e-mail indesiderati provenienti dal territorio degli Stati Uniti d'America (12,1%) abbia presentato una forte diminuzione rispetto al mese precedente, quantificabile in quasi 5 punti percentuali; in tal modo, gli USA sono scesi al

terzo posto della speciale graduatoria globale delle fonti di spam da noi elaborata, "perdendo" di fatto una posizione rispetto all'analogo rating relativo allo scorso mese di marzo. Complessivamente, nel periodo analizzato nel presente report, oltre la metà del volume complessivo dei messaggi di posta elettronica “spazzatura” diffusi su scala mondiale è stato inoltrato verso le e-mail box degli utenti dal territorio dei tre suddetti paesi.



Geografia delle fonti di spam rilevate nel mese di aprile 2014 - Graduatoria su scala mondiale

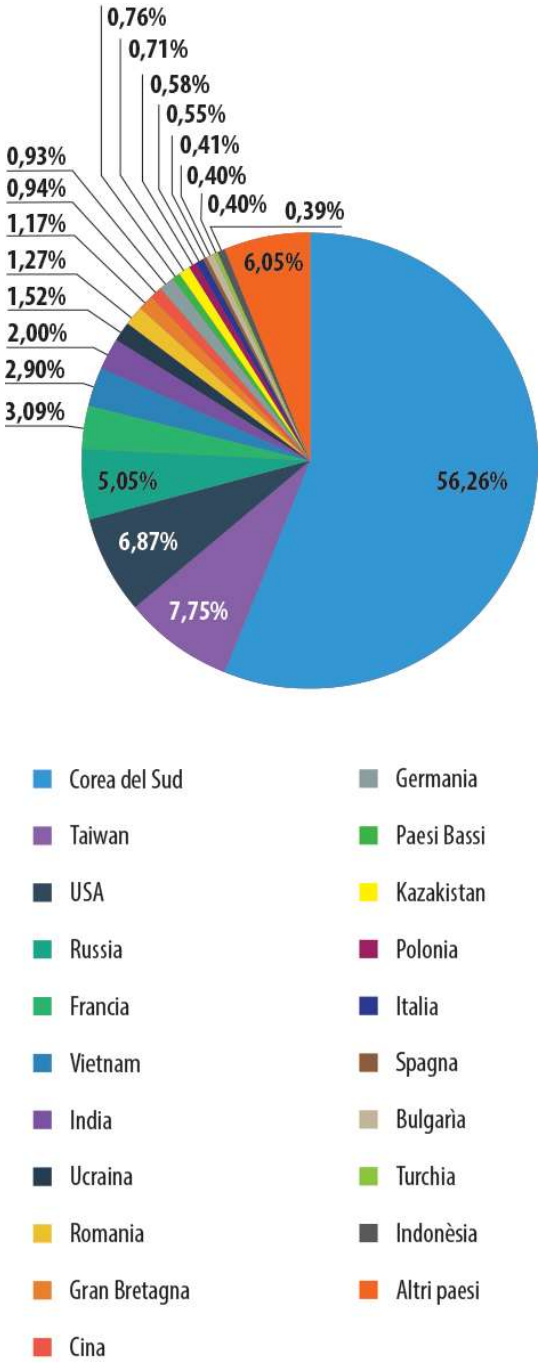
Osserviamo poi come abbiano conservato le rispettive posizioni all’interno della TOP-5 sia la Russia (9,1%) che Taiwan (6,5%). L'indice ascrivibile alle attività svolte dagli spammer insediati entro i confini

del territorio della Federazione Russa ha tuttavia evidenziato un sostanziale incremento (+ 2,5%) rispetto al mese scorso.

Risultano leggermente aumentate - nell'ambito della classifica riguardante la geografia delle fonti di spam rilevate nel mese di aprile 2014 relativamente ai messaggi e-mail indesiderati inviati dagli spammer verso ogni angolo del globo - anche le quote inerenti a Vietnam (4,2%), Ukraina (2,7%) e Filippine (1,9%); in media, gli indici ascrivibili a tali paesi hanno fatto registrare un incremento pari a 0,6 punti percentuali. In tal modo, le Filippine si sono collocate al 9° posto della graduatoria oggetto della nostra analisi, "guadagnando" di fatto due posizioni rispetto all'analogo rating di marzo 2014; ricordiamo, con l'occasione, che nel mese passato il popoloso paese-arcipelago situato nel Sud-Est asiatico insulare occupava "soltanto" l'undicesima piazza del rating in questione.

In ultima posizione, nella TOP-10 di aprile 2014, troviamo infine il Giappone (1,9%). La quota relativa ai messaggi di spam distribuiti dal territorio del Paese del Sol Levante è rimasta sostanzialmente invariata rispetto ad un mese fa; il Giappone è tuttavia passato dal nono al decimo posto della speciale classifica da noi elaborata. La Romania (1,4%), da parte sua, ha "perso" una posizione all'interno del ranking qui analizzato, abbandonando così la TOP-10 relativa ai paesi da cui vengono attualmente generati in misura maggiore i flussi dello spam "mondiale".

Desideriamo ugualmente porre in evidenza come, lungo tutto l'arco del mese di aprile, sia stato riscontrato un significativo aumento delle attività condotte dagli spammer sul suolo della Francia (1%); il paese transalpino è in tal modo entrato a far parte "d'emblée" della TOP-20 qui sopra riportata, andando immediatamente a collocarsi al 12° posto della speciale graduatoria globale delle fonti di spam. Completiamo la nostra analisi rilevando la presenza della Germania (0,7%) alla ventesima piazza della TOP-20; si tratta, nella circostanza, di una "new entry" a tutti gli effetti.



Geografia delle fonti di spam rilevate nel mese di aprile 2014 relativamente ai messaggi e-mail indesiderati inviati agli utenti della Rete situati sul territorio di paesi europei

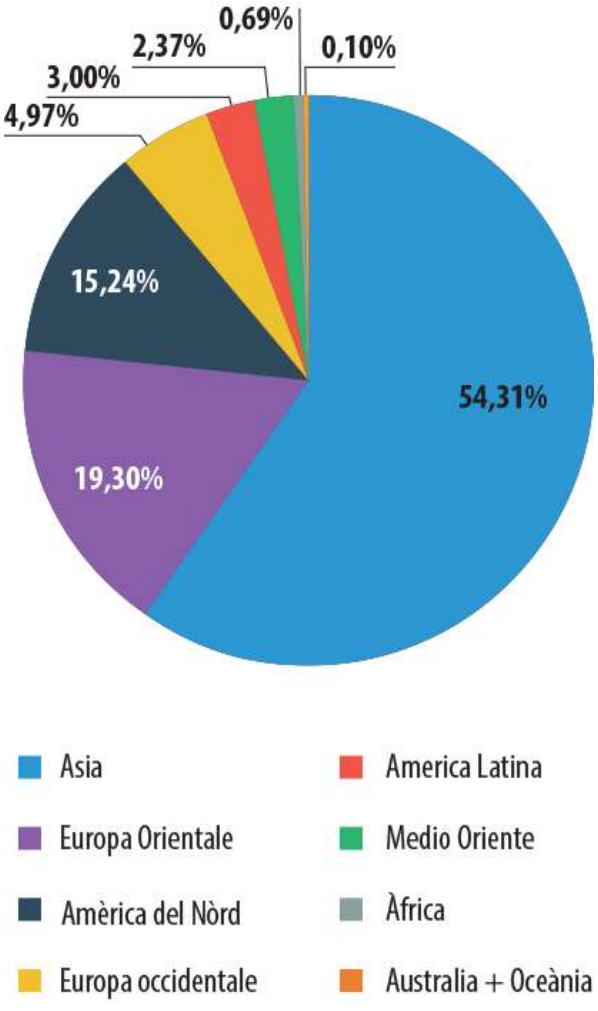
In aprile, la prima posizione della classifica relativa alla distribuzione geografica delle fonti dei messaggi di spam giunti nelle caselle di posta elettronica degli utenti della Rete europei, è andata nuovamente ad appannaggio della Corea del Sud; la quota attribuibile al paese dell'Estremo Oriente ha fatto segnare un ulteriore marcato aumento (+ 5,5%) rispetto allo scorso mese di marzo e si è quindi ancora una volta attestata su un valore complessivo notevolmente elevato (56,3%). Sul secondo gradino del "podio" virtuale di aprile 2014 spicca la presenza di Taiwan (7,8%); la quota riconducibile al paese asiatico risulta in effetti sensibilmente aumentata (+ 1,8%) rispetto ad un mese fa. Gli Stati Uniti, da parte loro, con un indice pari al 6,9%, si sono collocati al terzo posto della classifica relativa alle fonti geografiche dello spam "europeo"; nel mese qui analizzato la quota riconducibile agli USA ha fatto tuttavia registrare un decremento dello 0,7% rispetto all'analogo valore riscontrato per il paese nordamericano nel mese di marzo 2014.

Così come in precedenza, al quarto posto della consueta graduatoria da noi elaborata troviamo la Russia (5,1%), la cui quota, nell'arco di un mese, ha fatto registrare un significativo aumento, quantificabile in 0,8 punti percentuali. Ancor più marcato risulta essere l'incremento relativo all'indice percentuale attribuibile alla Francia (3,1%), passata in maniera assolutamente repentina dal 19° al 5° posto del rating riguardante i flussi di spam diretti verso il continente europeo.

Rispetto all'analogo rating di marzo 2014 è stata invece rilevata una non trascurabile diminuzione degli indici percentuali relativi ad Ukraina (1,5%) e Romania (1,3%), quantificabile, rispettivamente, in un valore pari allo 0,3% e allo 0,4%. L'ultima posizione della TOP-10 risulta occupata, così come in precedenza, dalla Gran Bretagna (1,2%); nel volgere di un mese, la quota attribuibile al Regno Unito ha fatto segnare una diminuzione pari a mezzo punto percentuale.

Allo stesso modo, rispetto allo scorso mese di marzo, hanno evidenziato significative flessioni le quote ascrivibili, rispettivamente, a Cina (1%), Polonia (0,6%) e Italia (0,6%); nella circostanza, ha presentato una diminuzione particolarmente marcata (- 2%) proprio l'indice relativo alla Repubblica Popolare Cinese, mentre per gli altri due paesi è stata rilevata una diminuzione decisamente più contenuta, quantificabile, per entrambi, in 0,3 punti percentuali. Per contro, è stato da noi osservato un lieve incremento delle attività svolte dagli spammer insediati in territorio tedesco; nel mese di aprile, nell'ambito della speciale classifica "regionale" delle fonti di spam, l'indice attribuibile alla Germania si è così attestato su un valore pari allo 0,9%.

Rileviamo, infine, come siano entrati a far parte del rating relativo allo spam destinato agli utenti della Rete europei due ulteriori nazioni, ovvero i Paesi Bassi (0,8%) e la Turchia (0,4%).



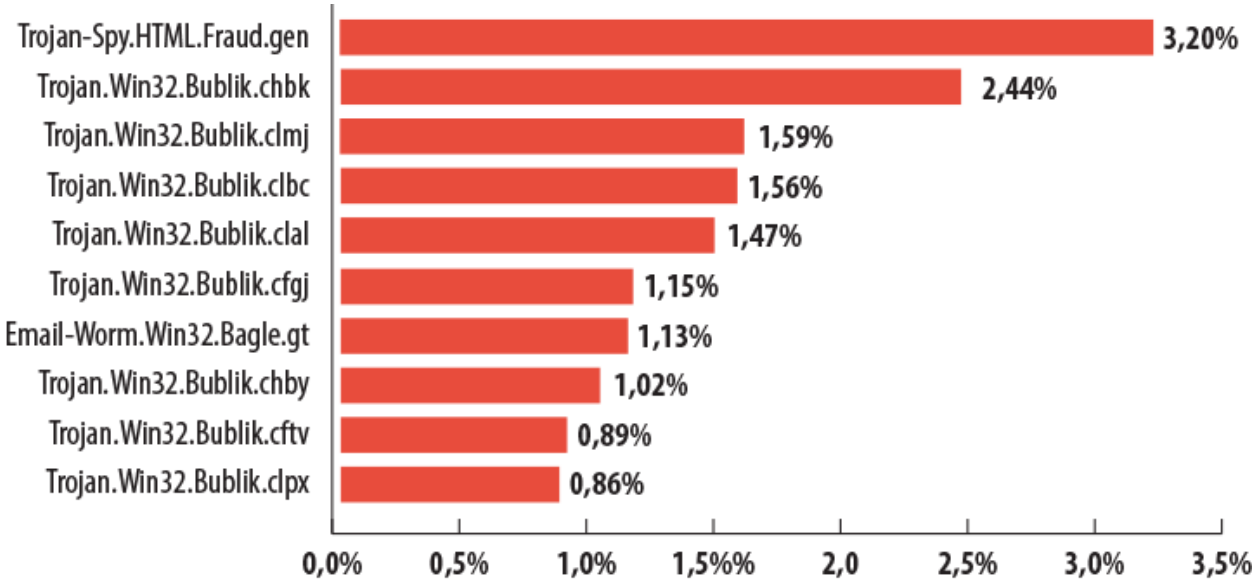
Suddivisione per macro-regioni geografiche delle fonti di spam rilevate nel mese di aprile 2014

Il ranking relativo alla ripartizione delle fonti di spam per macro-regioni geografiche mondiali evidenzia ancora una volta un netto dominio da parte dell'Asia, la cui quota si è attestata su un valore complessivo pari al 59,8%. Da parte loro, Europa Orientale (16,9%) e America Settentrionale (12,3%) si sono scambiate le posizioni occupate nell'ambito di tale graduatoria nel precedente mese di marzo, e sono andate a collocarsi, rispettivamente, sul secondo e sul terzo gradino del "podio" virtuale di aprile 2014. Nella circostanza, è di particolare interesse osservare come, nel mese oggetto del presente report, l'indice attribuibile ai messaggi e-mail indesiderati distribuiti dal territorio di paesi ubicati nell'Europa Orientale abbia fatto registrare un aumento superiore ai 2 punti percentuali, mentre, al contempo, l'analoga quota relativa al continente nordamericano ha manifestato una pronunciata flessione; tale diminuzione ha quasi sfiorato il 5%.

In quarta e quinta posizione, nel quadro del rating relativo alle fonti di spam suddivise per macro-regioni mondiali, troviamo poi Europa Occidentale (5,3%) ed America Latina (2,9%); anche per tali macro-aree geografiche è stato riscontrato un significativo incremento delle relative quote di "competanza", quantificabile, rispettivamente, in un valore pari allo 0,6% ed allo 0,5%.

Allegati dannosi rilevati nel traffico e-mail

La TOP-10 del mese di aprile 2014 relativa ai software nocivi più frequentemente rilevati all'interno dei flussi di posta elettronica globali si presenta nel modo seguente.



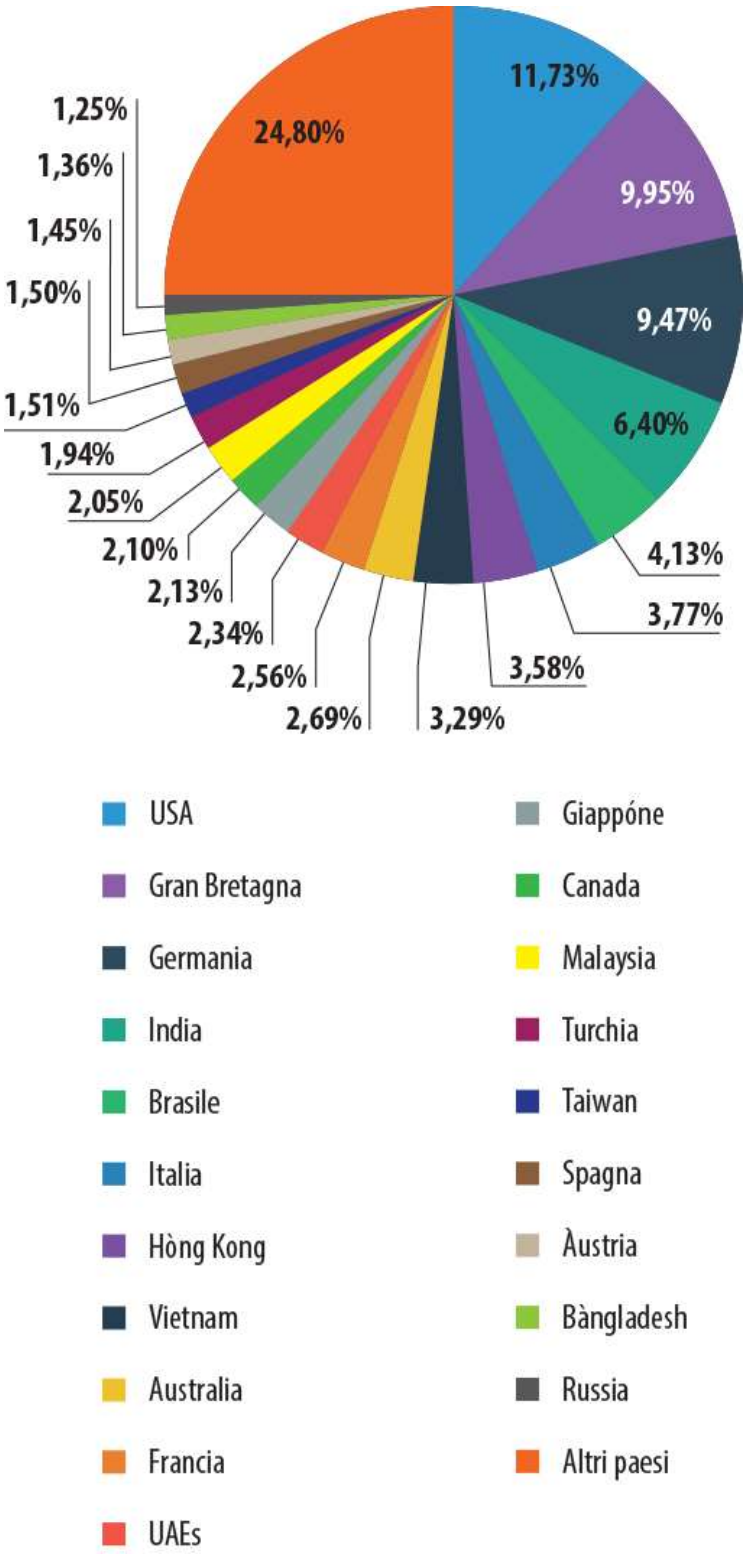
TOP-10 relativa ai programmi dannosi maggiormente diffusi nel traffico di posta elettronica nel mese di aprile 2014

Come da tradizione ormai ampiamente consolidata, apre la TOP-10 del mese di aprile 2014 - relativa ai software nocivi maggiormente presenti nei flussi di posta elettronica globali - il malware classificato con la denominazione di Trojan-Spy.HTML.Fraud.gen (3,2%); la quota attribuibile a tale programma nocivo ha tuttavia fatto registrare una diminuzione di oltre due punti percentuali rispetto all'analogo indice rilevato in marzo. A questo punto, riteniamo più che lecito confidare nel fatto che, dopo aver dedicato ampio spazio, all'interno dei nostri consueti report ed articoli specializzati, al malware che tuttora detiene saldamente la leadership del rating qui sopra riportato, il numero degli utenti che rimangono attualmente vittima del trojan Fraud.gen possa essersi ormai ridotto ai minimi termini. Ci pare doveroso

ad ogni caso ricordare, una volta di più, le temibili funzionalità nocive espletate dal suddetto software maligno: il malware Trojan-Spy.HTML.Fraud.gen è stato elaborato dai suoi autori sotto forma di una pagina HTML di phishing, in grado di riprodurre i form di registrazione di determinati servizi di banking online o di altri servizi erogati nel World Wide Web. Il Trojan-Spy in causa è stato appositamente creato dai virus writer per compiere il furto dei dati sensibili (login e password) relativi, in primo luogo, agli account di Internet banking aperti in Rete dagli utenti. In pratica, se l'utente inserisce i propri dati all'interno dei campi presenti nei form contraffatti, e provvede a trasmettere tali dati tramite l'apposito pulsante di invio, le informazioni personali cadranno direttamente ed inevitabilmente nelle mani di malintenzionati senza scrupoli. Fraud.gen viene abitualmente distribuito dai malfattori della Rete tramite la posta elettronica, sotto forma di importanti notifiche e comunicazioni provenienti (in apparenza!) da istituti bancari, negozi Internet, servizi online di primaria importanza, etc.

Esaminando la composizione della TOP-10 di aprile 2014, salta immediatamente agli occhi la presenza di un considerevole numero di programmi nocivi appartenenti alla famiglia di malware denominata Bublik. Tutti i software nocivi - riconducibili a tale famiglia - collocatisi nella parte alta della graduatoria qui analizzata (le prime dieci posizioni della stessa) provvedono ad effettuare il download, sul computer-vittima sottoposto ad attacco, di un temibile programma Trojan appartenente alla famigerata famiglia ZeuS/Zbot (malware del quale abbiamo più volte riferito all'interno dei nostri abituali resoconti mensili, nelle sezioni appositamente dedicate al fenomeno della diffusione dello spam nocivo). Ricordiamo, nella circostanza, come i software dannosi riconducibili alla famiglia di malware denominata ZeuS/Zbot si contraddistinguano per il fatto di essere particolarmente complessi e sofisticati; nello specifico, tali programmi dannosi risultano preposti ad attaccare sia i server che i computer degli utenti, allo scopo di intercettare e carpire dati di natura sensibile e riservata. Sebbene i trojan sopra menzionati siano in grado di eseguire attività dannose di vario genere, nella maggior parte dei casi essi vengono utilizzati proprio per compiere il furto delle informazioni bancarie custodite nei computer degli utenti, incluso - ovviamente - i dati sensibili relativi alle carte di credito. I malware appartenenti alla famiglia ZeuS/Zbot possono ugualmente generare l'installazione di CryptoLocker, un programma "estorsore" che richiede all'utente-vittima una certa somma di denaro per effettuare la decodifica dei dati precedentemente criptati.

Il malware rilevato dalle soluzioni antivirus di Kaspersky Lab come Email-Worm.Win32.Bagle.gt, collocatosi alla settima piazza del rating di aprile 2014, rappresenta una sorta di "sopravvissuto" al massiccio attacco sferrato nell'occasione dai rappresentanti della famiglia Bublik. Si tratta, come è noto, di un virus-worm di posta elettronica preposto a raccogliere gli indirizzi e-mail presenti nei computer-vittima contagiati, e più precisamente negli elenchi dei contatti, per poi auto-diffondersi in Rete tramite gli account di posta illecitamente carpiti. Tale programma nocivo risulta inoltre provvisto di ulteriori "doti": esso è stato appositamente progettato e sviluppato dai virus writer per interagire con specifici siti web allestiti dai cybercriminali, al fine di scaricare dalla Rete ulteriori file nocivi sui computer sottoposti ad attacco, all'insaputa degli utenti-vittima.



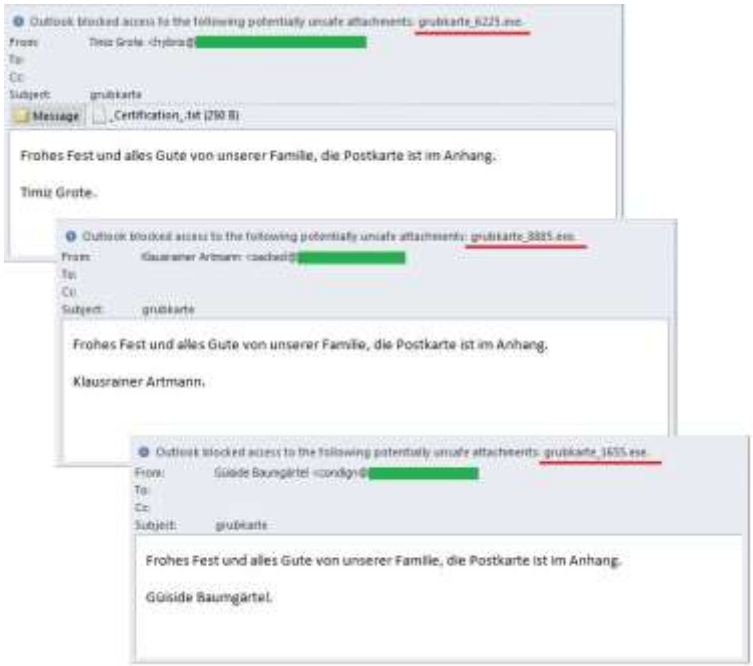
Ripartizione per paesi dei rilevamenti eseguiti nel mese di aprile 2014 dall'antivirus e-mail

Il primo posto della classifica qui sopra riportata - riguardante i paesi nei quali, durante il mese di aprile 2014, il nostro modulo antivirus dedicato alla posta elettronica ha eseguito il maggior numero di rilevamenti volti a neutralizzare i programmi malware distribuiti attraverso i flussi e-mail - è andato nuovamente ad appannaggio degli Stati Uniti (11,73%); l'indice percentuale ascrivibile agli USA ha presentato tuttavia un lieve decremento (- 0,28%) rispetto all'analogo valore rilevato nel mese precedente. Sul secondo e sul terzo gradino del "podio" virtuale si sono poi collocate, rispettivamente, Gran Bretagna (9,95%) e Germania (9,47%).

La quota relativa ai rilevamenti effettuati dall'antivirus e-mail entro i confini del territorio brasiliano (4,13%) ha fatto segnare un sensibile aumento (+ 2,13%) rispetto ad un mese fa; il Brasile è andato in tal modo ad occupare in maniera repentina la quinta posizione della speciale graduatoria qui esaminata. Risulta invece lievemente diminuita (- 0,25%) la quota attribuibile alla Federazione Russa; come conseguenza, la Russia ha "perso" quattro posizioni in classifica, scendendo dal 16° al 20° posto del rating da noi elaborato. Nel periodo oggetto del presente report, gli indici relativi ai rimanenti paesi presenti in graduatoria non hanno subito significative variazioni percentuali rispetto a quanto riscontrato nel mese di marzo 2014.

Peculiarità e tratti caratteristici dello spam nocivo di aprile

Nel giorno immediatamente successivo alla festività di Pasqua, gli spammer dediti alla distribuzione di pericolosi programmi dannosi nelle e-mail box degli utenti della Rete hanno condotto un esteso mailing di massa volto a diffondere messaggi di auguri elaborati in lingua tedesca; le e-mail in questione risultavano inviate a nome di utenti le cui caselle di posta elettronica, con ogni probabilità, erano state precedentemente violate da malintenzionati. Attraverso tali messaggi venivano quindi formulati auguri in forma particolarmente cordiale ed amichevole; oltre a ciò, le e-mail in causa, secondo le intenzioni del mittente, avrebbero dovuto recare al destinatario, in allegato, un'innocua e variopinta cartolina elettronica a tema. In realtà, il file eseguibile trasmesso assieme al messaggio celava un insidioso malware, classificato dagli esperti di sicurezza IT con la denominazione di Trojan-PSW.Win32.Fareit.aonw. A differenza di altre varianti di malware riconducibili alla famiglia Fareit le funzionalità nocive di cui è provvisto tale programma dannoso - individuato dai nostri analisti nell'ambito della campagna di spam nocivo sopra descritta - sono risultate essere di portata decisamente inferiore: in effetti, esso non esegue il furto delle password legate all'utilizzo di determinati software, bensì genera "esclusivamente" il download ed il successivo avvio, sul computer infetto, di un ulteriore programma Trojan, denominato Trojan-Spy.Win32.Zbot.sbba, un temibile programma maligno preposto sia alla conduzione di attacchi informatici nei confronti dei server, sia al furto dei dati personali degli utenti.

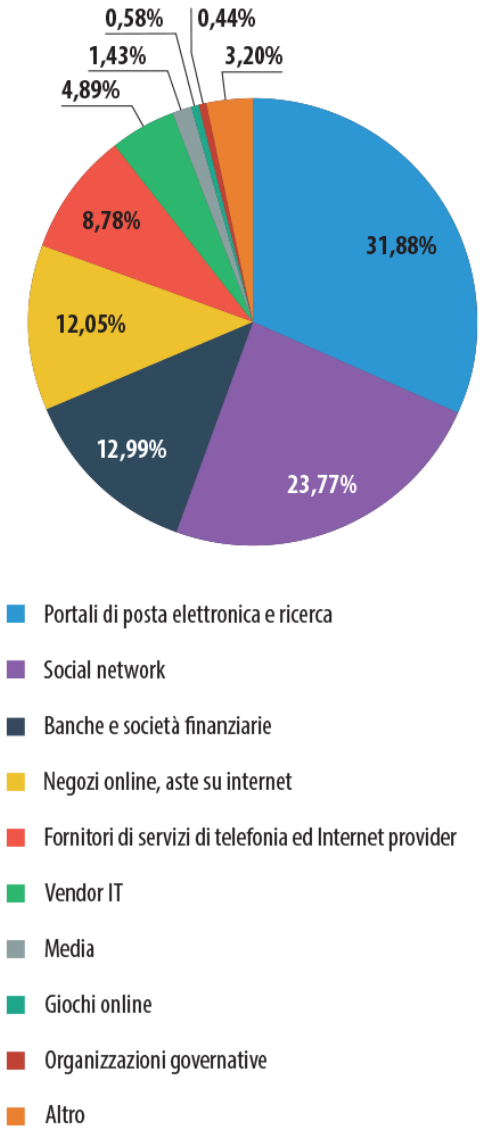


Allo stesso modo, lungo tutto l'arco del mese di aprile 2014, sono stati da noi individuati vari attacchi nocivi, particolarmente estesi ed insistiti, mascherati in veste di mailing di massa recanti ai destinatari messaggi e-mail provenienti (in apparenza!) dal noto servizio online eFax, il quale, come è noto, consente di inviare e ricevere fax sotto forma di allegati di posta elettronica. I messaggi contraffatti contenevano, generalmente, un'apposita notifica relativa alla ricezione di un determinato fax da parte del destinatario dell'e-mail fasulla; nella circostanza, nel tentativo di conferire maggiore credibilità al messaggio di posta, gli spammer si sono addirittura premurati di indicare il numero di pagine di cui si componeva il "documento" apparentemente trasmesso attraverso il suddetto servizio fax via Internet. In realtà, gli archivi compressi allegati ai messaggi di spam nocivo qui esaminati, custodivano un temibile programma malware, ed in particolar modo il software maligno denominato Trojan-Downloader.Win32.Cabby.a, un programma Trojan-Downloader (come recita in maniera inequivocabile la denominazione ad esso attribuita) di dimensioni piuttosto contenute, il quale si caratterizza per il fatto di celare, nel proprio "corpo", un file CAB contenente un documento o un'immagine; questi ultimi vengono così mostrati all'utente non appena il software nocivo in causa viene avviato ed eseguito sul computer infetto. Mentre il potenziale utente-vittima è intento a visualizzare l'allegato ricevuto nell'occasione, il trojan Cabby provvede ad effettuare, da parte sua, a totale insaputa dell'utente sottoposto ad attacco informatico, il download di un ulteriore programma dannoso. Nel caso specifico da noi esaminato, il suddetto programma Trojan è risultato essere preposto al caricamento, sulla macchina infetta, di un temibile rappresentante della famigerata famiglia di malware denominata ZeuS/Zbot (Trojan-Spy.Win32.Zbot.shqe).

Phishing

A partire dallo spam report stilato riguardo al mese di aprile 2014, abbiamo deciso di unire due delle principali categorie da noi precedentemente definite per ciò che riguarda, nello specifico, le organizzazioni sottoposte con maggior frequenza agli attacchi portati dai phisher. In effetti, i raggruppamenti «Posta elettronica, programmi di instant messaging» e «Motori di ricerca» sono stati in

pratica fusi in un'unica, nuova categoria, denominata «Portali di posta elettronica e ricerca». La TOP-100 da noi stilata relativamente al mese oggetto della nostra analisi sul fenomeno spam, vede proprio in prima posizione questa nuova categoria, la quale ha fatto complessivamente registrare un indice pari al 31,9%. Come evidenzia il grafico qui sotto riportato, la seconda piazza del rating - relativo alle organizzazioni (suddivise per categorie) rimaste più frequentemente vittima degli assalti di phishing nel corso del mese di aprile - risulta occupata dai social network, con una quota pari al 23,8%; l'indice percentuale ascrivibile agli attacchi condotti dai phisher nei confronti delle reti sociali ha tuttavia fatto registrare un lieve decremento rispetto ad un mese fa, diminuzione quantificabile in 0,2 punti percentuali. La terza posizione della speciale classifica di aprile dedicata al fenomeno phishing è andata ad appannaggio della categoria “Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari” (13%), la quale ha ugualmente evidenziato, nell'arco di un mese, la medesima lieve flessione (-0,2%). Allo stesso modo, la quota riconducibile agli attacchi di phishing orditi nei confronti dei negozi online (12,1%) ha presentato, rispetto al precedente mese di marzo, un leggero decremento (- 0,8%), pur risultando tale diminuzione più pronunciata in relazione ai valori rilevati per le due categorie che si sono collocate sul secondo e sul terzo gradino del "podio". Terminiamo la nostra breve rassegna dedicata alla TOP-100 del phishing di aprile 2014, osservando come gli indici percentuali relativi alle rimanenti categorie presenti in graduatoria abbiano anch'essi evidenziato variazioni piuttosto trascurabili, le quali non hanno in alcun modo determinato conseguenti cambiamenti di posizione all'interno del rating.



TOP-100 relativa alle organizzazioni maggiormente sottoposte agli attacchi di phishing nel mese di aprile 2014 - Suddivisione per categorie dei rilevamenti eseguiti dal modulo Anti-phishing

La classifica delle 100 organizzazioni (ripartite per categorie) i cui clienti sono risultati bersaglio prediletto degli assalti di phishing si basa sui rilevamenti eseguiti dal nostro componente «Anti-phishing» attraverso le soluzioni anti-malware installate sui computer degli utenti. Tale modulo è in grado di individuare e neutralizzare tutti i link di phishing sui quali l'utente si imbatte, siano essi collegamenti ipertestuali nocivi contenuti all'interno di messaggi di spam oppure link disseminati nel World Wide Web.

Le grandi società ed organizzazioni cinesi divengono spesso bersaglio delle losche attenzioni dei phisher; ad esempio, nel periodo oggetto della nostra analisi sono stati registrati insistiti attacchi di phishing nei confronti di Tencent, nota compagnia operante nel settore delle telecomunicazioni, la quale, tra l'altro, è proprietaria di QQ, il più diffuso e popolare programma di messaggistica istantanea in Cina (con centinaia di milioni di utenti). Nel caso specifico da noi esaminato, i malfattori hanno cercato di carpire login e password utilizzati dai clienti della suddetta società cinese per accedere ai propri account di instant messaging; nella circostanza, i phisher hanno fatto ampiamente ricorso agli abituali trucchi e sotterfugi di cui generalmente si avvale tale categoria di malintenzionati nel tentativo di raggirare il pubblico della Rete. Attraverso i messaggi di phishing in questione, indirizzati verso le caselle di posta elettronica dei potenziali utenti di QQ, si comunicava al destinatario dell'e-mail contraffatta, mediante una notifica fasulla appositamente elaborata, che dall'account di cui quest'ultimo risultava essere titolare era stata inoltrata una richiesta, piuttosto sospetta, relativa al ripristino dell'account stesso. Nella fattispecie, visto che la richiesta "incriminata" era stata effettuata da un utente non autorizzato, al fine di evitare ogni possibile tentativo di furto delle informazioni personali, si era quindi provveduto a limitare l'accesso all'account in questione.

Per annullare, di fatto, la richiesta eseguita, con l'occasione si invitava il destinatario del messaggio a cliccare sul link appositamente inserito nell'e-mail; seguendo il collegamento ipertestuale proposto, in realtà, l'ignaro utente sarebbe giunto su una pagina web di phishing, peraltro allestita dai malintenzionati in maniera piuttosto sapiente, con notevole cura. E' di particolare interesse osservare come la falsa notifica qui sotto riprodotta sia stata inviata sotto forma di immagine grafica; in tal modo, i phisher hanno considerevolmente complicato l'azione svolta dai filtri antispam, mentre, al tempo stesso, hanno agevolmente conferito al messaggio un aspetto di apparente legittimità.

Conclusioni

Nel mese di aprile 2014 la quota dello spam presente nel traffico di posta elettronica globale ha fatto registrare un incremento del 7,6%, attestandosi in tal modo su un valore medio pari al 71,1%. L'indice percentuale più elevato, relativamente alla presenza dei messaggi di spam in seno ai flussi e-mail mondiali, è stato riscontrato nell'ultima settimana del mese oggetto del presente report (73%).

In aprile, come era lecito attendersi, ha raggiunto il suo picco massimo lo spam "festivo" ispirato alle tradizionali tematiche suggerite dalla festività di Pasqua, la più importante ricorrenza e celebrazione stagionale. In particolar modo, gli spammer hanno inondato le e-mail box degli utenti di ogni angolo del pianeta di messaggi di posta recanti le più disparate proposte commerciali relative a prodotti e servizi "pasquali" appositamente offerti e confezionati per l'occasione; al tempo stesso, tuttavia, gli spammer non hanno affatto disdegnato di effettuare l'invio di vere e proprie montagne di messaggi e-mail indesiderati reclamizzanti articoli e prodotti per nulla correlati con le classiche tematiche legate alla principale festività del mese. Il tema della celebrazione della Pasqua è stato ampiamente "sfruttato" anche nell'allestimento di varie campagne di spam fraudolento, volte a recapitare ai destinatari dei messaggi false notifiche relative ad improbabili vincite realizzate mediante inesistenti lotterie online; tutto ciò, naturalmente, allo scopo di catalizzare al massimo l'attenzione degli utenti dei client di posta elettronica, potenziali vittime - secondo le subdole intenzioni degli spammer dediti alle truffe in Rete - di inganni e raggiri di ogni genere. Inoltre, nell'impetuosa ondata di messaggi di spam che ha caratterizzato il periodo pasquale, non sono di certo mancate le consuete e-mail nocive contenenti temibili programmi dannosi, camuffate sotto forma di tradizionali e rassicuranti messaggi di auguri.

Nell'ambito delle prime tre posizioni della speciale graduatoria di aprile relativa alle fonti dello spam "globale" - riguardante i paesi dal cui territorio sono state distribuite in Rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail “spazzatura” - sono intervenuti significativi cambiamenti. Il "podio" virtuale del ranking da noi stilato riguardo al mese di aprile 2014 risulta composto dalle seguenti nazioni: Cina (24,1%), Corea del Sud (15,6%), Stati Uniti (12,1%). Da parte sua, la classifica relativa alla ripartizione delle fonti di spam per macro-regioni geografiche mondiali evidenzia ancora una volta l'incontrastato dominio del continente asiatico, la cui quota, nel mese oggetto della nostra analisi, si è attestata su un valore complessivo pari al 59,8%.

La TOP-100 riguardante le organizzazioni (suddivise per categorie) rimaste vittima con maggior frequenza degli assalti portati dai phisher risulta capeggiata dalla nuova categoria da noi definita, denominata «Portali di posta elettronica e ricerca», la quale ha fatto complessivamente registrare un indice pari al 31,9%. La seconda posizione del rating di aprile 2014 dedicato alla diffusione del fenomeno phishing è andata ad appannaggio dei social network (23,8%), mentre la categoria "Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari" si è collocata al terzo posto della graduatoria (13%).