Lo spam nel mese di Settembre 2014

Tat'jana Šerbakova, Marija Vergelis, Nadežda Demidova

Sommario

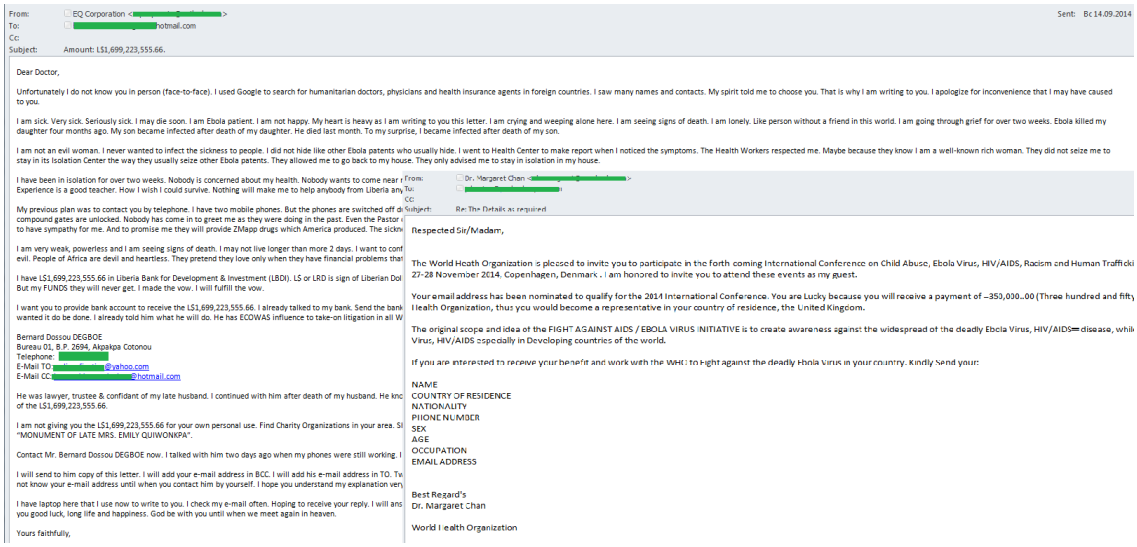
Le peculiarità del mese

Nel mese oggetto del presente report, i truffatori "nigeriani" hanno sfruttato nuove tematiche per la conduzione dei loro mailing di massa fraudolenti; al centro delle inverosimili "storie" da essi abitualmente narrate è risultata essere, in particolar modo, la grave emergenza sanitaria causata a livello globale dal virus Ebola, con i numerosi casi di contagio che si sono via via manifestati in diversi paesi, costantemente ed attentamente riportati dai mass media di tutto il mondo. In settembre, il cosiddetto spam "festivo" si è principalmente ispirato alle tematiche suggerite sia dal Labor Day - l'importante festività nazionale statunitense dedicata ai lavoratori, tradizionalmente celebrata negli USA il primo lunedì di settembre - sia dalle principali festività dell'imminente stagione invernale; di fatto, gli spammer hanno già iniziato ad inondare le e-mail box degli utenti della Rete di montagne di messaggi di spam pubblicitario, volti a reclamizzare prodotti e servizi "essenziali" per preparare al meglio i festeggiamenti di Natale e Capodanno. Una parte considerevole dei mailing di massa a tema di notevoli proporzioni è stata poi dedicata alla promozione di prodotti e servizi mediante un attivo utilizzo dei social network attualmente più frequentati dal pubblico della Rete: in questo caso, gli spammer non hanno mancato di garantire, ai destinatari dei messaggi di spam, un immediato afflusso di nuova clientela e, di conseguenza, un rapido aumento dei profitti derivanti dall'attività commerciale svolta.

Il virus Ebola nello spam «nigeriano»

Nello scorso mese di luglio, i mass media di ogni angolo del pianeta riferivano già, con particolare enfasi, in merito al primo focolaio di Ebola, registratosi in Africa. Mentre l'attenzione di tutta la comunità internazionale si concentrava sulla possibile lotta da intraprendere contro la terribile malattia e sui metodi da adottare per prevenirne l'ulteriore diffusione, i truffatori della Rete iniziavano ad utilizzare le tematiche connesse al virus Ebola per inventarsi nuove, improbabili storie da diffondere attraverso le abituali e-mail "nigeriane".

Così, nel mese di settembre 2014, all'interno del traffico di spam globale, sono stati da noi individuate varie mailing di massa di natura fraudolenta in cui si citava esplicitamente il virus Ebola. I truffatori hanno fatto ricorso non solo alle più classiche "storielle" dello spam nigeriano, con i consueti messaggi apparentemente scritti a nome di persone affette dalle più disparate e terribili malattie, ma hanno ugualmente dato libero sfogo ad una buona dose di fantasia, inventandosi falsi racconti ed episodi dai contenuti piuttosto insoliti. Nell'e-mail inviata (in apparenza!) da una sedicente ricca signora residente in Liberia, in procinto di morire per i devastanti effetti della febbre emorragica provocata dall'aver contratto l'infezione da virus Ebola, si narra una lunga e commovente storia: la tremenda malattia ha già impietosamente ucciso tutti i figli della donna, mentre il centro medico locale si è rifiutato di prestare, a quest'ultima, i necessari soccorsi. L'autrice del messaggio si dichiara pronta ad effettuare una donazione di oltre 1,5 milioni di dollari al destinatario dell'e-mail, purché tale ingente somma venga poi destinata in beneficenza ad un'organizzazione caritatevole. Come si può osservare nello screenshot qui sotto riportato, il testo del messaggio risulta essere scritto in maniera estremamente dettagliata e contiene, per di più, un'accurata spiegazione riguardo alla terribile situazione che si è venuta a creare; è questo, indubbiamente, un elemento che si incontra piuttosto raramente nella composizione delle e-mail "nigeriane". Tuttavia, la presenza di un resoconto così dettagliato riguardo alla fantasiosa "storia" ideata dal "nigeriano" di turno altro non è, di fatto, se non uno specifico stratagemma per far sì che il destinatario dell'e-mail non abbia il minimo dubbio riguardo all'autenticità e alla veridicità del racconto narrato ed entri in tal modo subito in corrispondenza con i truffatori.



From: EQ Corporation <[redacted]>
To: [redacted]hotmail.com
Cc:
Subject: Amount: LS1,699,223,555.66.
Sent: Fr 14.09.2014

Dear Doctor,

Unfortunately I do not know you in person (face-to-face). I used Google to search for humanitarian doctors, physicians and health insurance agents in foreign countries. I saw many names and contacts. My spirit told me to choose you. That is why I am writing to you. I apologize for inconvenience that I may have caused to you.

I am sick. Very sick. Seriously sick. I may die soon. I am Ebola patient. I am not happy. My heart is heavy as I am writing to you this letter. I am crying and weeping alone here. I am seeing signs of death. I am lonely. Like person without a friend in this world. I am going through grief for over two weeks. Ebola killed my daughter four months ago. My son became infected after death of my daughter. He died last month. To my surprise, I became infected after death of my son.

I am not an evil woman. I never wanted to infect the sickness to people. I did not hide like other Ebola patents who usually hide. I went to Health Center to make report when I noticed the symptoms. The Health Workers respected me. Maybe because they know I am a well-known rich woman. They did not seize me to stay in its Isolation Center the way they usually seize other Ebola patents. They allowed me to go back to my house. They only advised me to stay in isolation in my house.

I have been in isolation for over two weeks. Nobody is concerned about my health. Nobody wants to come near
Experience is a good teacher. How I wish I could survive. Nothing will make me to help anybody from Liberia any

My previous plan was to contact you by telephone. I have two mobile phones. But the phones are switched off d
compound gates are unlocked. Nobody has come in to greet me as they were doing in the past. Even the Pastor
to have sympathy for me. And to promise me they will provide ZMapp drugs which America produced. The sickn

I am very weak, powerless and I am seeing signs of death. I may not live longer than more 2 days. I want to cont
evil. People of Africa are devil and heartless. They pretend they love only when they have financial problems that

I have LS1,699,223,555.66 in Liberia Bank for Development & Investment (LBDI). LS or LRD is sign of Liberian Dol
But my FUNDS they will never get. I made the vow. I will fulfill the vow.

I want you to provide bank account to receive the LS1,699,223,555.66. I already talked to my bank. Send the bank
wanted it do be done. I already told him what he will do. He has ECOWAS influence to take-on litigation in all W

Bernard Dossou DEGBOE
Bureau 01, B.P. 2694, Akpakpa Cotonou
Telephone: [redacted]
E-Mail TO: [redacted]@yahoo.com
E-Mail CC: [redacted]@hotmail.com

He was lawyer, trustee & confidant of my late husband. I continued with him after death of my husband. He kno
of the LS1,699,223,555.66.

I am not giving you the LS1,699,223,555.66 for your own personal use. Find Charity Organizations in your area. Sl
"MONUMENT OF LATE MRS. EMILY QUIWONKPA".

Contact Mr. Bernard Dossou DEGBOE now. I talked with him two days ago when my phones were still working.

I will send to him copy of this letter. I will add your e-mail address in BCC. I will add his e-mail address in TO. Tw
not know your e-mail address until when you contact him by yourself. I hope you understand my explanation very

I have laptop here that I use now to write to you. I check my e-mail often. Hoping to receive your reply. I will ans
you good luck, long life and happiness. God be with you until when we meet again in heaven.

Yours faithfully,

From: Dr. Margaret Chan <[redacted]>
To: [redacted]
Cc:
Subject: Re: The Details as required

Respected Sir/Madam,

The World Heath Organization is pleased to invite you to participate in the forth coming International Conference on Child Abuse, Ebola Virus, HIV/AIDS, Racism and Human Traffick
27-28 November 2014, Copenhagen, Denmark. I am honored to invite you to attend these events as my guest.

Your email address has been nominated to qualify for the 2014 International Conference. You are Lucky because you will receive a payment of –350,000.00 (Three hundred and fift
Health Organization, thus you would become a representative in your country of residence, the United Kingdom.

The original scope and idea of the FIGHT AGAINST AIDS / EBOLA VIRUS INITIATIVE is to create awareness against the widespread of the deadly Ebola Virus, HIV/AIDS= disease, whil
Virus, HIV/AIDS especially in Developing countries of the world.

If you are interested to receive your benefit and work with the WHO to Fight against the deadly Ebola Virus in your country. Kindly Send your:

NAME
COUNTRY OF RESIDENCE
NATIONALITY
PHONE NUMBER
SEX
AGE
OCCUPATION
EMAIL ADDRESS

Best Regard's
Dr. Margaret Chan

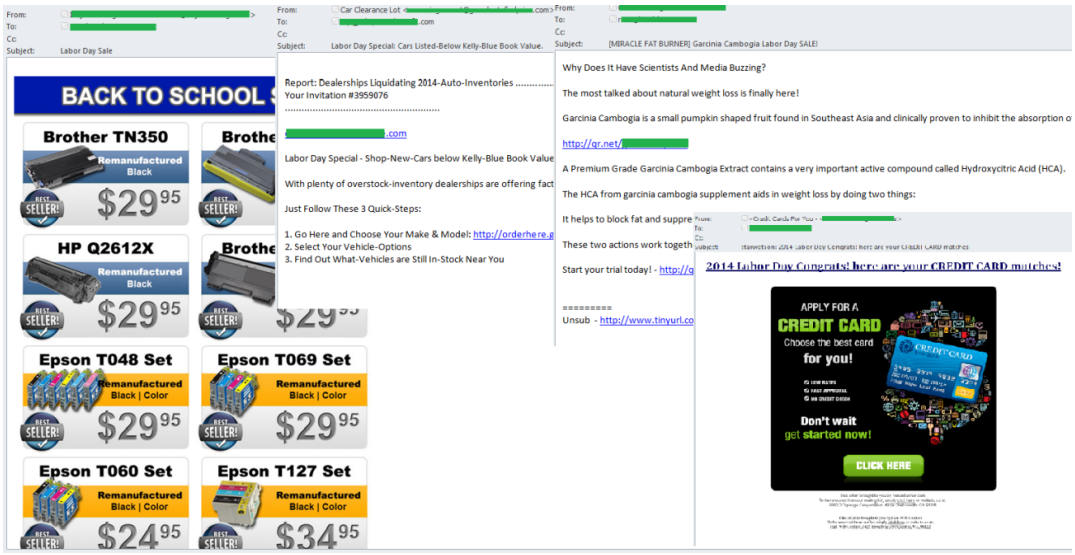
World Health Organization

Gli autori di un'altra campagna di spam fraudolento hanno poi assunto le vesti di una sedicente operatrice dell'Organizzazione Mondiale della Sanità (World Health Organization), cercando di attirare l'attenzione del destinatario del messaggio mediante l'utilizzo di un metodo alquanto inusuale nell'ambito dello spam "nigeriano", ovvero l'invito a partecipare ad una specifica conferenza, durante la quale si sarebbe dovuto discutere, tra l'altro, in merito alla lotta da sostenere urgentemente nei confronti della diffusione del virus Ebola. Nel messaggio, non solo si proponeva alla potenziale vittima

del raggiro di prendere parte alla suddetta conferenza, in qualità di ospite, ma si prometteva ugualmente una somma di 350.000 euro, nonché un'autovettura, per la futura attività di rappresentante dell'OMS che il destinatario del messaggio avrebbe dovuto poi svolgere in Gran Bretagna. Nel caso in cui il potenziale utente-vittima si fosse dichiarato disponibile ad accettare l'allettante proposta, egli avrebbe comunque dovuto subito comunicare i propri dati personali al mittente dell'e-mail. Con ogni probabilità i malintenzionati hanno confidato sul fatto che la promessa di un'ingente quantità di denaro e di un'interessante occupazione nell'ambito di una prestigiosa organizzazione internazionale avrebbe potuto dissipare ogni eventuale dubbio riguardo alla veridicità del messaggio di posta elettronica ricevuto.

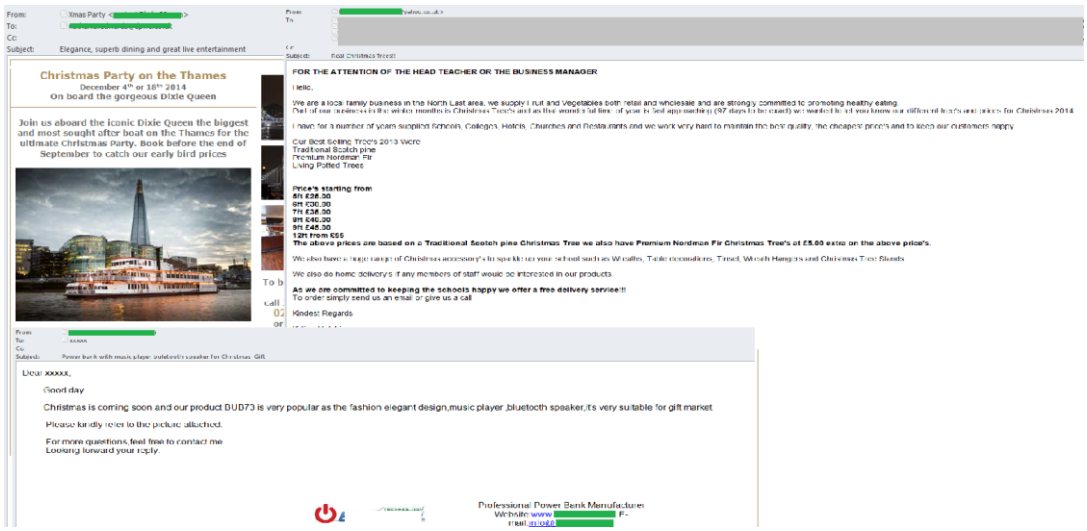
Spam e festività

Come abbiamo detto, all'inizio di settembre (per l'esattezza il primo lunedì del mese) si celebra, negli Stati Uniti, il Labor Day, la nota festività dedicata ai lavoratori; da parte loro gli spammer, come al solito, non hanno certo ignorato tale importante ricorrenza. Questi ultimi, tradizionalmente, alla vigilia delle festività di maggior rilievo, cercano di attirare al massimo l'attenzione degli utenti con proposte commerciali che prevedono sostanziosi sconti, allettanti saldi e svendite di ogni genere. Nel mese di settembre, le società specializzate nella vendita di toner e cartucce per stampanti hanno ad esempio offerto considerevoli sconti sui prodotti da esse commercializzati, e non soltanto in occasione dei festeggiamenti dedicati al Labor Day, ma anche in previsione dell'inizio del nuovo anno scolastico ed accademico. Nell'ambito dello spam "farmaceutico" ci siamo imbattuti, come al solito, nelle consuete pubblicità di prodotti per il dimagrimento, proposti a prezzi ancor più convenienti proprio in occasione della celebrazione della suddetta festività statunitense.



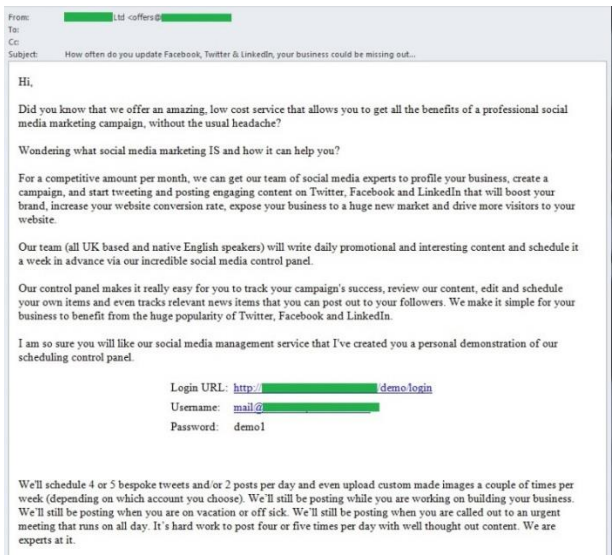
Nel traffico di spam globale, hanno inoltre già fatto la loro comparsa le tradizionali pubblicità di prodotti e servizi ispirati alle tematiche suggerite dalle ormai non troppo lontane festività di Natale e Capodanno. Nel segmento dei messaggi e-mail indesiderati composti in lingua inglese abbiamo ad esempio individuato un'originale proposta per festeggiare l'atteso evento natalizio a Londra, a bordo di un bellissimo battello in navigazione sul fiume Tamigi; prenotando i biglietti con largo anticipo si sarebbero potuti ottenere prezzi estremamente vantaggiosi per la mini-crociera offerta. Nel corso del mese di settembre, infine, gli spammer hanno già proposto ai destinatari dei loro messaggi pubblicitari di interessarsi con il dovuto anticipo all'acquisto dei regali e comprare, magari, dispositivi digitali di vario

genere direttamente presso i produttori cinesi. Non sono nemmeno mancate alcune proposte (forse un po' premature...) per ordinare in tempo il proprio albero di Natale.



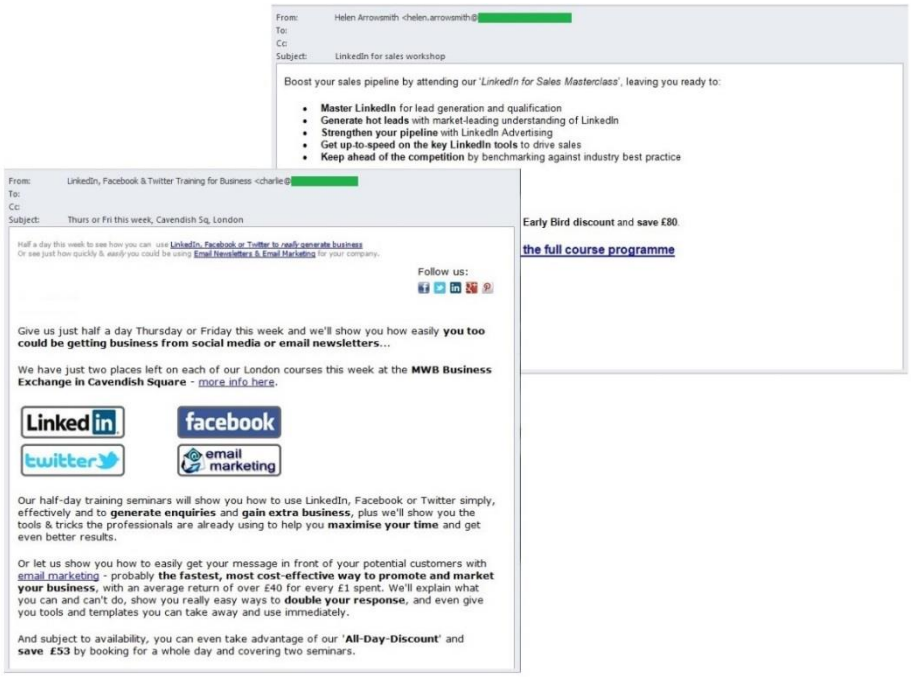
Guadagnare in Internet: farsi pubblicità sui social network

Nel quadro delle mailing di massa a tema - particolarmente estesi - che hanno caratterizzato i flussi di spam nel mese di settembre 2014, segnaliamo la presenza di varie campagne volte a reclamizzare alcuni metodi per poter realizzare consistenti guadagni attraverso Internet, in particolar modo mediante l'utilizzo dei social network maggiormente frequentati dal vasto pubblico della Rete. Il più delle volte, gli spammer hanno offerto, per un determinato prezzo, l'opportunità di poter creare un profilo individuale o un gruppo su Twitter, Facebook o LinkedIn, e di realizzare poi la relativa pagina rispettando la specifica filosofia aziendale; in seguito, il prodotto/servizio sarebbe stato promosso nella maniera più adeguata, assicurando i primi follower, componendo attentamente i contenuti iniziali e pubblicizzando attivamente il tutto. Gli autori di tali mailing di massa garantivano inoltre che, una volta poste le dovute basi, seguendo i criteri sopra elencati, si sarebbe rapidamente osservato un considerevole aumento del numero dei clienti e, di conseguenza, del volume delle vendite realizzate dalla società-committente. Per poter usufruire del servizio commerciale offerto, gli utenti destinatari delle e-mail in questione avrebbero dovuto presentare una semplice ed immediata richiesta, cliccando sul link appositamente inserito nel corpo del messaggio.

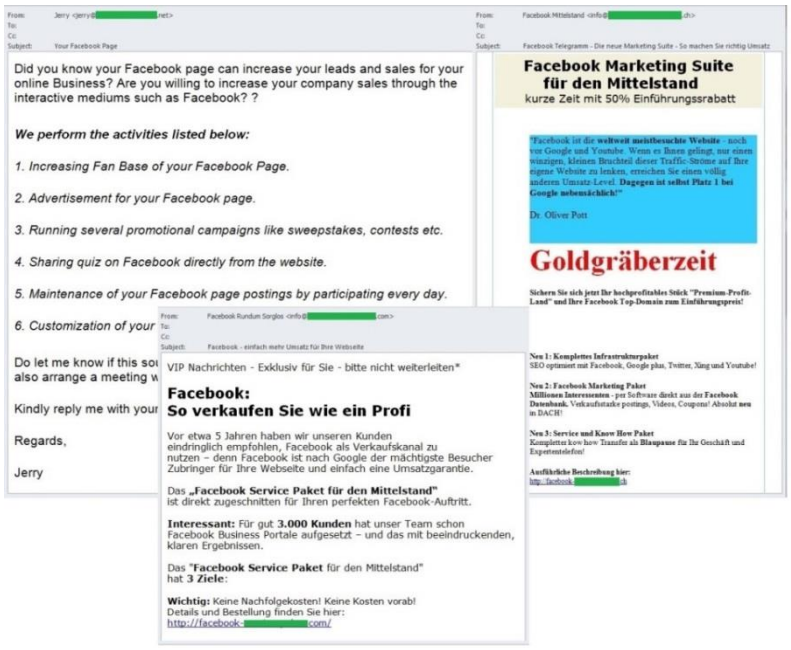


Sembrano attualmente godere di altrettanta popolarità, presso le nutrite schiere degli spammer, anche quei servizi volti a promuovere in maniera professionale società, aziende, business ed attività commerciali di vario genere, mediante l'inserimento di particolari foto e video all'interno di social network specializzati. Allo stesso modo, anche gli autori di tali campagne di spam promettono ai propri committenti di poter garantire in tempi rapidi un numero adeguato di follower, ad esempio su Instagram; più precisamente, gli spammer dichiarano che, trascorsi soltanto tre giorni dall'inserimento del materiale video-fotografico relativo ai prodotti da reclamizzare, verranno di sicuro ottenuti i primi risultati positivi, generati dalla campagna pubblicitaria intrapresa. Piuttosto di frequente, inoltre, è stata proposta ai destinatari delle e-mail di spam riconducibili a tale tipologia, la realizzazione di video professionali per presentare nella maniera più adeguata l'attività della propria società, oppure un determinato prodotto - ed il successivo inserimento del filmato all'interno della nota video-piattaforma YouTube. Inoltre, gli spammer hanno sbandierato ai quattro venti l'opportunità di poter ricavare "un vero e proprio mucchio di soldi" - sempre servendosi di YouTube - impiegando, in tutto, solo 40 minuti al giorno del proprio tempo. Tali messaggi di spam, tuttavia, rappresentavano, in primo luogo, una pubblicità più o meno occulta dell'ennesimo corso di marketing proposto sul già saturo mercato da un rinomato autore, corso presentato, come d'abitudine, su supporto DVD. Il disco contenente tutte le istruzioni per poter realizzare i guadagni stratosferici promessi, avrebbe potuto essere acquistato semplicemente cliccando sul link inserito nel messaggio, recandosi, di conseguenza, sul sito web preposto alla vendita del DVD.

Lungo tutto l'arco del mese di settembre, ci siamo ugualmente imbattuti, in seno ai flussi di spam, in numerose mailing di massa recanti inviti a partecipare a seminari o webinar a tema, dedicati alla "scienza" relativa all'amministrazione di gruppi e comunità nell'ambito dei social network. Nella fattispecie, gli autori di tali corsi promettevano di svelare tutti i dettagli, le finezze e le impercettibili sfumature relative alla professione di amministratore - ad esempio - di un gruppo creato su Facebook o LinkedIn, professione che avrebbe poi garantito, ai partecipanti al corso, un costante e stabile guadagno mensile, grazie ad Internet. Per potersi iscrivere al webinar, gli utenti avrebbero dovuto semplicemente cliccare sull'apposito link inserito nel messaggio.

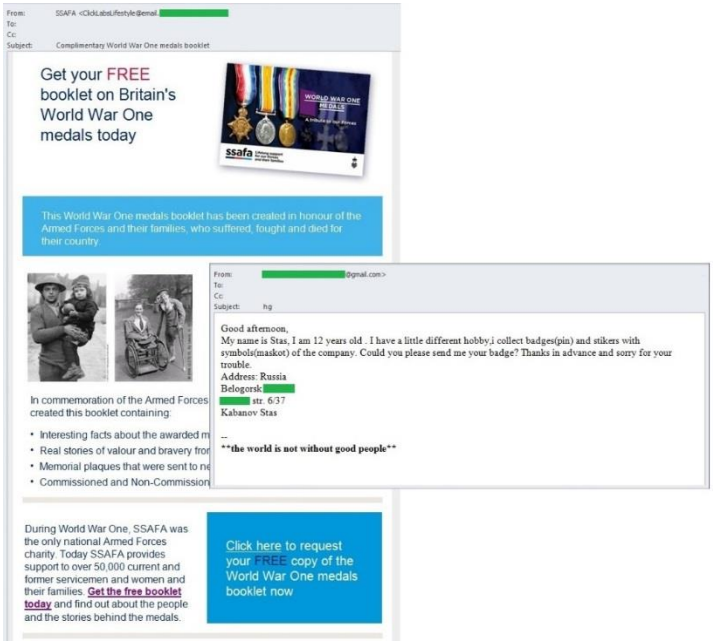


Secondo gli autori delle mailing di massa elaborate in varie lingue straniere, la fonte in assoluto più diffusa ed efficace per attirare nuovi clienti ed aumentare, di conseguenza, i propri profitti in Rete, è indubbiamente rappresentata da Facebook, il social network più diffuso del pianeta. Così, gli spammer hanno proposto di utilizzare le possibilità offerte dalla Rete per promuovere la pubblicità personale, inserire appositi redirect preposti a condurre a specifici post e fotografie. Naturalmente, gli spammer non hanno mancato di sottolineare che il numero dei potenziali clienti dipende, naturalmente, dalla qualità dei contenuti introdotti e dal desiderio, da parte degli utenti interessati, di cliccare, in seguito, sui link pubblicati all'interno dei social network. Per realizzare tutto ciò, è stato ad esempio proposto di utilizzare un software speciale, il cui acquisto poteva essere effettuato, per una determinata somma, direttamente attraverso la relativa campagna di spam. I siti web contenenti la descrizione di tale tipologia di software erano stati creati nel corso degli ultimi mesi e presentavano, a livello di denominazione, parole quali "clienti", "profitto", "Facebook".



Spam per collezionisti

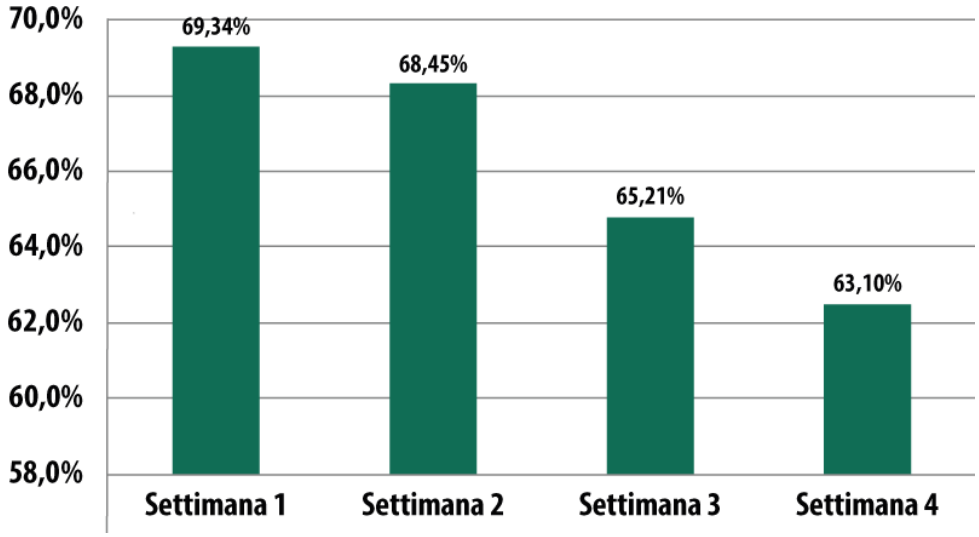
Segnaliamo infine, tra le mailing di massa più interessanti del mese, le campagne di spam destinate ai collezionisti, o allestite per conto di collezionisti. Agli utenti di lingua inglese, ad esempio, è stato proposto di ricevere un opuscolo gratuito, avente per tema le medaglie britanniche risalenti ai tempi della Prima Guerra Mondiale. I messaggi e-mail con questa generosa offerta risultavano essere stati inviati a nome di SSAFA, l'organizzazione caritatevole appositamente creata per sostenere le necessità e i bisogni degli ex-militari delle forze armate britanniche e delle loro famiglie. Il sito ufficiale di tale organizzazione, tuttavia, non riportava in alcun modo informazioni riguardo a tale attività di posta elettronica; le opinioni individuate in Rete hanno poi ulteriormente confermato come si trattasse di un mailing di natura indesiderata. Seguendo il link presente nel messaggio di spam, il destinatario dell'e-mail sarebbe giunto sulla pagina web appositamente predisposta per effettuare l'ordine del libretto - pagina all'interno della quale l'utente avrebbe dovuto poi inserire le proprie informazioni di contatto, numero di telefono incluso. Spesso, proprio con modalità simili, viene eseguita in Rete la raccolta di dati personali, i quali, successivamente, vengono utilizzati per fini pubblicitari. Sfruttando il database dei numeri di telefono dei potenziali clienti, precedentemente raccolti, possono essere in seguito allestite campagne telefoniche mirate, volte a condurre pratiche di hard selling relativamente a prodotti e servizi di ogni genere.



Un'ulteriore mailing di massa, dai toni e dai contenuti piuttosto simili a quella sopra descritta, è stata poi condotto da parte di un giovanissimo, sedicente collezionista. L'autore di tali messaggi riferiva innanzitutto del proprio hobby, ovvero quello di collezionare spille, badge e distintivi recanti il logo di società ed organizzazioni. In questo caso, il collezionista in erba pregava i destinatari delle e-mail di inviare il materiale di suo specifico interesse, allo scopo di arricchire la propria collezione; tali richieste sono state di fatto inviate a numerose società. Sebbene dietro a tali messaggi di posta elettronica non si celasse, probabilmente, alcun tipo di possibile frode, le e-mail in questione si sono ad ogni caso rivelate essere di natura indesiderata, e sono state pertanto classificate come spam a tutti gli effetti.

Le statistiche

Quota di spam nel traffico e-mail globale

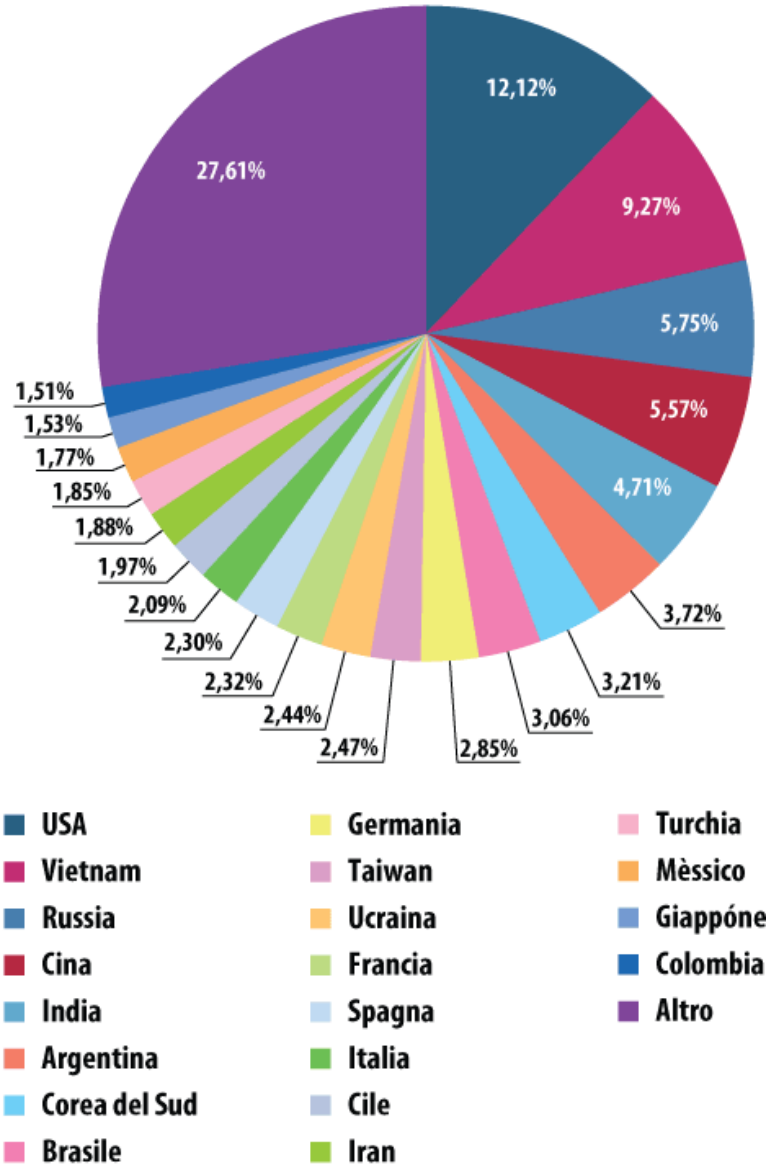


Quote di spam rilevate nel traffico di posta elettronica

Nel mese oggetto del presente report, la quota inerente ai messaggi "spazzatura" rilevati nel traffico globale di posta elettronica ha fatto registrare un decremento dello 0,7% rispetto all'analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 66,5% del volume complessivo di messaggi e-mail circolanti in Rete. Come evidenzia il grafico qui sopra riportato, la quota percentuale relativa alle e-mail indesiderate è diminuita in maniera stabile e progressiva lungo tutto l'arco del mese di settembre 2014. In effetti, nella prima settimana del mese qui analizzato, all'interno dei flussi di posta elettronica è stata rilevata una quota media di spam pari al 69,3%, mentre alla fine di settembre l'indice in questione ha raggiunto un valore decisamente inferiore (63,1%).

Geografia delle fonti di spam

Le posizioni di vertice della speciale graduatoria globale delle fonti di spam - relativa ai paesi dal cui territorio, nel mese di settembre 2014, sono state distribuite in Rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura" - presentano significative variazioni rispetto all'analogo rating del mese precedente. Rileviamo, ad ogni caso, come la leadership della classifica qui analizzata sia andata nuovamente ad appannaggio degli Stati Uniti (12%); rispetto all'indice rilevato nello scorso mese di agosto la quota relativa al paese nordamericano ha fatto tuttavia registrare una sensibile diminuzione, pari a quasi 4 punti percentuali. Al secondo posto della graduatoria da noi elaborata incontriamo il Vietnam (9,3%); la quota riconducibile al popoloso paese del Sud-Est asiatico risulta significativamente aumentata (+ 4,6%) rispetto all'analogo rating di agosto 2014. Il Vietnam ha quindi guadagnato ben due posizioni in classifica, salendo dalla quarta alla seconda piazza del rating relativo alla ripartizione geografica delle fonti di spam. Sul terzo gradino del podio virtuale di settembre troviamo poi la Russia (5,8%), passata, nell'arco di un mese, dalla seconda alla terza posizione del ranking qui esaminato, nonostante l'indice ascrivibile ai flussi di spam generati entro i confini della Federazione Russa abbia fatto registrare solo una lievissima flessione rispetto all'analoga quota riscontrata nel mese precedente.

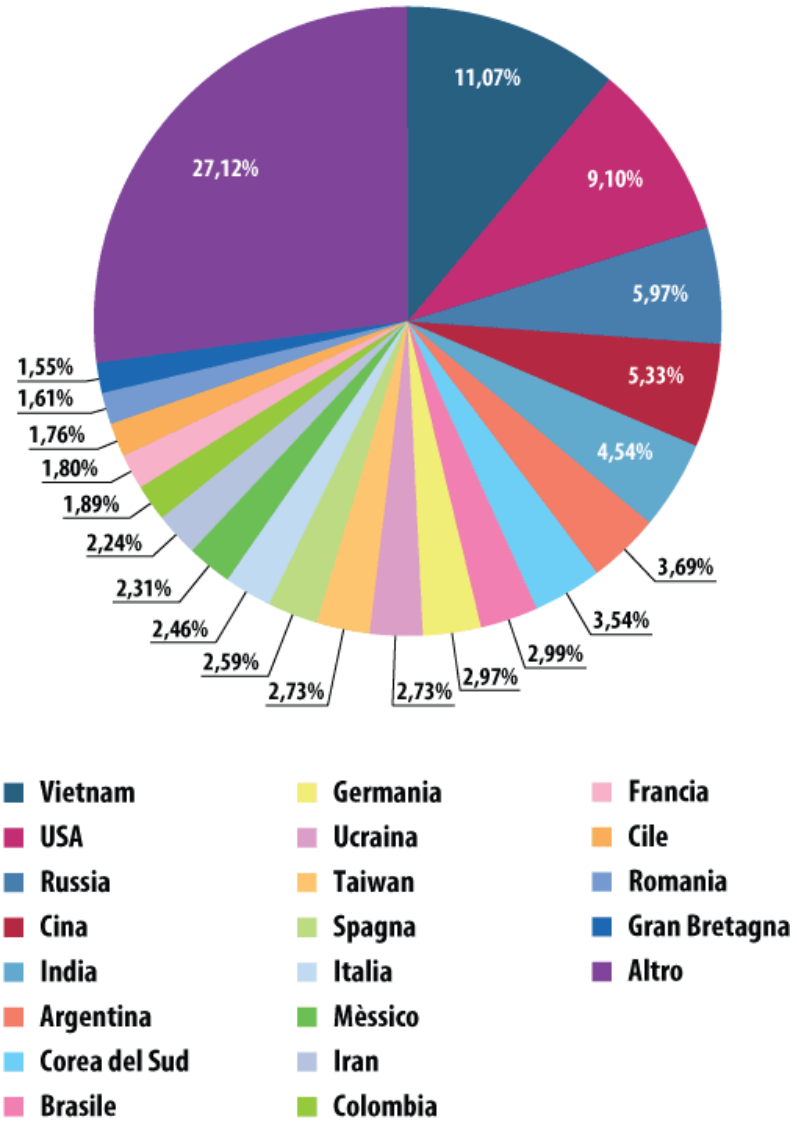


Geografia delle fonti di spam rilevate nel mese di settembre 2014 - Graduatoria su scala mondiale

La quarta posizione del rating in questione risulta occupata dalla Cina (5,6%); ricordiamo, a tal proposito, come un mese fa il colosso dell'Estremo Oriente occupasse la terza posizione della speciale graduatoria da noi stilata. Nel periodo oggetto del presente report, l'indice ascrivibile alla Repubblica Popolare Cinese ha ad ogni caso evidenziato un significativo aumento, pari, all'incirca, ad un punto percentuale. Al quinto posto della graduatoria troviamo poi l'India (4,7%), la cui quota risulta notevolmente cresciuta rispetto ad un mese fa, quando il paese asiatico occupava l'ultima posizione della TOP-10 relativa alla geografia delle fonti dello spam mondiale.

Allo stesso modo, ha fatto registrare un significativo incremento anche la quota ascrivibile ai flussi di messaggi e-mail indesiderati provenienti dalla Corea del Sud (3,2%); il paese dell'Estremo Oriente - che nell'analogo rating relativo al mese precedente occupava soltanto la quindicesima posizione della graduatoria - si è in tal modo collocato al settimo posto del ranking di settembre 2014, facendo complessivamente segnare un aumento di 1,3 punti percentuali rispetto alla quota per esso rilevata nello scorso mese di agosto. Per contro, l'indice ascrivibile alla Germania (2,9%) ha manifestato un'evidente flessione (- 0,7%) rispetto ad un mese fa; ciò ha determinato, per il paese europeo, la perdita di ben tre posizioni in classifica. Di fatto, la Germania è scesa dalla sesta alla nona posizione della

speciale graduatoria qui sopra riportata. La decima ed ultima posizione della TOP-10 da noi stilata risulta infine occupata da Taiwan, con una quota pari al 2,5%. Concludiamo la nostra breve analisi riguardo alle fonti geografiche dei messaggi e-mail indesiderati diffusi su scala mondiale osservando come, nel mese di settembre 2014, gli indici relativi ad alcuni paesi dell'Europa Occidentale, quali Francia, Spagna e Italia, si siano attestati su valori di poco superiori ai 2 punti percentuali.



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

Nel mese oggetto della nostra analisi, 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 ad appannaggio del Vietnam (11,1%). Il secondo gradino del podio virtuale di settembre 2014 risulta occupato dagli Stati Uniti (9,1%). Da parte sua, la Federazione Russa, con una quota pari al 6%, è andata a collocarsi al terzo posto del ranking relativo alle fonti dello spam europeo.

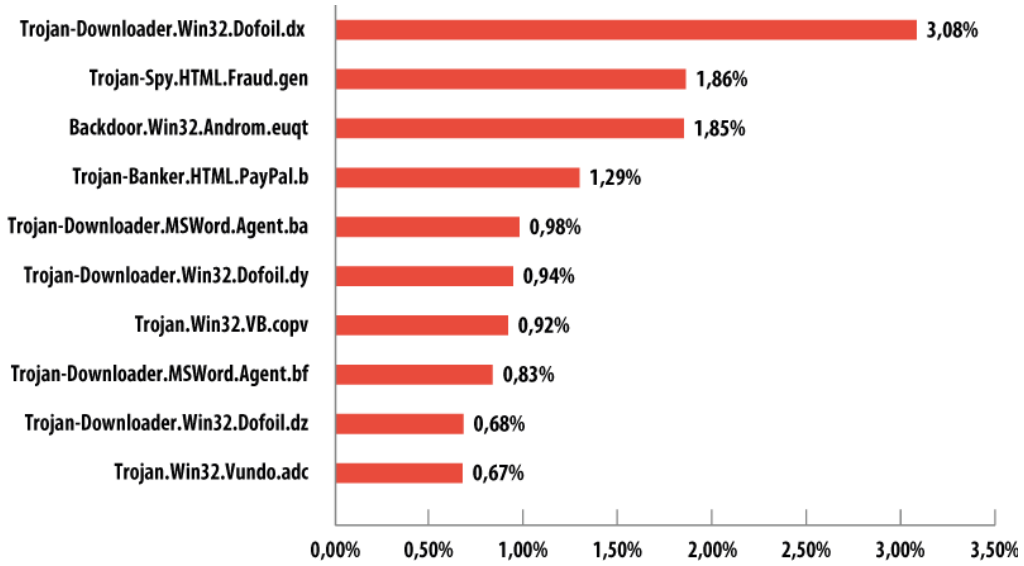
Continuando ad analizzare il grafico qui sopra inserito, osserviamo come Cina (5,3%), India (4,5%), Argentina (3,7%) e Corea del Sud (3,5%) siano andate a collocarsi, rispettivamente, al quarto, quinto, sesto e settimo posto della graduatoria. Le quote relative a Brasile, Germania ed Ukraina si sono poi

attestate attorno al 3%. Quest'ultima occupa, di fatto, l'ultima posizione della TOP-10 di settembre 2014.

Segnaliamo inoltre la presenza, nell'ambito della classifica qui analizzata, di Taiwan (2,7%), Spagna (2,6%), Italia (2,5%) e Messico (2,3%). Tali paesi occupano dall'undicesima alla quattordicesima posizione della graduatoria da noi elaborata. Al quindicesimo posto - quale fonte dei messaggi di spam distribuiti nelle e-mail box degli utenti situati sul territorio di paesi europei - troviamo l'Iran, con una quota pari al 2,2%. Osserviamo, infine, come gli indici relativi ai rimanenti paesi presenti nella speciale graduatoria di settembre 2014 non abbiano superato il valore del 2%.

Allegati maligni rilevati nel traffico e-mail

La TOP-10 del mese di settembre 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 maligni maggiormente diffusi nel traffico di posta elettronica nel mese di settembre 2014

La prima, la sesta e la nona posizione della speciale TOP-10 di settembre 2014 relativa ai software nocivi maggiormente presenti all'interno dei flussi e-mail globali risultano occupate da programmi malware appartenenti alla famiglia di Trojan-Downloader denominata Dofoil: si tratta, rispettivamente, di Trojan-Downloader.Win32.Dofoil.dx, Trojan-Downloader.Win32.Dofoil.dy e Trojan-Downloader.Win32.Dofoil.dz. I software dannosi riconducibili a tale tipologia provvedono a generare il download di un ulteriore programma maligno sul computer-vittima sottoposto ad attacco; in seguito, avvalendosi dell'aiuto fornito da tale malware, realizzano il furto delle più svariate informazioni sensibili custodite dall'utente (in particolar modo le password) ed inviano i dati illecitamente carpiti ai malintenzionati di turno.

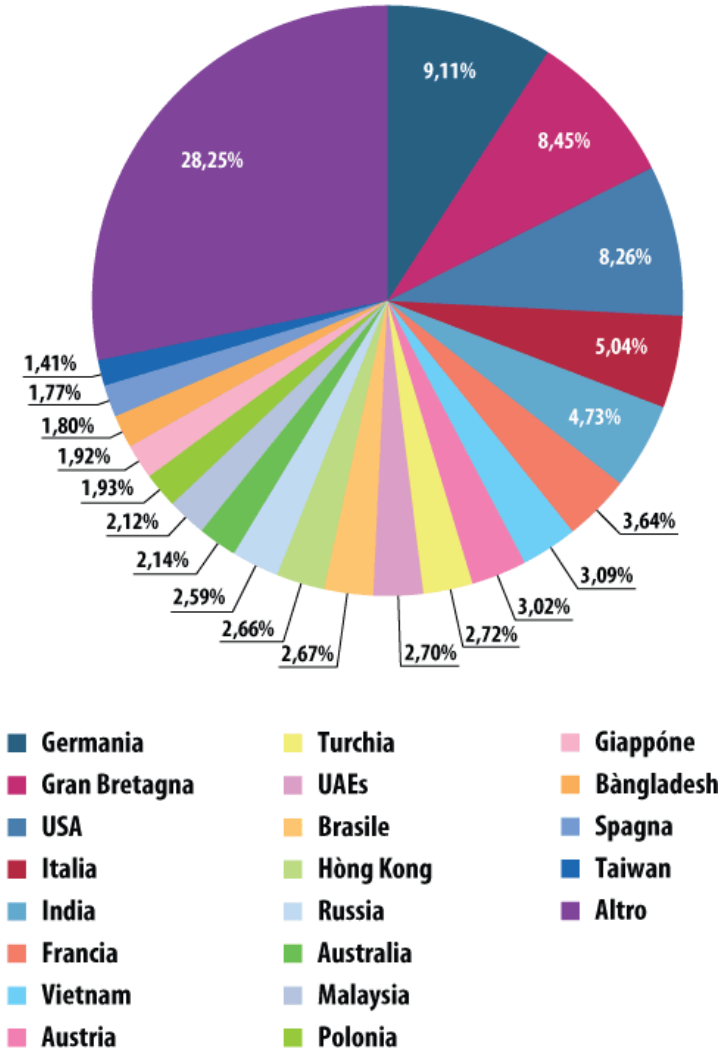
Al secondo posto della graduatoria di settembre 2014 relativa ai programmi nocivi maggiormente diffusi nel traffico e-mail globale troviamo il software malevolo classificato dagli esperti di sicurezza IT come Trojan-Spy.HTML.Fraud.gen, un vero e proprio habitué, ormai da lunga data, della classifica qui esaminata. Ricordiamo, nella circostanza, come tale software dannoso sia 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 Web; il Trojan-Spy in questione 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. Il malware Fraud.gen viene abitualmente distribuito dai malfattori della Rete tramite la posta elettronica, sotto forma di importanti notifiche e comunicazioni provenienti (in apparenza!) da famosi istituti bancari, celebri negozi Internet, software house di primaria importanza, etc.

La quarta posizione del ranking risulta occupata dal malware rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Trojan-Banker.HTML.PayPal.b; si tratta, a tutti gli effetti, di una pagina HTML di phishing, appositamente predisposta dai malintenzionati per imitare un particolare modulo di PayPal, il noto sistema di pagamento online. Tramite l'allegato maligno in questione, si invita il destinatario del messaggio e-mail a compilare un apposito modulo per aggiornare il proprio profilo PayPal, a seguito dell'introduzione di un nuovo sistema di sicurezza online. Il form presenta numerosi campi, quali: E-Mail Adresse (*indirizzo e-mail*), PayPal passwort (*password PayPal*), Vollständiger Name (*nome e cognome*), Nachname der Mutter (Fakultativ) (*cognome della madre - facoltativo*), Geburtsdatum (*data di nascita*), Telefonnummer (*numero di telefono*), Adresse (*indirizzo*), Stadt (*città*), Land (*paese*), Postzahl (*codice postale*), Kartennummer (*numero della carta di credito*), Verfallsdatum (*data di scadenza*), Kartenprüfnummer (*numero di sicurezza della carta*), VBV Passwort / MasterCard (*password Verified by Visa / MasterCard SecureCode*). A quanto pare, si tratta di un'azione cybercriminale specificamente indirizzata agli utenti di lingua tedesca titolari di account PayPal.

Il quinto e l'ottavo posto del rating analizzato nel presente capitolo del nostro consueto report mensile dedicato al fenomeno spam risultano occupati dai software nocivi denominati, rispettivamente, Trojan-Downloader.MSWord.Agent.ba e Trojan-Downloader.MSWord.Agent.bf. Tali programmi malware sono stati realizzati dai virus writer sotto forma di file provvisti di estensione *.doc, con tanto di apposita macro incorporata, scritta in VBA (Visual Basic for Applications), la quale viene automaticamente eseguita al momento dell'apertura del documento. In tal caso, è la stessa macro che, di fatto, provvede a generare il download e la successiva esecuzione del malware, il quale può essere costituito da software dannosi riconducibili alla famiglia Andromeda.

All'ultimo posto della TOP-10 relativa ai software dannosi maggiormente diffusi tramite i flussi e-mail globali troviamo infine il programma nocivo rilevato dalle nostre soluzioni anti-malware come Trojan.Win32.Vundo.adc. Tale software dannoso provvede a realizzare il download di ulteriori malware, quali, ad esempio, Trojan-Banker.Win32.Fibbit, un programma Trojan in grado di carpire i dati sensibili introdotti tramite determinate applicazioni di cui si avvale l'utente per eseguire le operazioni di banking online. Nella fattispecie, il Trojan in causa intercetta le sequenze dei tasti premuti dal cliente dell'istituto bancario, copia i dati dal buffer di scambio, ricerca i file certificato provvisti di estensione .jks, realizza degli screenshot e cerca, al contempo, di leggere il contenuto del file "keys.dat". Tutti i dati illegalmente carpiti vengono in primo luogo compressi all'interno di un archivio CAB, per poi essere inoltrati al server remoto predisposto dai malintenzionati di turno.



Ripartizione per paesi dei rilevamenti eseguiti dall'antivirus e-mail

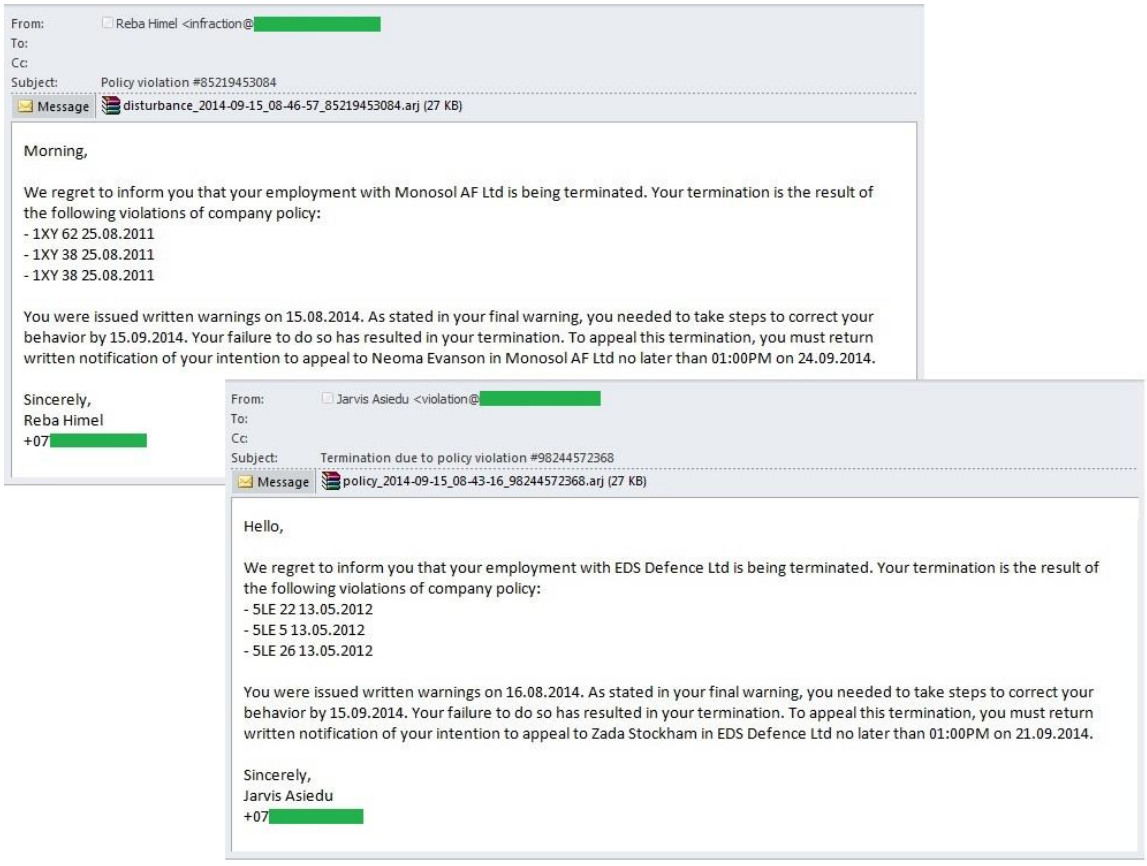
Così come nel mese precedente, le posizioni di vertice del rating riguardante i paesi nei quali il nostro modulo antivirus dedicato alla posta elettronica ha eseguito il maggior numero di rilevamenti volti a neutralizzare i programmi malware distribuiti attraverso i flussi e-mail - risultano occupate da Germania, Gran Bretagna e Stati Uniti, ovvero quei paesi che, tradizionalmente, in questi ultimi mesi, si stanno scambiando di continuo le rispettive posizioni in classifica nell'ambito di questa importante e significativa graduatoria del malware. Come evidenzia il grafico qui sopra inserito, nel mese oggetto del presente report la leadership del rating in questione è andata ad appannaggio della Germania (9,11%), mentre Gran Bretagna (8,45%) e Stati Uniti (8,26%) si sono collocati, rispettivamente, sul secondo e sul terzo gradino del podio virtuale.

La Federazione Russa (2,59%), da parte sua, è passata dalla quarta posizione (occupata in maniera alquanto sorprendente nell'analogo rating relativo allo scorso mese di agosto) alla tredicesima posizione della speciale graduatoria qui esaminata; in sostanza, nell'arco di un mese, l'indice relativo alla Russia ha fatto registrare una marcata diminuzione, pari a 4,14 punti percentuali.

Peculiarità e tratti caratteristici dello spam nocivo di settembre

Come abbiamo visto nella prima sezione del nostro report mensile dedicato al fenomeno spam, le tematiche connesse al mondo del lavoro e delle professioni (opportunità di impiego, assunzioni,

licenziamenti) hanno ampiamente caratterizzato i flussi di posta elettronica indesiderata di settembre 2014. Nel mese qui analizzato, tale specifico tema è stato ugualmente oggetto di numerose campagne di spam nocivo, volte a recapitare pericolosi allegati maligni nelle e-mail box degli utenti della rete. All'interno del traffico di spam di settembre sono stati ad esempio da noi individuate varie mailing di massa volti a recapitare messaggi di posta elettronica in cui, in maniera brusca e indelicata, si informava il destinatario del messaggio dell'avvenuta interruzione del rapporto di lavoro intrattenuto con una determinata azienda (i nominativi delle società in causa cambiavano, ovviamente, da messaggio a messaggio), a seguito di ripetute violazioni della policy aziendale. I messaggi sopra descritti riportavano persino, in dettaglio, i numeri e le date relative ai documenti societari contenenti le regole apparentemente violate. Attraverso tali e-mail si ribadiva, inoltre, che il destinatario del messaggio era stato in precedenza oggetto di tutta una serie di richiami scritti, nell'ultimo dei quali si affermava la necessità impellente di adottare particolari misure correttive riguardo al comportamento tenuto in seno all'azienda. Tuttavia, in considerazione del fatto che tali misure non erano state in alcun modo adottate dal dipendente entro la data indicata, il contratto di lavoro precedentemente in essere veniva di conseguenza interrotto.


From: Reba Himel <infraction@[redacted]
To:
Cc:
Subject: Policy violation #85219453084
Message disturbance_2014-09-15_08-46-57_85219453084.arj (27 KB)

Morning,

We regret to inform you that your employment with Monosol AF Ltd is being terminated. Your termination is the result of the following violations of company policy:
- 1XY 62 25.08.2011
- 1XY 38 25.08.2011
- 1XY 38 25.08.2011

You were issued written warnings on 15.08.2014. As stated in your final warning, you needed to take steps to correct your behavior by 15.09.2014. Your failure to do so has resulted in your termination. To appeal this termination, you must return written notification of your intention to appeal to Neoma Evanson in Monosol AF Ltd no later than 01:00PM on 24.09.2014.

Sincerely,
Reba Himel
+07[redacted]

From: Jarvis Asiedu <violation@[redacted]
To:
Cc:
Subject: Termination due to policy violation #98244572368
Message policy_2014-09-15_08-43-16_98244572368.arj (27 KB)

Hello,

We regret to inform you that your employment with EDS Defence Ltd is being terminated. Your termination is the result of the following violations of company policy:
- 5LE 22 13.05.2012
- 5LE 5 13.05.2012
- 5LE 26 13.05.2012

You were issued written warnings on 16.08.2014. As stated in your final warning, you needed to take steps to correct your behavior by 15.09.2014. Your failure to do so has resulted in your termination. To appeal this termination, you must return written notification of your intention to appeal to Zada Stockham in EDS Defence Ltd no later than 01:00PM on 21.09.2014.

Sincerely,
Jarvis Asiedu
+07[redacted]

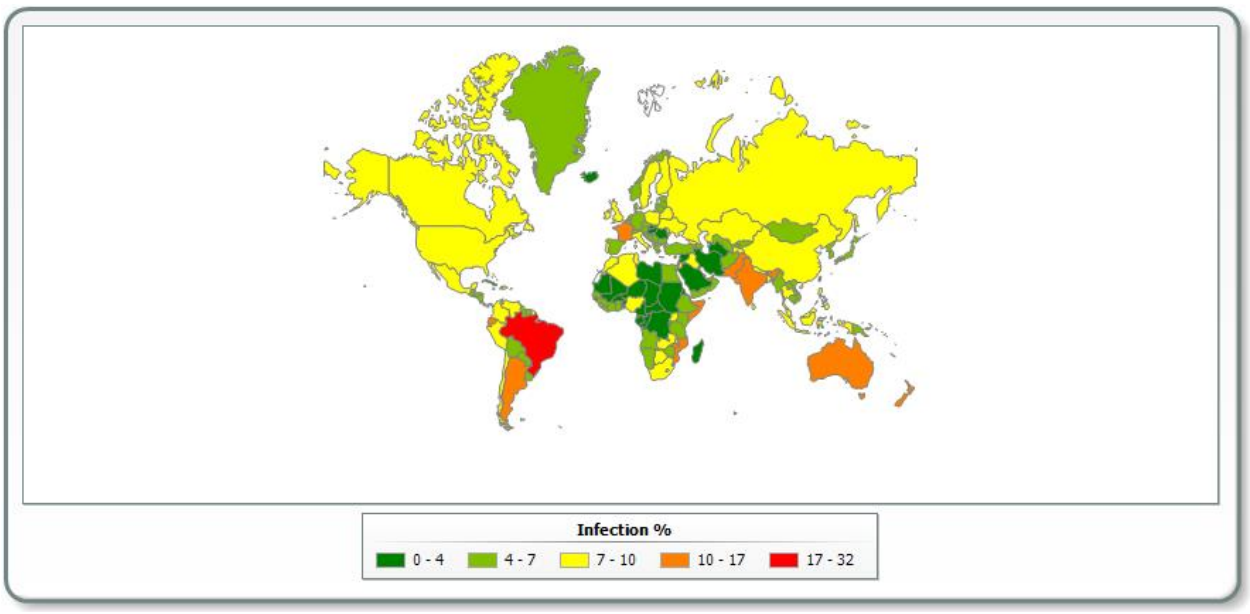
Per presentare eventuale ricorso contro tale provvedimento disciplinare, il destinatario dell'e-mail si sarebbe comunque potuto rivolgere ad un determinato studio legale, non oltre il termine specificato nel corpo del messaggio. Le e-mail distribuite nell'ambito di tali campagne di spam nocivo recavano in allegato un file archivio provvisto di estensione .arj, il quale, apparentemente, avrebbe dovuto contenere la dovuta documentazione riguardo alle presunte violazioni del regolamento aziendale, documentazione che il potenziale utente-vittima, secondo le intenzioni dei malfattori, avrebbe dovuto consultare aprendo il file appositamente allegato. In realtà, l'archivio in questione non custodiva null'altro se non un file nocivo, e più precisamente un temibile trojan downloader riconducibile alla famiglia di malware classificata dagli esperti di sicurezza IT con la denominazione di Trojan-

Downloader.Win32.Cabby. Si tratta di un programma maligno appositamente creato e sviluppato dai virus writer per generare il download - sul computer-vittima sottoposto ad attacco informatico - di ulteriori software nocivi, incluso numerose varianti di malware riconducibili alla famiglia di Trojan conosciuta con l'appellativo di Zbot.

Phishing

Nel mese di settembre 2014, sui computer degli utenti dei prodotti Kaspersky Lab si sono complessivamente registrati 18.779.357 rilevamenti eseguiti grazie al componente di sicurezza "Anti-phishing", ovvero 13.874.415 rilevamenti in meno rispetto all'analogo valore riscontrato relativamente allo scorso mese di agosto. Con la fine del lungo periodo caratterizzato dalle ferie e dalle vacanze estive e con la conseguente ripresa delle consuete attività lavorative, la quota relativa al phishing subisce, tradizionalmente, una significativa contrazione. Occorre tuttavia tenere ugualmente in considerazione il fatto che, lungo tutto l'arco del mese di settembre, si succedono, per le aziende, eventi, manifestazioni, presentazioni ed altri avvenimenti di rilievo. Spesso, alla vigilia di tali eventi, viene rilevato un sensibile aumento delle attività condotte in rete dai phisher, il che produce, in genere, verso la fine della stagione estiva, un temporaneo incremento del numero complessivo dei tentativi di truffa orditi tramite subdole campagne di phishing.

Nel mese oggetto del presente report, la poco ambita leadership del rating relativo ai paesi maggiormente sottoposti agli attacchi portati dai phisher è andata nuovamente ad appannaggio del Brasile (17,8%); l'indice attribuibile al colosso del continente latino-americano, tuttavia, ha presentato una significativa flessione rispetto al mese precedente, quantificabile in 1,7 punti percentuali. L'Australia, che deteneva la prima posizione nell'ambito dell'analoga graduatoria di agosto 2014, è andata ad occupare la terza posizione della classifica qui esaminata, con una quota pari all' 11,1%. Come evidenzia la tabella qui sotto riportata, il secondo posto nel rating di settembre 2014 è andato ad appannaggio dell'India (13,4%). In quarta ed in quinta posizione, nella speciale classifica geografica del phishing da noi stilata, si sono poi collocati, rispettivamente, gli Emirati Arabi Uniti (10,5%) e la Francia (10,4%).



Ripartizione geografica degli attacchi di phishing - Situazione relativa al mese di settembre 2014*

** Quote percentuali relative al numero di utenti sui computer dei quali si sono registrati rilevamenti da parte del sistema "Anti-phishing", rispetto al numero complessivo di utenti dei prodotti Kaspersky Lab nel paese.*

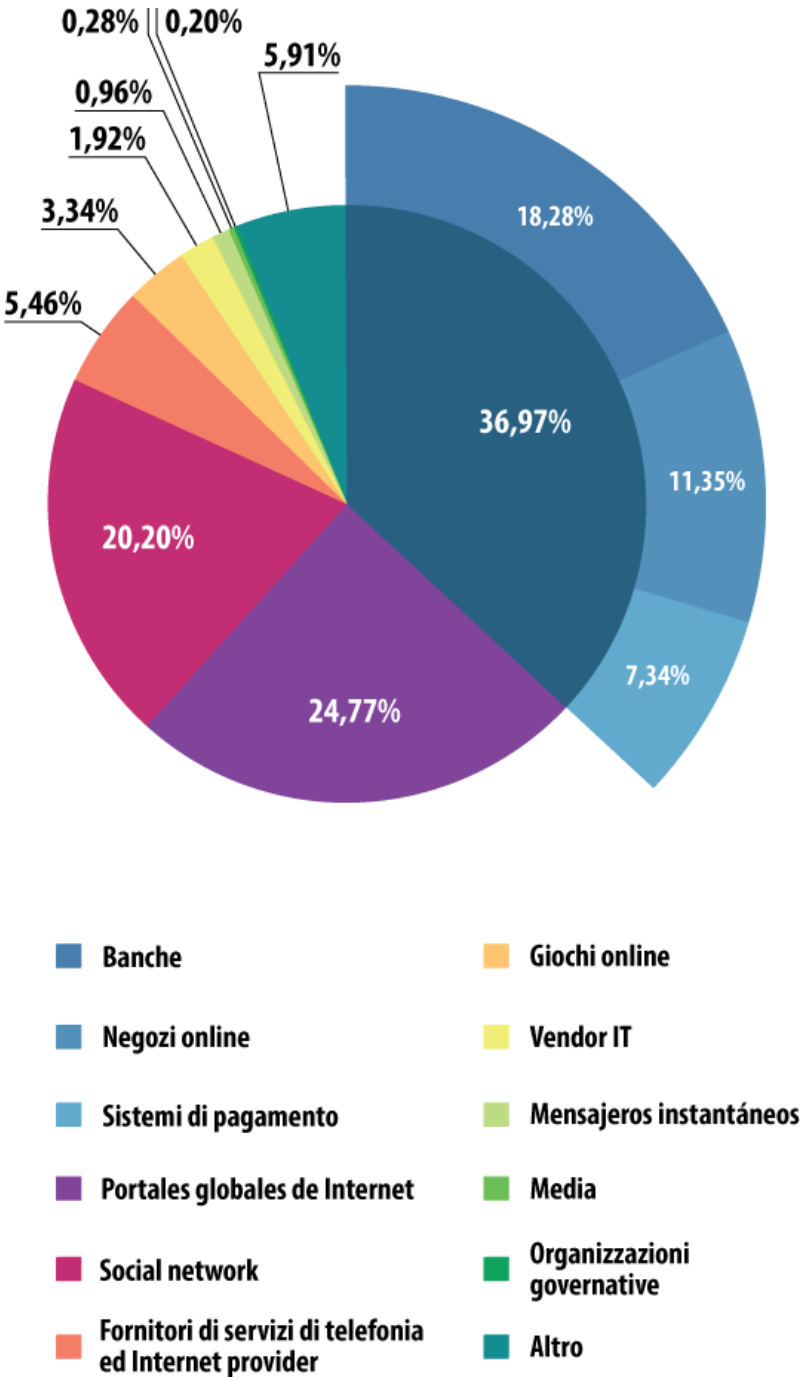
TOP-10 relativa ai paesi in cui sono state riscontrate le quote percentuali più elevate di utenti sottoposti ad attacchi di phishing:

	Paese	% di utenti sottoposti ad attacco
1	Brasile	17,8
2	India	13,4
3	Australia	11,2
4	Emirati Arabi Uniti	10,5
5	Francia	10,4
6	Canada	9,9
7	Cina	9,9
8	Colombia	9,4
9	Bangladesh	9,0
10	Gran Bretagna	8,0

Quadro delle organizzazioni sottoposte agli attacchi di phishing

Le statistiche relative agli obiettivi presi di mira dagli assalti dei phisher si basano sui rilevamenti eseguiti dal componente euristico implementato nel sistema "Anti-phishing". Il componente euristico del sistema "Anti-phishing" entra in azione nel momento stesso in cui l'utente clicca su un link maligno preposto a condurre verso una pagina di phishing, nel caso in cui le informazioni relative a tale pagina non risultino ancora presenti all'interno dei database appositamente allestiti da Kaspersky Lab. In tal caso, non riveste alcuna importanza la specifica modalità attraverso la quale viene effettuato il click, da parte dell'utente, su tale collegamento: può in effetti trattarsi sia di un click eseguito su un link presente in un'e-mail di phishing, oppure in un messaggio inserito all'interno di un social network, sia di una situazione determinata dall'attività dannosa svolta da un programma malware. Non appena il sistema di protezione qui sopra descritto entra in azione, l'utente visualizza sul proprio browser un apposito banner di avvertimento riguardo alla possibile minaccia cui sta per andare incontro.

Così come nello scorso mese di agosto, al primo posto della graduatoria troviamo la nuova categoria da noi recentemente definita, comprendente i portali di posta elettronica e di ricerca, con una quota pari al 24,7%; rileviamo, in questo caso, come l'indice percentuale ascrivibile agli attacchi di phishing complessivamente condotti nei confronti di tali risorse web abbia ad ogni caso fatto registrare un sensibile decremento rispetto ad un mese fa, quantificabile in 6,1 punti percentuali. Sono invece aumentati, peraltro in maniera significativa (+ 2,8%), gli assalti di phishing organizzati a danno della categoria che raggruppa i social network; in settembre, la quota relativa alle reti sociali si è in effetti attestata su un valore medio pari al 20,2%.



Ripartizione per categorie delle organizzazioni sottoposte agli attacchi di phishing* nel corso del mese di settembre 2014

Complessivamente, al phishing di natura finanziaria è risultato riconducibile il 36,97% del volume complessivo degli attacchi rilevati grazie al componente euristico implementato nel sistema "Anti-phishing"; tale indice ha quindi evidenziato un aumento dell'1,7% rispetto all'analogo valore rilevato nello scorso mese di agosto. Nella fattispecie, è stato osservato un lieve incremento percentuale (+ 0,5%) per ciò che riguarda la quota relativa ai rilevamenti eseguiti rispetto alla categoria "Istituti bancari" (18,28%). Le due ulteriori categorie "finanziarie" abitualmente prese in considerazione, ovvero "Negozi Internet" (11,35%) e "Sistemi di pagamento" (7,34%) hanno anch'esse fatto registrare un incremento dell'indice percentuale ad esse attribuibile, pari, rispettivamente, all' 1,4% ed allo 0,5%.

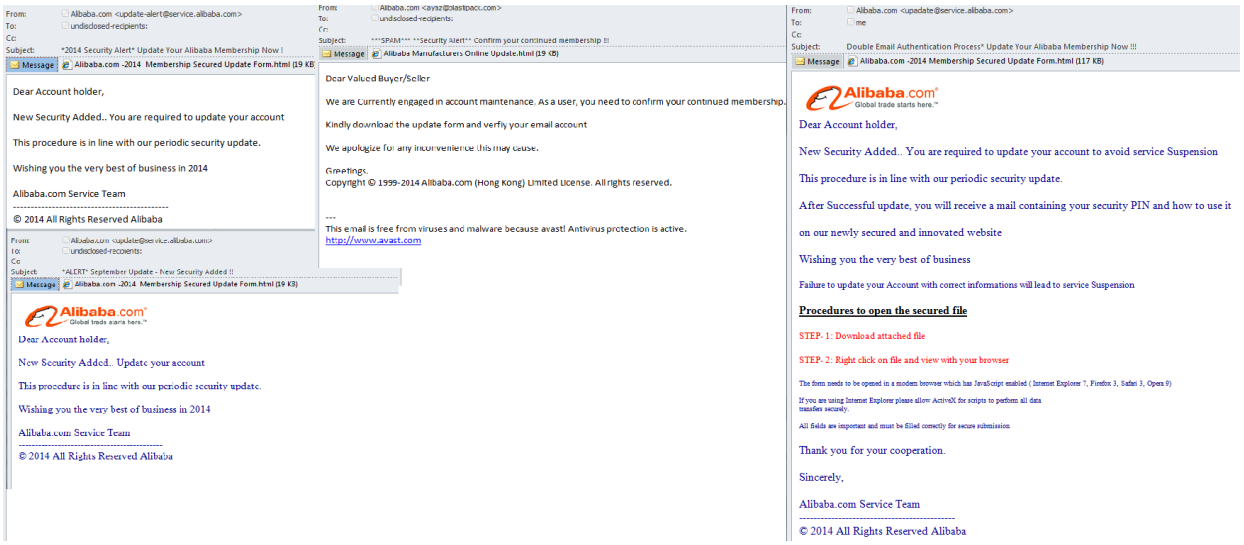
TOP-3 relativa alle organizzazioni maggiormente sottoposte ad attacchi di phishing

	Organizzazione	% di rilevamenti eseguiti
1	Facebook	11,16%
2	Yahoo!	7,10%
3	Google	6,31%

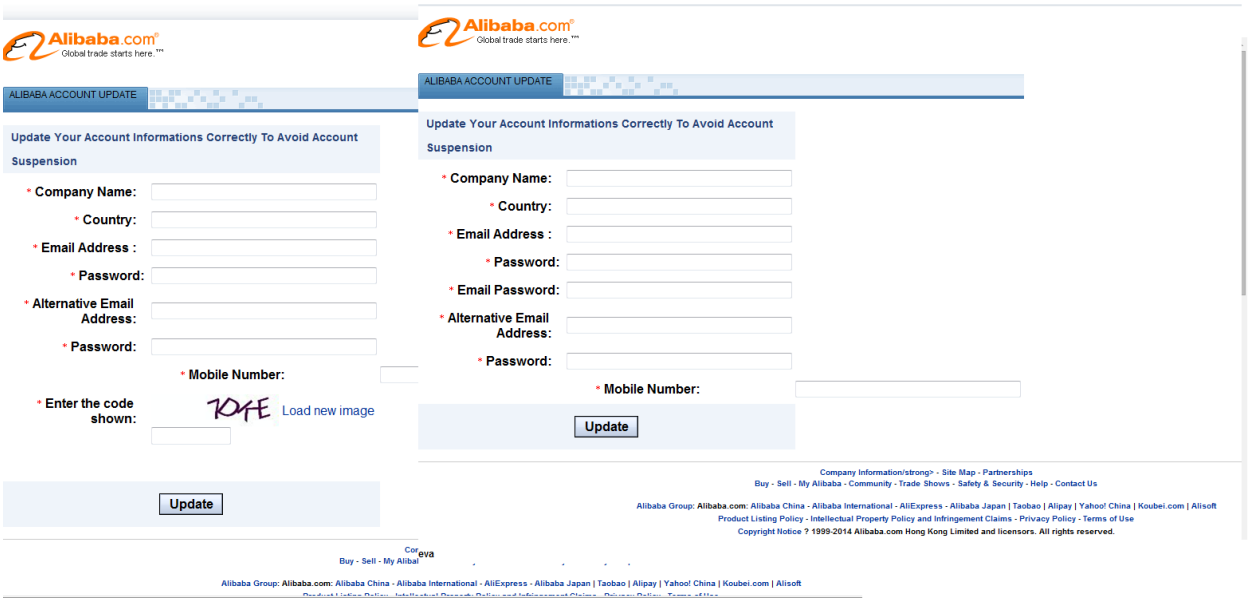
Nel mese di settembre 2014, la leadership della speciale graduatoria riguardante le organizzazioni maggiormente sottoposte agli assalti orditi dai phisher è andata ad appannaggio di Facebook; la quota ascrivibile al social network più diffuso del pianeta ha fatto registrare un aumento di 1,1 punti percentuali rispetto allo scorso mese di agosto ed è quindi risultata pari all' 11,1% del numero complessivo di rilevamenti eseguiti grazie al componente euristico "Anti-phishing". Il secondo gradino della TOP-3 qui esaminata, come evidenzia l'apposita tabella, risulta occupato dal motore di ricerca Yahoo!, con un indice pari al 7,1%. Continuando la nostra breve analisi sottolineiamo come, nel mese di settembre 2014, si siano in pratica dimezzati gli attacchi organizzati dai phisher nei confronti di Google; i link di phishing preposti a condurre gli utenti verso pagine web contraffatte volte ad imitare le pagine Internet ufficiali relative ai servizi online offerti da Google hanno in effetti costituito "solo" il 6,3% dei rilevamenti compiuti dallo speciale modulo "Anti-phishing". Ricordiamo, a tal proposito, che Google capeggiava l'analoga graduatoria di agosto, mentre nel mese oggetto del presente report la società di Mountain View è andata ad occupare l'ultima posizione del rating riguardante le organizzazioni più frequentemente bersagliate dai phisher.

È stata da noi rilevata, all'interno del traffico di spam che ha caratterizzato i flussi di posta elettronica di settembre 2014, la conduzione di numerose campagne di phishing specificamente indirizzate al furto di login e password relativi agli account aperti dagli utenti della Rete presso Alibaba.com, l'importante ed ormai popolarissima piattaforma di compravendita su scala globale allestita da un noto gruppo cinese, composto da una serie di compagnie operanti principalmente nella sfera del commercio elettronico (piattaforme commerciali online, specifici motori di ricerca dedicati allo shopping, servizi "in-the-cloud"). Attraverso tali e-mail ingannevoli, i phisher hanno cercato di convincere le potenziali vittime, ovvero i destinatari dei messaggi di posta in questione, riguardo alla necessità di provvedere al più presto all'aggiornamento dei dati relativi al proprio account, oppure di confermare l'utilizzo corrente di quest'ultimo, adottando, quale pretesto, l'introduzione di un nuovo sistema di sicurezza nell'ambito della nota piattaforma commerciale, oppure la conduzione temporanea di operazioni di manutenzione degli account degli utenti. Per allestire le e-mail di phishing, i malintenzionati sono ricorsi sia all'utilizzo del logo ufficiale della società Alibaba.com, sia all'inserimento della firma automatica abitualmente apposta da quest'ultima in calce ai propri messaggi di posta elettronica. Oltre a ciò, nel tentativo di catalizzare al massimo l'attenzione dei destinatari delle e-mail fraudolente, i phisher si sono preoccupati di adottare vari colori per il testo presente nel messaggio; talvolta, poi, i criminali hanno addirittura provveduto ad inserire la consueta notifica standard, emessa tramite l'antivirus, riguardo all'assenza di eventuali minacce informatiche (virus e malware) nell'ambito del messaggio ricevuto dall'utente. Inoltre, come evidenziano gli screenshot esemplificativi qui sotto riportati, nel campo <From>, in qualità di nome del mittente, è stato sempre indicato Alibaba.com, mentre per ciò che riguarda gli indirizzi di posta elettronica inseriti in tali messaggi di phishing, sono stati principalmente utilizzati nomi di dominio

del tutto legittimi. Tuttavia, se andiamo ad esaminare attentamente le e-mail fraudolente sopra descritte, notiamo subito come, in alcune delle mailing di massa organizzate in questo caso dai phisher, siano presenti errori di ortografia a livello di indirizzi del mittente, mentre traspare ugualmente, in tutta evidenza, come certi nomi di dominio non siano affatto riconducibili alla società cinese.



Le relative pagine di phishing, poi, erano state inserite direttamente nelle e-mail fasulle e presentavano tutte quante, in pratica, lo stesso layout e la stessa composizione grafica. Secondo le intenzioni dei malfattori, il destinatario del messaggio fraudolento avrebbe dovuto inserire, nei campi predisposti dai phisher, non solo l'indirizzo di posta elettronica e la password utilizzata per accedere alla piattaforma commerciale, ma anche il nome dell'azienda, il paese di provenienza, e addirittura il proprio numero di telefonia mobile. In tal modo, i malintenzionati avrebbero carpito preziose informazioni aggiuntive riguardo alle vittime dell'operazione di phishing da essi allestita, dati che, successivamente, avrebbero potuto essere utilizzati per gli scopi più diversi.



Conclusioni

Nel mese di settembre 2014 la quota dello spam presente nel traffico di posta elettronica mondiale ha fatto registrare un decremento dello 0,7% rispetto all'analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 66,5% del volume complessivo di messaggi e-mail circolanti in rete. Le posizioni di vertice della speciale graduatoria a livello globale delle fonti di spam - relativa ai paesi dal cui territorio, nel mese oggetto della nostra analisi, sono state distribuite in rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura" - risultano occupate, rispettivamente, da Stati Uniti (12%), Vietnam (9,3%) e Russia (5,8%).

La prima posizione della speciale TOP-10 di settembre 2014 relativa ai software nocivi maggiormente presenti all'interno dei flussi e-mail mondiali è andata ad appannaggio di un Trojan-Downloader appartenente alla famiglia di malware denominata Dofoil; tale software nocivo viene di fatto utilizzato dai cybercriminali per generare il download di ulteriori programmi maligni sul computer-vittima sottoposto ad attacco.

Nel mese di settembre si sono complessivamente registrati 18.779.357 rilevamenti eseguiti grazie al componente di sicurezza "Anti-phishing" di Kaspersky Lab. I dati statistici da noi raccolti evidenziano come la leadership del rating relativo ai paesi più frequentemente sottoposti agli attacchi organizzati dai phisher sia andata ad appannaggio del Brasile; l'indice relativo al paese sudamericano si è attestato su un valore complessivo pari al 17,8%. L'Australia, che deteneva la prima posizione nell'analoga graduatoria di agosto 2014, è andata ad occupare la terza posizione di tale classifica, con una quota pari all'11,1%. Così come nello scorso mese di agosto, al primo posto della speciale graduatoria inerente alle organizzazioni - suddivise per categorie - maggiormente bersagliate dai phisher troviamo la categoria che raggruppa i portali di posta elettronica e di ricerca, con una quota complessiva pari al 24,7%. L'indice relativo alle campagne di phishing riconducibili alla sfera finanziaria ha evidenziato un aumento dell'1,7% rispetto ad un mese fa, raggiungendo così un valore medio pari al 36,9%. In settembre, la leadership della TOP-3 riguardante le organizzazioni maggiormente sottoposte, individualmente, agli assalti orditi dai phisher, è andata ad appannaggio di Facebook; la quota ascrivibile al celebre social network è risultata pari all'11,1%. Nell'ambito di tale classifica abbiamo assistito ad una chiara redistribuzione delle posizioni precedentemente occupate.

Nel periodo oggetto della nostra analisi, i truffatori "nigeriani" hanno sfruttato nuove tematiche per la conduzione delle loro mailing di massa fraudolente, passando così dagli avvenimenti politici che si sono prodotti in Ukraina nel corso di questi ultimi mesi alla grave emergenza sanitaria causata a livello globale dal virus Ebola, con i numerosi casi di contagio che si sono via via manifestati in diversi paesi, costantemente ed attentamente riportati dai mass media di tutto il mondo.

Nell'ambito delle consuete campagne di spam pubblicitario, volte a reclamizzare i prodotti ed i servizi più disparati, ci siamo imbattuti in varie mailing di massa ispirate alle tematiche suggerite sia dal Labor Day - l'importante festività nazionale statunitense dedicata ai lavoratori, tradizionalmente celebrata negli USA il primo lunedì di settembre - sia dalle principali festività dell'imminente stagione invernale. Nel corso dei prossimi mesi - sino a dicembre, periodo in cui il volume dei messaggi di spam improntati alle classiche tematiche di Natale e Capodanno raggiunge, come al solito, il proprio picco massimo - ci attendiamo un progressivo aumento della quota relativa alle campagne di spam dedicate a tali festività invernali.