Lo spam nel mese di Maggio 2014

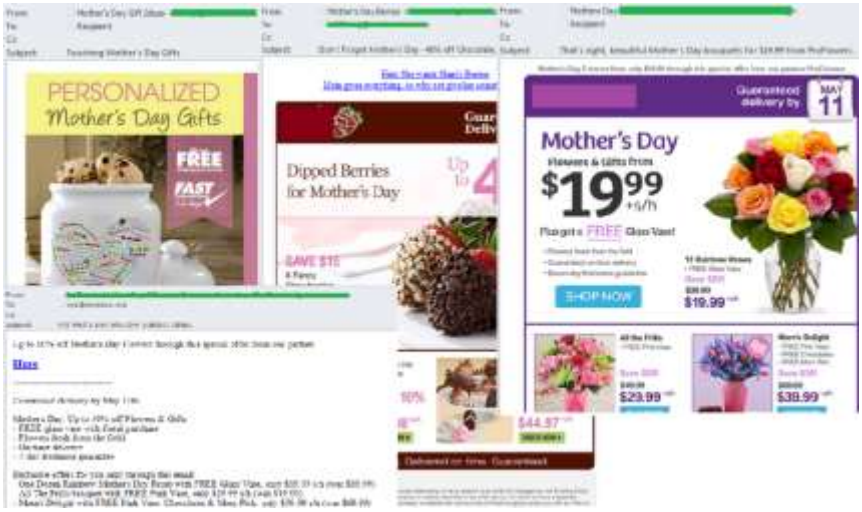
Sommario

Le peculiarità del mese

Iniziamo il nostro consueto report mensile dedicato all'analisi del persistente fenomeno della diffusione, all'interno dei flussi di posta elettronica globali, delle cosiddette e-mail "spazzatura", osservando come, alla vigilia della stagione estiva, gli spammer abbiano distribuito nelle caselle di posta degli utenti del web un considerevole numero di messaggi indesiderati preposti a promuovere la vendita, ai potenziali clienti della Rete, di sementi da giardino e da prato, così come di piante e piantine di ogni genere. Inoltre, nel mese di maggio 2014, nel vasto segmento anglofono dello spam ispirato alle principali tematiche suggerite dalle festività stagionali del momento, è stato dato ampio spazio alla celebrazione della Festa della Mamma; più precisamente, gli spammer di ogni latitudine hanno "sfruttato" tale ricorrenza, particolarmente sentita, al fine di pubblicizzare articoli da regalo di vario genere, sotto forma, in particolar modo, di prodotti floreali, dolci e realizzazioni di pasticceria.

Lo spam dedicato alla Festa della Mamma

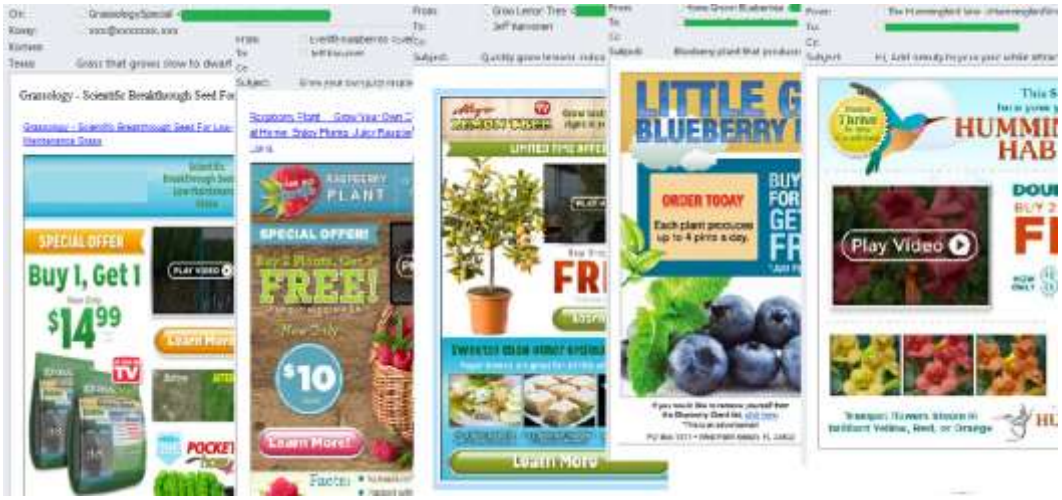
Come era lecito attendersi, nel mese oggetto del nostro report gli spammer hanno ampiamente rivolto le loro attenzioni alle tematiche inerenti alla celebrazione della Festa della Mamma, inondando, come al solito, le e-mail box degli utenti della Rete di messaggi di posta elettronica volti a reclamizzare i più disparati articoli floreali e prodotti dolciari, confezionati quasi sempre in veste di ambito regalo in occasione della suddetta ricorrenza. Per cercare di attirare al massimo l'attenzione dei destinatari di tali variopinti messaggi di spam, accuratamente elaborati, gli autori delle e-mail indesiderate in questione hanno posto ampiamente in risalto il nome della sentita festività di maggio, promettendo, tra l'altro, consistenti sconti sulla vendita dei prodotti pubblicizzati, nonché una tempestiva consegna degli articoli acquistati, da effettuarsi proprio il giorno stesso della celebrazione della Festa della Mamma.



E' tuttavia risultato come la maggior parte dei link inseriti dagli spammer nel corpo dei suddetti messaggi conducesse, di fatto, i destinatari delle e-mail, verso appositi redirect, preposti a reindirizzare gli utenti non tanto sui siti web dedicati agli articoli da regalo via via pubblicizzati, quanto piuttosto su pagine web dai contenuti del tutto diversi. Tali redirect erano stati a loro volta collocati all'interno di domini di recente creazione, utilizzati, nella circostanza, non solo nell'ambito dei collegamenti ipertestuali presenti nel corpo del messaggio di spam, ma anche in qualità di nome di dominio relativamente all'indirizzo di posta elettronica del mittente. E' di particolare interesse porre in evidenza come alcuni dei messaggi da noi esaminati presentassero ugualmente, al loro interno, un link apparentemente preposto ad una funzionalità del tutto legittima e corretta, ovvero la cancellazione del nominativo dell'utente dall'elenco degli indirizzi di posta interessati dal mailing di massa. In realtà, il suddetto link veniva subdolamente utilizzato dagli spammer per raccogliere gli indirizzi di posta elettronica degli utenti, account da impiegare, successivamente, nell'ambito delle nuove campagne di spam di volta in volta allestite.

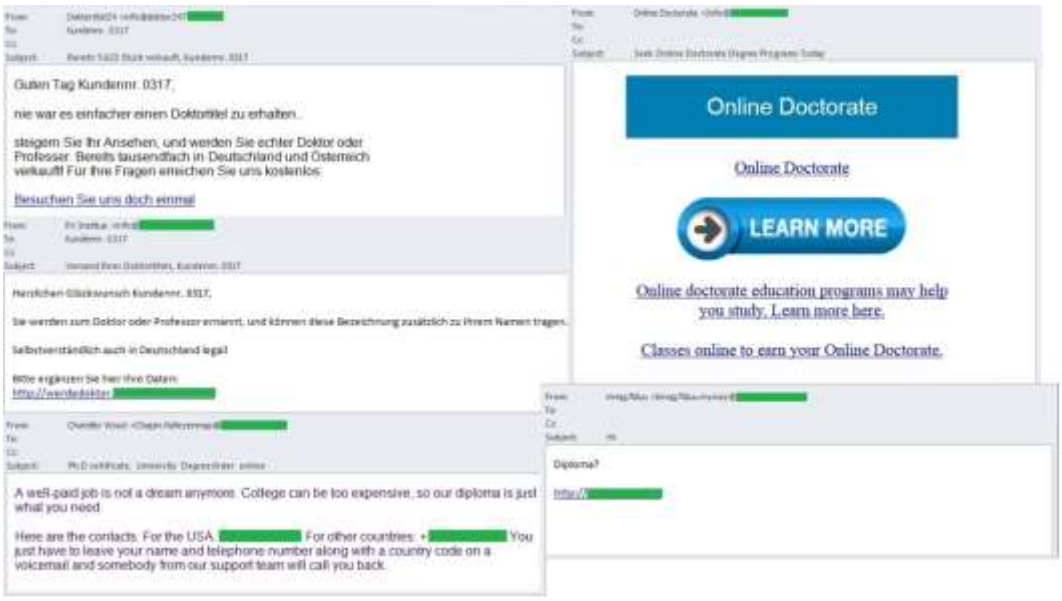
Spam per giardinieri e orticoltori

Non è di certo un segreto il fatto che gli americani tengano in particolare considerazione e curino assiduamente il terreno adiacente alle loro abitazioni; di fatto, il giardinaggio rappresenta uno degli hobby preferiti, ed in assoluto più praticati, da parte dei cittadini statunitensi. Non costituisce quindi motivo di particolare sorpresa l'aver rilevato come, lungo tutto l'arco del mese oggetto della nostra analisi, gli spammer si siano "dilettati" ad elaborare ed inviare in Rete un cospicuo numero di messaggi e-mail in lingua inglese contenenti le più svariate proposte ed offerte riguardo all'acquisto di sementi da prato e da giardino, così come di piante e piantine di ogni tipo, in particolar modo bacche e frutti esotici. I potenziali acquirenti di tale genere di articoli sono stati spesso allettati da frasi del tipo "offerta speciale", oppure "offerta limitata"; di frequente, inoltre, gli spammer hanno promesso una piantina in omaggio in caso di acquisto di almeno altre due. I messaggi in questione presentavano realizzazioni grafiche molto ben curate e piacevoli immagini multicolori, sulle quali, in genere, risultava direttamente inserito il consueto collegamento ipertestuale. E' infine davvero interessante rilevare come la maggior parte dei domini verso i quali avrebbero condotto tali link, fosse stata creata addirittura meno di una settimana prima dell'inizio della conduzione di tali campagne di spam.



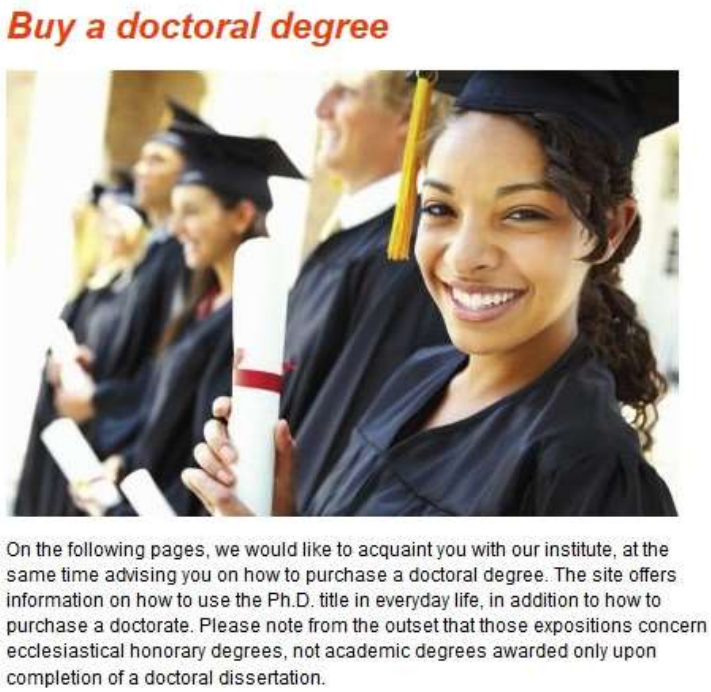
Diplomi e titoli accademici

All'interno dei flussi di spam che hanno caratterizzato il traffico di posta elettronica del mese di maggio 2014 sono stati individuati numerosi mailing di massa volti a pubblicizzare istituti scolastici e college in grado di fornire servizi di insegnamento a distanza. I nostri esperti si sono tuttavia imbattuti, al tempo stesso, in varie campagne di spam attraverso le quali gli spammer, in maniera alquanto disinvolta, hanno proposto ai destinatari dei messaggi e-mail l'acquisto di diplomi e titoli accademici. Per ottenere l'ambito titolo, si sarebbe rivelato sufficiente effettuare una semplice donazione in favore di un istituto ecclesiastico, il quale, in maniera del tutto legittima ed ufficiale, avrebbe poi insignito il benefattore di un dottorato honoris causa.



In Germania, ad esempio, soltanto le università e gli istituti di istruzione superiore equivalenti hanno il diritto di conferire lauree e titoli accademici. La situazione si presenta tuttavia in maniera diversa quando si parla di lauree e dottorati ad honorem in forma ecclesiastica, di fatto rilasciati a nome della Chiesa. E sebbene l'ottenimento di simili titoli non presupponga in alcun modo il completamento dell'abituale ciclo di studi, così come nessuna stesura o dissertazione di tesi, i mailing di massa che convogliano nelle caselle di posta elettronica degli utenti del web proposte relative a servizi del genere

non esitano comunque a presentare le loro pubblicità utilizzando immagini che richiamano esplicitamente tematiche legate allo studio e all'istruzione.

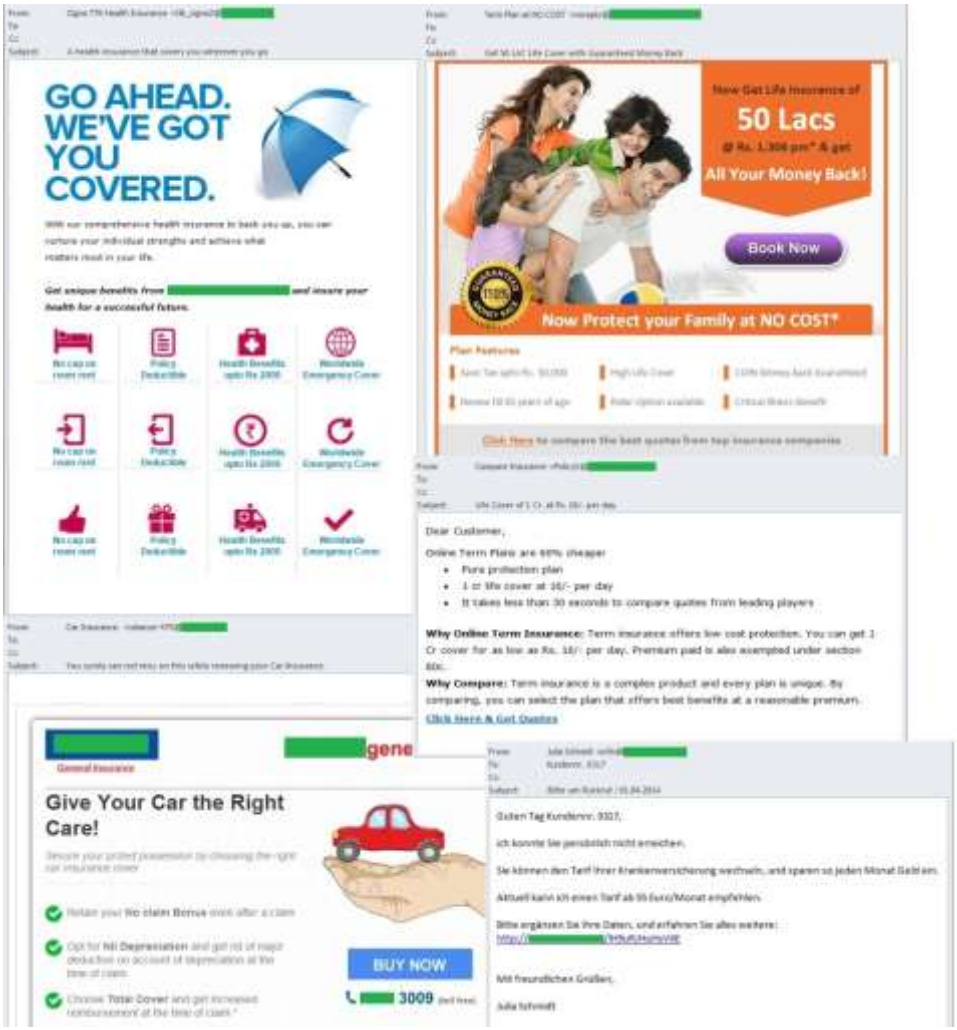


Nel traffico e-mail di maggio 2014 abbiamo ugualmente incontrato numerose proposte riguardanti l'opportunità di estinguere il debito accumulato a seguito del prestito precedentemente ottenuto per poter realizzare il ciclo di studi desiderato; i potenziali destinatari di tali proposte, secondo le intenzioni degli spammer, avrebbero dovuto ovviamente essere tutti coloro i quali, pur avendo terminato ormai da tempo gli studi superiori, non hanno di fatto ancora avuto la possibilità di restituire la somma di denaro conseguita in precedenza sotto forma di prestito. In sostanza, attraverso tali messaggi si proponeva ai destinatari delle e-mail di consultare il sito web raggiungibile mediante il link appositamente predisposto nel corpo del messaggio, sito in cui il potenziale interessato avrebbe trovato ad attenderlo la pubblicità di varie organizzazioni impegnate nella selezione di volontari e collaboratori da reclutare all'interno di istituzioni non profit di vario genere. In tal modo, compilando il modulo presente sulla pagina web in questione, l'utente avrebbe potuto verificare in prima persona le opportunità e le opzioni esistenti per poter restituire entro un ragionevole lasso di tempo la somma di denaro precedentemente ricevuta in prestito. Tale singolare tipologia di messaggi di spam è stata di fatto predisposta ed elaborata per essere poi specificamente indirizzata ai cittadini statunitensi, visto che proprio negli USA sono stati espressamente allestiti speciali programmi governativi grazie ai quali si può sfruttare l'opportunità di veder progressivamente ridotti i debiti in precedenza contratti, semplicemente occupandosi di attività utili per il paese. Desideriamo tuttavia sottolineare, nella circostanza, come i messaggi di spam qui analizzati non siano stati distribuiti in Rete da organizzazioni di tipo statale, bensì da entità estranee, non pertinenti, i cui indirizzi di posta elettronica sono peraltro risultati variare di continuo. Oltre a ciò, è stato da noi osservato come i link contenuti nelle e-mail in causa conducessero, di fatto, su siti web di recente creazione, all'interno dei quali l'utente avrebbe dovuto poi lasciare i propri dati personali.

Per coinvolgere ed interessare ancor di più i destinatari di tali messaggi, gli spammer hanno infine fatto ricorso ad una forma di comunicazione alquanto diretta ed immediata, del tipo: «Non avete ancora potuto rimborsare il prestito ottenuto da studente? Ho trovato per Voi un programma davvero formidabile, che merita assolutamente di essere visionato. Vi aiuterà di sicuro a ridurre notevolmente l'importo dei pagamenti mensili da effettuare».

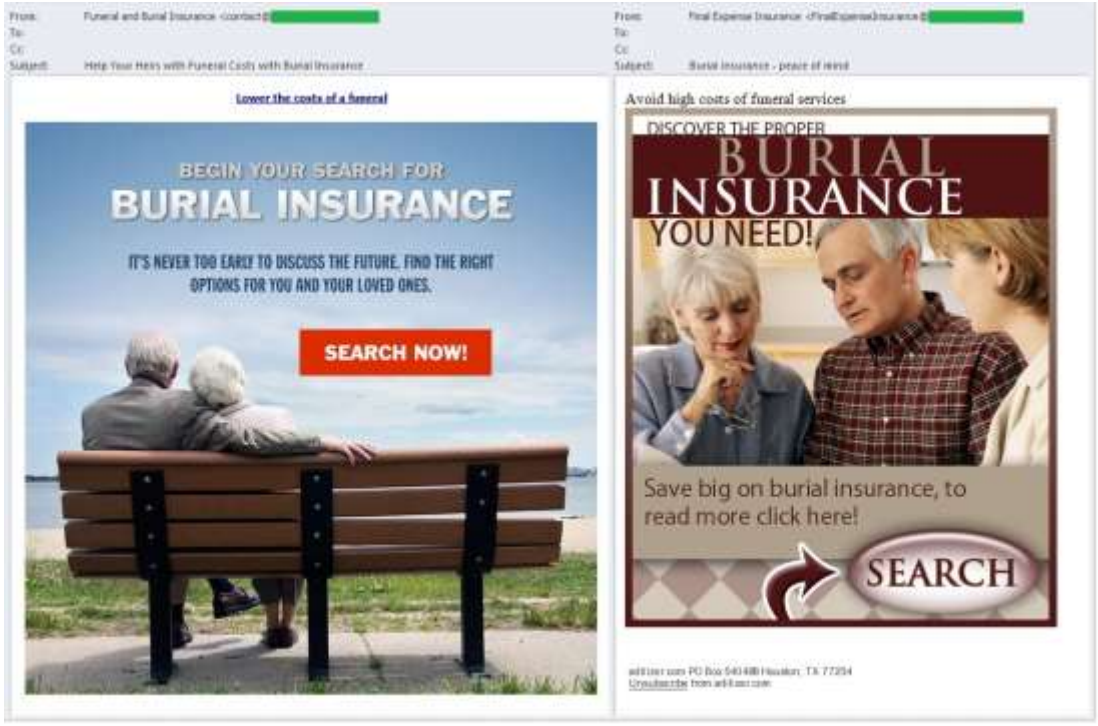
Polizze assicurative per ogni genere di rischio

Nel periodo oggetto della nostra consueta analisi mensile sul fenomeno spam, le polizze assicurative a copertura dei più svariati rischi hanno rappresentato un ulteriore tema ampiamente sfruttato all'interno dei flussi mondiali di posta indesiderata; in particolar modo, gli spammer hanno distribuito nelle e-mail box dei potenziali clienti proposte relative alla stipula di assicurazioni sulla vita, a copertura di eventuali infortuni e incidenti. Non sono ad ogni caso mancate numerose offerte commerciali riguardanti la sottoscrizione di polizze per autovetture.

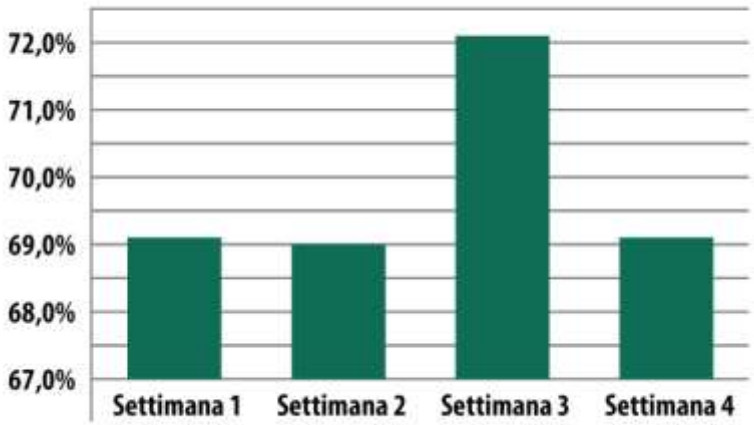


Fondamentalmente, lo scopo di tali campagne di spam si è rivelato essere quello di redirigere i destinatari delle e-mail verso un sito web grazie al quale sarebbe poi risultato possibile comparare i costi delle diverse coperture assicurative proposte sul mercato dalle varie compagnie, al fine di poter scegliere le condizioni più favorevoli. In altri casi, tuttavia, i link presenti sui messaggi di posta in questione indirizzavano verso siti web (spesso monopagina) appositamente allestiti dagli spammer, attraverso i quali si proponeva al visitatore una scelta ancor più ampia di possibili tipologie di polizze, di programmi e di compagnie assicurative. Una volta effettuata la scelta, dopo aver cliccato su uno dei link proposti all'interno della pagina web visitata, l'utente sarebbe giunto su un'ulteriore risorsa Internet. Allo stesso modo, i collegamenti ipertestuali inseriti dagli spammer nelle e-mail sopra descritte, conducevano talvolta verso un sito web preposto a pubblicizzare le offerte di una singola compagnia di assicurazione, in genere di dimensioni piuttosto contenute, creata quasi sempre di recente.

Una tipologia assicurativa di sicuro alquanto singolare ed inconsueta, proposta esclusivamente all'interno del segmento anglofono di Internet, è rappresentata da quelle particolari assicurazioni stipulate allo scopo di garantire la copertura delle spese inerenti ai servizi funebri, nel caso di un improvviso trapasso della persona assicurata. Si tratta, in pratica, di una sorta di vera e propria versione estesa ed integrata dell'ordinaria forma di assicurazione sulla vita: nella circostanza, i maggiori costi assicurativi prevedono l'inclusione, nella polizza, delle spese relative ai servizi funebri da svolgere in caso di morte improvvisa dell'assicurato. Nel mese di maggio, i messaggi di spam di tal genere hanno presentato un'accurata veste grafica, con estese immagini provviste di apposito link, volto ad indirizzare i destinatari delle e-mail verso i consueti siti allestiti dagli spammer, dedicati, nella fattispecie, alle tematiche assicurative, spesso formati da un'unica pagina web. I collegamenti ipertestuali in questione variavano, in genere, da un messaggio di spam all'altro; i relativi indirizzi Internet sono poi risultati a loro volta collocati in domini diversi, di solito registrati dagli spammer appena poco prima della data di inizio del mailing di massa.



Quota di spam nel traffico di posta elettronica

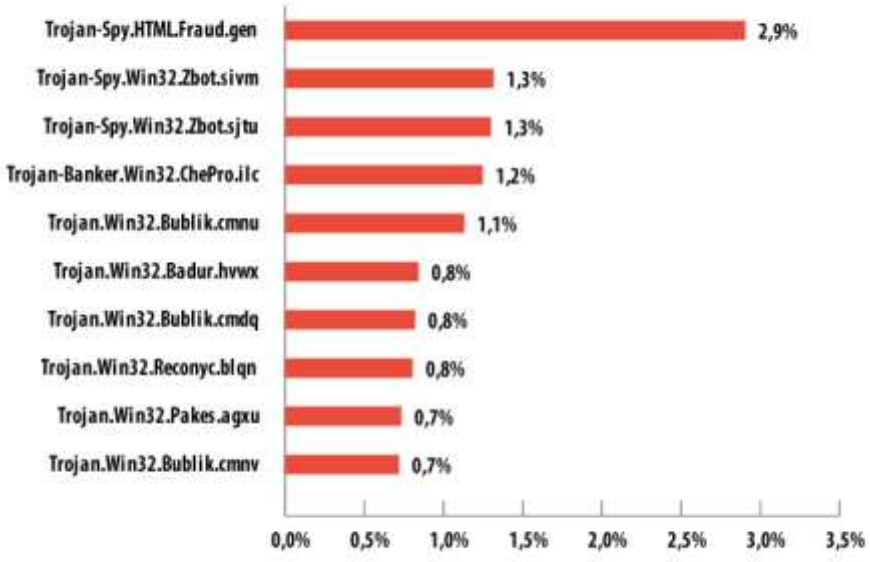


Quote di spam rilevate settimanalmente all'interno del traffico di posta elettronica

Nel mese oggetto del presente report, la quota inerente ai messaggi "spazzatura" rilevati nel traffico globale di posta elettronica ha fatto registrare un decremento dell' 1,3% rispetto all'analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 69,8% del volume complessivo di messaggi e-mail circolanti in Rete. L'indice percentuale più elevato è stato osservato nella terza settimana di maggio (72,1%); la quota di spam più contenuta è stata invece rilevata, all'interno dei flussi e-mail mondiali, nella seconda settimana del mese qui analizzato (69%).

Allegati dannosi rilevati nel traffico e-mail

La TOP-10 del mese di maggio 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 nocivi maggiormente diffusi
nel traffico di posta elettronica nel mese di maggio 2014

TOP-10 dei programmi malware maggiormente diffusi nel traffico e-mail

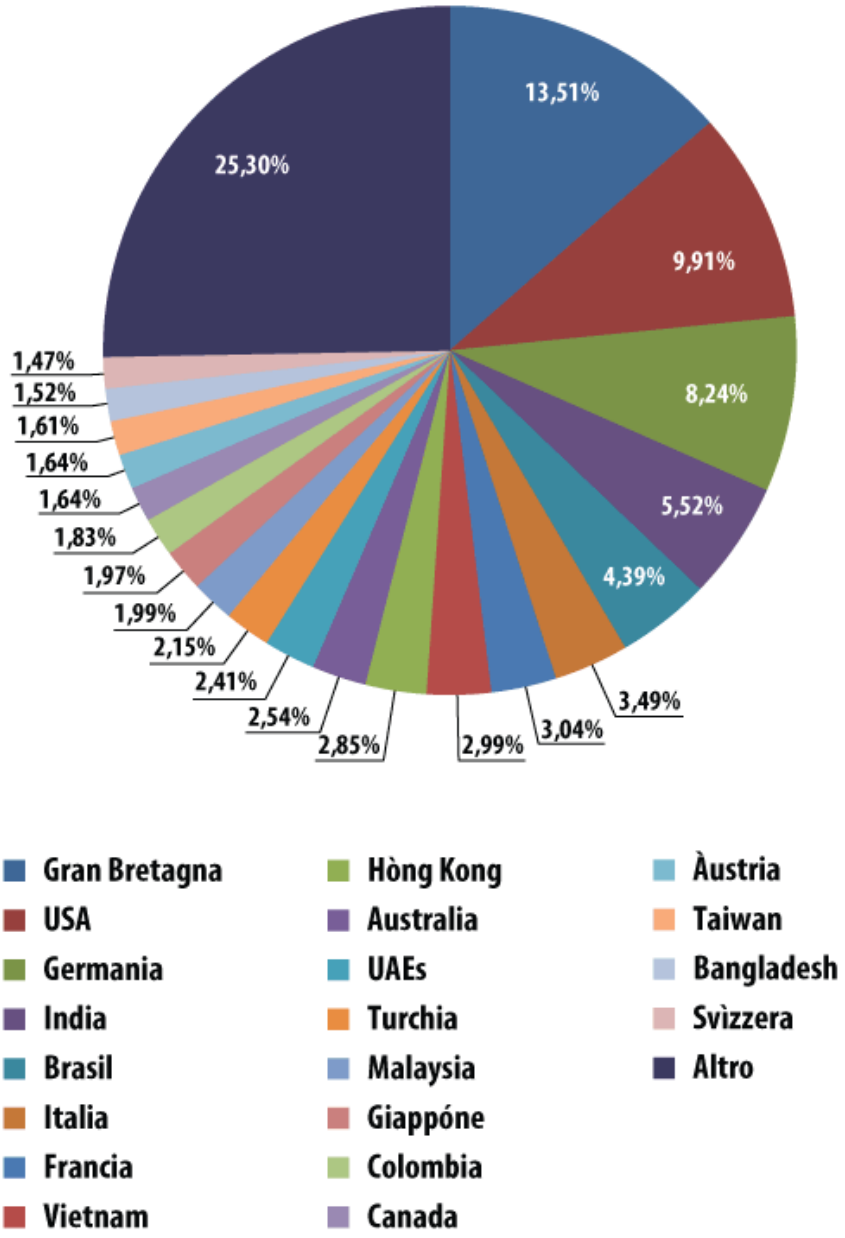
La speciale graduatoria relativa ai software nocivi maggiormente presenti nel traffico e-mail globale risulta nuovamente capeggiata dai Trojan riconducibili alla famiglia di malware denominata Trojan-Spy.HTML.Fraud.gen. Ricordiamo, nella circostanza, come tali software dannosi siano stati elaborati dai loro autori sotto forma di pagine 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; i Trojan-Spy in questione sono stati appositamente creati 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.

Continuando ad esaminare la composizione della TOP-10 di maggio 2014, salta immediatamente agli occhi la presenza di un cospicuo numero di programmi nocivi appartenenti alla famiglia di malware denominata Bublik, i quali sono andati a collocarsi, rispettivamente, al 2°, 3°, 5°, 7° e 10° posto del rating da noi elaborato. Rispetto all'analoga classifica del mese precedente, tuttavia, la presenza dei software dannosi riconducibili alla famiglia Bublik risulta sensibilmente diminuita; la TOP-10 relativa allo scorso mese di aprile annoverava, in effetti, ben 8 programmi malware (una sorta di monopolio!) appartenenti alla famigerata famiglia in questione. Come è noto, le principali funzionalità di cui sono provvisti tali programmi dannosi consistono nel download e nella successiva installazione sul computer-vittima di nuove versioni di ulteriori software nocivi, a totale insaputa dell'utente. Una volta portato a termine il proprio compito, i programmi malware ascrivibili alla famiglia Bublik non rimangono allo stato attivo, anche se provvedono a realizzare una copia di se stessi all'interno della cartella <%temp%>. Riteniamo di particolare utilità sottolineare come i trojan Bublik siano soliti camuffarsi sotto forma di applicazioni o documenti Adobe. Nello specifico, le varianti classificate dagli esperti di sicurezza IT con la denominazione di Trojan.Win32.Bublik.cpik e Trojan.Win32.Bublik.cpil (collocatesi, rispettivamente, sul secondo e sul terzo gradino del "podio virtuale" di maggio 2014) 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). Sebbene i trojan ZeuS/Zbot siano in grado di eseguire attività dannose di vario genere, nella maggior parte dei casi essi vengono utilizzati dai cybercriminali 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 a tale temibile famiglia 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.

La quarta posizione del rating da noi stilato è andata ad appannaggio del software nocivo rilevato dalle soluzioni anti-malware di Kaspersky Lab come Trojan-Banker.Win32.ChePro.ilc; si tratta, nella fattispecie, di un Trojan bancario appositamente sviluppato dai virus writer per colpire gli utenti di alcune banche brasiliane di primaria importanza. Come si può facilmente presupporre, al pari di numerosi altri malware riconducibili a tale specifica tipologia, il Trojan in causa risulta preposto al furto delle password e delle informazioni sensibili legate alla sfera del banking online.

Concludiamo la nostra breve rassegna - riguardo ai software dannosi rilevati con maggior frequenza all'interno del traffico di posta elettronica nel corso del mese di maggio 2014 - osservando come la nona posizione della speciale classifica qui esaminata sia andata ad appannaggio del malware denominato Trojan.Win32.Pakes.agxu. Si tratta, più precisamente, di un programma nocivo che evidenzia palesi funzioni di spyware, appositamente dispiegato dai cybercriminali sia per tenere traccia delle sequenze dei tasti via via premuti dall'utente, sia per realizzare continui screenshot delle schermate visualizzate, sul momento, dalla potenziale vittima; le informazioni e i dati illecitamente carpiti vengono poi trasmessi all'indirizzo di posta elettronica del malintenzionato di turno.



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

Suddivisione per paesi dei rilevamenti effettuati dall'antivirus e-mail

Al primo posto della classifica qui sopra riportata - riguardante i paesi nei quali, durante il mese di maggio 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 andata a collocarsi la Gran Bretagna (13,5%); nel periodo oggetto del presente report, l'indice percentuale ascrivibile al Regno Unito ha in effetti presentato un significativo incremento (+ 3,5%) rispetto all'analogo valore rilevato nel mese precedente. Gli Stati Uniti,

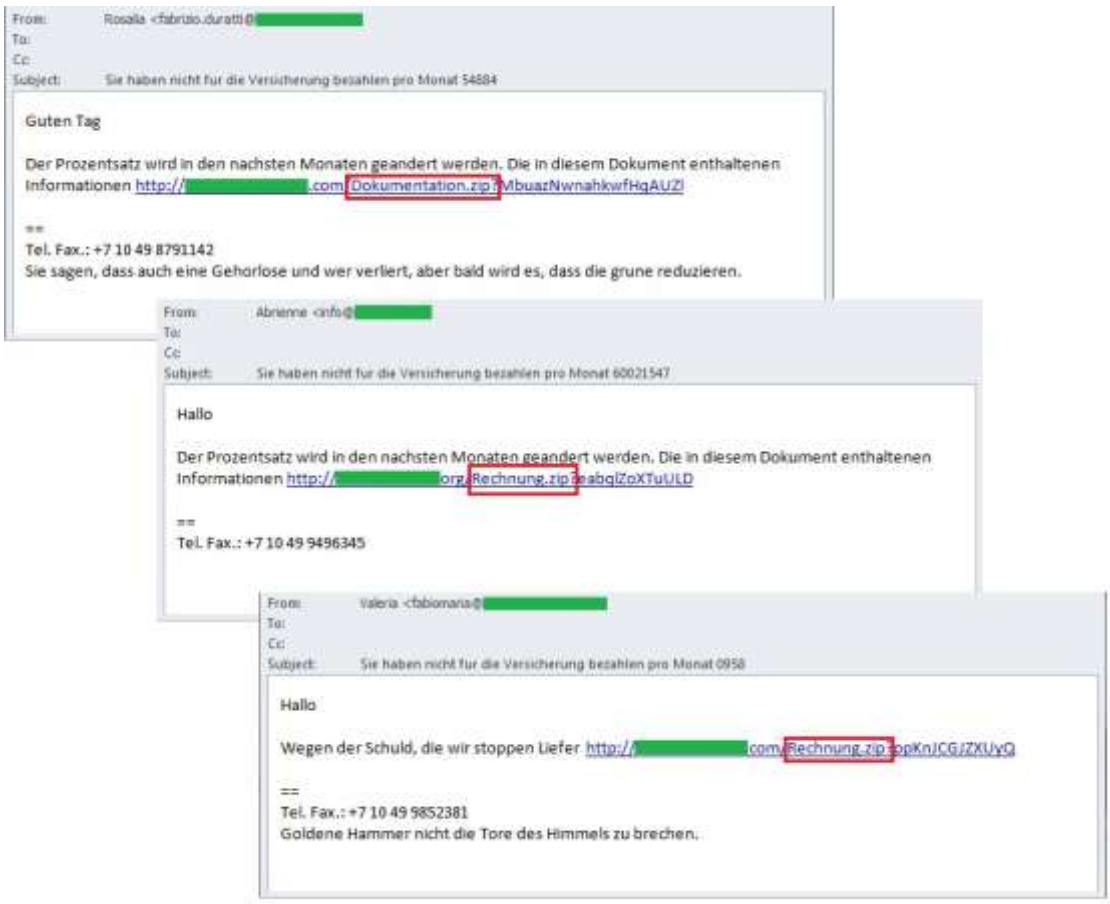
paese leader del rating relativo allo scorso mese di aprile, hanno in tal modo "perso" una posizione in classifica, andando ad occupare, di fatto, il secondo gradino del "podio" virtuale di maggio 2014. Gli USA hanno fatto registrare una quota media pari al 9,9% (- 1,8% rispetto ad un mese fa) del volume complessivo dei rilevamenti eseguiti grazie al modulo antivirus e-mail. La Germania, da parte sua, ha conservato la terza piazza della speciale graduatoria, evidenziando, nel mese oggetto della nostra analisi, un indice quantificabile in 8,2 punti percentuali.

Segnaliamo, inoltre, l'ingresso in classifica della Colombia (1,83%); il paese latino-americano è quindi entrato a far parte, in veste di assoluta "new entry", della speciale TOP-20 qui sopra riportata, stilata dagli esperti di Kaspersky Lab. La Russia, per contro, non compare più nelle prime venti posizioni del ranking relativo ai paesi che presentano gli indici percentuali più elevati riguardo ai rilevamenti effettuati dal nostro modulo antivirus operante a livello di flussi e-mail globali.

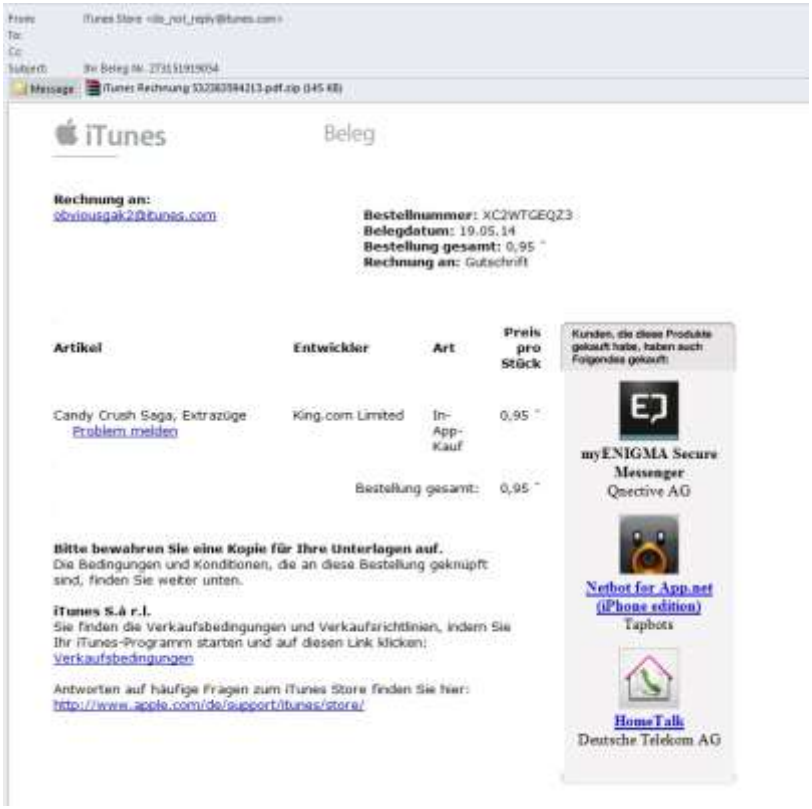
Osserviamo, infine, come le quote relative ai rimanenti paesi presenti nella graduatoria di maggio non abbiano subito significative variazioni percentuali rispetto a quanto riscontrato nel mese di aprile 2014.

Peculiarità e tratti caratteristici dello spam nocivo di maggio

Come abbiamo visto nella prima sezione del nostro report mensile dedicato al fenomeno spam, le tematiche connesse al settore delle assicurazioni hanno ampiamente caratterizzato i flussi di posta elettronica indesiderata di maggio 2014; nel mese qui analizzato, tale specifico tema è stato ugualmente oggetto di numerose campagne di spam nocivo, volte a recapitare pericolosi allegati nocivi nelle e-mail box degli utenti della Rete. All'interno del traffico di posta elettronica di maggio sono stati ad esempio da noi individuati vari messaggi e-mail, elaborati in lingua tedesca, recanti esplicitamente, nel campo riservato all'oggetto, una frase alquanto minacciosa: «Lei non ha ancora provveduto a pagare la quota assicurativa mensile, per un importo di ...»; ai destinatari di tali e-mail veniva poi notificato che, nel mese successivo, sarebbe stato inoltre variato l'importo relativo al premio previsto dalla polizza assicurativa precedentemente sottoscritta. I messaggi di posta in questione contenevano inoltre, al loro interno, un link apparentemente preposto all'ottenimento di informazioni più dettagliate riguardo al tema specifico proposto dall'e-mail; di fatto, cliccando su tale collegamento ipertestuale, il potenziale utente-vittima avrebbe involontariamente generato il download, sul proprio computer, di un file archivio ZIP, esplicitamente denominato, da parte dei malintenzionati, «Dokumentation» (documentazione) o, in alternativa, «Rechnung» (fattura). In realtà, sia nel primo caso che nell'altro, è risultato che il file compresso in questione celava un temibile programma dannoso, rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Backdoor.Win32.Androm.dsqy. I software dannosi riconducibili alla famiglia di malware denominata Andromeda sono, in sostanza, programmi Backdoor che consentono ai cybercriminali di assumere il pieno controllo del computer sottoposto a contagio informatico, all'insaputa dell'utente-vittima. Inoltre, i computer infettati da programmi nocivi di tal genere entrano spesso a far parte di estese botnet, risultando poi completamente asserviti alle reti-zombie di volta in volta allestite dai malintenzionati.



Allo stesso modo, lungo tutto l'arco del mese di maggio 2014, i cybercriminali si sono dedicati alla distribuzione, nelle caselle di posta elettronica degli utenti del web, di messaggi e-mail mascherati sotto forma di notifiche provenienti (in apparenza!) da iTunes Store, il noto negozio on-line adibito alla vendita di prodotti digitali di vario genere (musica, video musicali, film, applicazioni, etc.). Nella circostanza, si comunicava ai destinatari delle e-mail nocive l'avvenuto acquisto di una determinata applicazione; a tal proposito, nel tentativo di conferire maggiore credibilità ed attendibilità all'e-mail nociva, veniva riportata, nel corpo del messaggio, l'esatta denominazione del software "acquistato" dall'utente, così il come il prezzo (unitario e complessivo) relativo all'applicazione in causa. In realtà, il file archivio allegato al messaggio di posta elettronica qui sopra descritto, anzichè contenere la fattura inerente all'acquisto effettuato, recava un temibile programma Trojan, e più precisamente il malware classificato come Trojan-Banker.Win32.Shiotob.f. I Trojan riconducibili a tale famiglia risultano essere specializzati nel sottrarre le password utilizzate nell'ambito dei client FTP; allo stesso modo, i suddetti software nocivi sono in grado di spiare ed intercettare il traffico Internet generato dai browser, con il preciso scopo di carpire i dati sensibili necessari per accedere a determinati siti web.



iTunes

Beleg

Rechnung an:
obviousgak2@itunes.com

Bestellnummer: XC2WTGEQZ3
Belegdatum: 19.05.14
Bestellung gesamt: 0,95 €
Rechnung an: Gutschrift

Artikel	Entwickler	Art	Preis pro Stück
Candy Crush Saga, Extrazüge Problem melden	King.com Limited	In-App-Kauf	0,95 €
		Bestellung gesamt:	0,95 €

Bitte bewahren Sie eine Kopie für Ihre Unterlagen auf.
Die Bedingungen und Konditionen, die an diese Bestellung geknüpft sind, finden Sie weiter unten.

iTunes S.à r.l.
Sie finden die Verkaufsbedingungen und Verkaufsrichtlinien, indem Sie Ihr iTunes-Programm starten und auf diesen Link klicken:
Verkaufsbedingungen

Antworten auf häufige Fragen zum iTunes Store finden Sie hier:
http://www.apple.com/de/support/itunes/store/

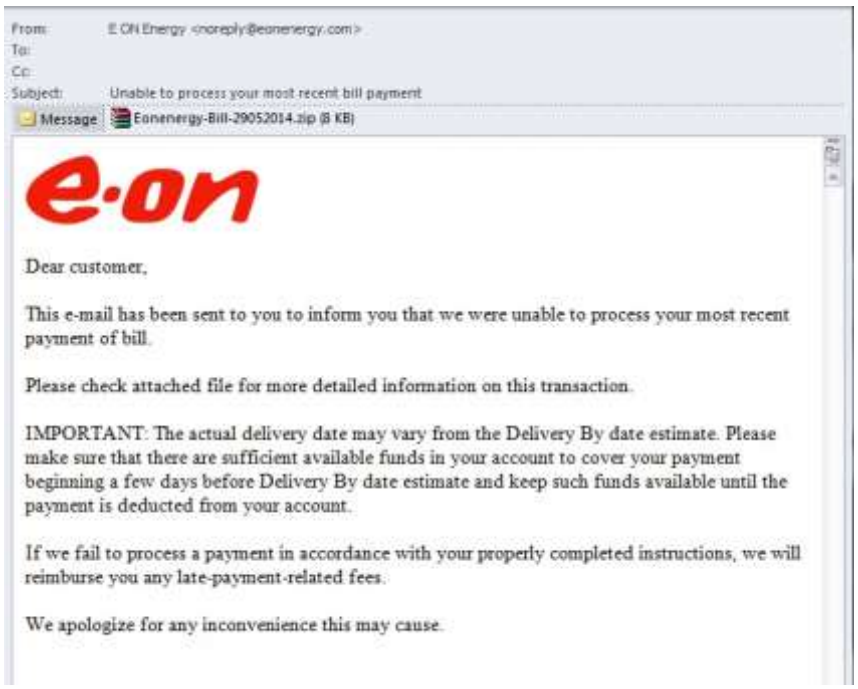
Kunden, die diese Produkte gekauft habe, haben auch Folgendes gekauft:

myENIGMA Secure Messenger
Qsective AG

Netbot for App.net (iPhone edition)
Tapbots

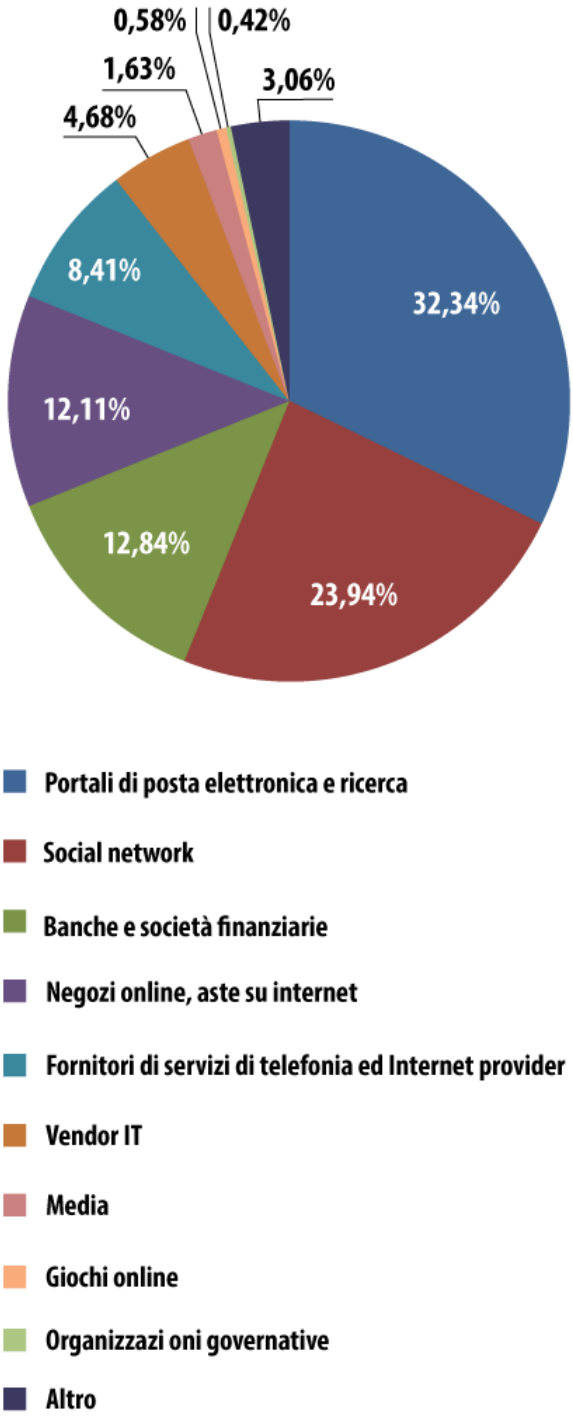
HomeTalk
Deutsche Telekom AG

Nel corso del mese di maggio 2014, un'ulteriore campagna di spam nocivo ha visto prendere di mira i clienti di E.ON, primaria società operante nel settore energetico, relativamente alla produzione ed alla fornitura di energia elettrica e di gas in numerosi paesi del globo, incluso la Federazione Russa. Nella fattispecie, i malintenzionati hanno provveduto a diffondere nelle e-mail box dei potenziali utenti-vittima, avvalendosi in maniera indebita del nominativo di tale importante gruppo energetico - riproducendo peraltro in maniera perfetta il logo ufficiale di quest'ultimo - un cospicuo numero di messaggi di posta elettronica contenenti il seguente testo: «Gentile Cliente, La informiamo, tramite la presente e-mail, che non siamo stati purtroppo in grado di elaborare l'ultimo pagamento da Lei effettuato. Informazioni dettagliate a tal riguardo sono contenute nel file allegato al messaggio». E' stato rilevato, nella circostanza specifica, che il file archivio allegato alle e-mail dannose qui sopra descritte custodiva, in realtà, il pericoloso software Trojan-Spy.Win32.Zbot.svvs, un ulteriore temibile rappresentante della famigerata famiglia di malware denominata Zbot, preposto al furto dei dati personali degli utenti, ed in primo luogo delle informazioni sensibili relative alla sfera bancaria di questi ultimi.



Phishing

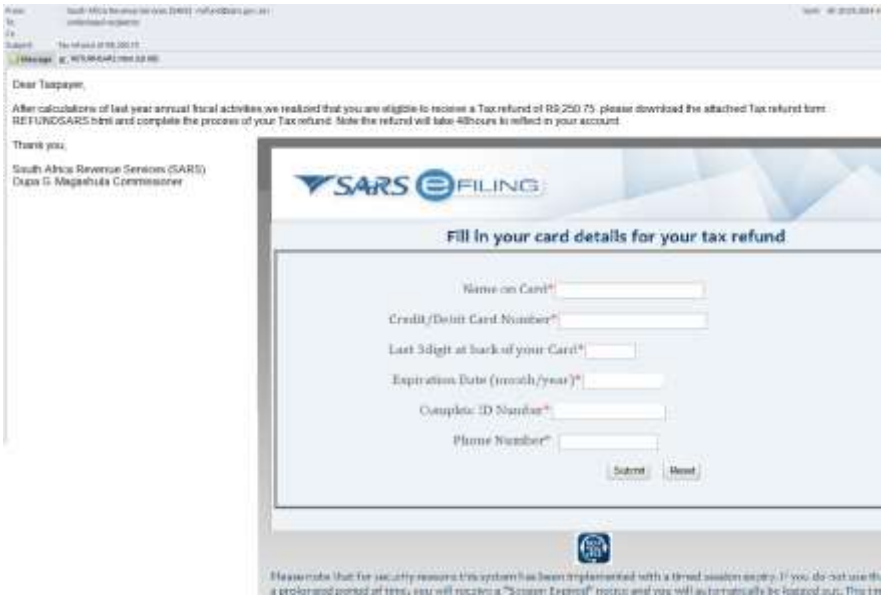
Così come nello scorso mese di aprile, al primo posto della speciale graduatoria relativa alle organizzazioni (suddivise per categorie) rimaste vittima con maggior frequenza degli assalti portati dai phisher, troviamo la nuova categoria da noi recentemente definita, denominata «Portali di posta elettronica e ricerca», con una quota pari al 32,3%; rileviamo, nella circostanza, come l'indice percentuale ascrivibile agli attacchi di phishing complessivamente condotti nei confronti di tali risorse web abbia fatto registrare un lieve incremento rispetto ad un mese fa, quantificabile in 0,5 punti percentuali. Come evidenzia il grafico qui sotto riportato, la seconda piazza del ranking di maggio 2014 risulta occupata dal raggruppamento che riunisce i social network - guidati da Facebook - con una quota pari al 23,9%. L'indice relativo alla categoria "Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari" (12,8%) ha evidenziato un aumento di 0,2 punti percentuali rispetto all'analogo rating del mese precedente. Alla quarta piazza della speciale TOP-100 di maggio dedicata al fenomeno phishing si conferma poi la categoria denominata "Negozi Internet ed aste online"; la quota riconducibile agli attacchi orditi dai phisher nei confronti dei negozi online ha ugualmente presentato un leggero incremento rispetto allo scorso mese di aprile, attestandosi così su un valore medio pari al 12,1%. Terminiamo la nostra breve rassegna dedicata alla classifica del phishing di maggio 2014, osservando come, rispetto a quanto riscontrato un mese fa, l'indice percentuale relativo alle risorse web, organizzazioni e società raggruppate nella categoria "Fornitori di servizi di telefonia ed Internet provider" abbia invece fatto registrare una lieve diminuzione, pari allo 0,4%.



TOP-100 relativa alle organizzazioni maggiormente sottoposte agli attacchi di phishing nel mese di maggio 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.

Spesso, come è noto, i messaggi e-mail contraffatti "dedicati" alle tematiche inerenti al pagamento di tasse ed imposte varie, vengono distribuiti dai malintenzionati nelle caselle di posta elettronica degli utenti del web allo scopo di generare l'installazione, sui computer di questi ultimi, dei più disparati e temibili programmi malware. Nel corso del mese oggetto del presente report, all'interno delle speciali "trappole" antispam da noi allestite, sono stati ad esempio individuati numerosi messaggi di posta mascherati sotto forma di notifiche ufficiali apparentemente inviate dal servizio di gestione e riscossione delle imposte della Repubblica Sudafricana (South African Revenue Service - SARS, in pratica l'equivalente dell'Agenzia delle Entrate in Italia); l'elemento di novità è tuttavia rappresentato dal fatto che tali e-mail non recavano in allegato il consueto file nocivo, bensì un'insidiosa pagina HTML di phishing. Nella circostanza, i malintenzionati di turno cercavano di convincere il destinatario del messaggio di posta fasullo ad introdurre nei campi del modulo di phishing appositamente predisposto i dati relativi alla propria carta di credito; in tal modo, secondo quanto asserito dal mittente dell'e-mail, il "contribuente" avrebbe potuto ricevere, in qualità di rimborso su tasse precedentemente pagate in eccesso, una determinata somma di denaro. Per conferire al modulo di phishing un aspetto di legittimità, i truffatori avevano inserito nella pagina HTML contraffatta il logo dell'agenzia statale in questione; all'interno del campo <From>, inoltre, i phisher avevano specificato non solo la denominazione completa del servizio di gestione tasse ed imposte allestito dal governo sudafricano, ma avevano ugualmente introdotto il nome di dominio ufficiale <sars.gov.za> a livello di indirizzo di posta elettronica del mittente.



Conclusioni

Nel mese di maggio 2014 la quota dello spam presente nel traffico di posta elettronica mondiale ha fatto registrare un decremento dell' 1,3%, attestandosi in tal modo su un valore medio pari al 69,8% del volume complessivo di messaggi e-mail circolanti in Rete.

Gli spammer hanno ampiamente sfruttato il rapido approssimarsi della stagione estiva e la conseguente fine dell'anno scolastico per organizzare la conduzione di numerosi mailing di massa riconducibili al cosiddetto spam "turistico", volto a reclamizzare, nella specifica circostanza, le più svariate offerte di vacanze e soggiorni estivi appositamente dedicati a bambini e ragazzi. Campagne di spam similari sono state ugualmente allestite per pubblicizzare particolari servizi di insegnamento ed attività scolastico-studentesche da condurre a distanza; non sono infine mancate le più disparate, singolari e spesso poco

trasparenti proposte relative all'acquisto di diplomi "preconfezionati" di ogni genere, rilasciati da certi istituti di insegnamento superiore od universitario, di specifico interesse del potenziale cliente. Desideriamo sottolineare, con l'occasione, come sia del tutto lecito attendersi, anche per questa estate, il consueto sensibile incremento - che si ripete puntualmente ogni anno, di questi tempi - del numero dei messaggi di spam riconducibili alla sfera del turismo, proprio in concomitanza con l'inizio delle ferie e delle vacanze estive.

Nel segmento anglofono dello spam ispirato, come d'abitudine, alle principali tematiche suggerite dalle festività stagionali, è stata attivamente sfruttata, da parte degli spammer di ogni angolo del globo, la sentita ricorrenza della Festa della Mamma, al fine di pubblicizzare regali di vario genere. Le polizze assicurative a copertura dei più svariati rischi hanno poi rappresentato un ulteriore tema di cui, lungo tutto l'arco del mese di maggio, si sono ampiamente avvalsi gli spammer per la conduzione delle proprie attività in Rete. Nel segmento russo di Internet la maggior parte dei messaggi di spam dedicati a tale specifica tematica ha convogliato verso le e-mail box degli utenti soprattutto proposte relative alla stipula di polizze per autovetture, mentre il segmento della Rete frequentato dagli utenti di lingua inglese ha visto prevalere, nello specifico, le offerte relative alle assicurazioni sulla vita.

Nel periodo oggetto della nostra consueta analisi mensile dedicata al fenomeno spam, la leadership della speciale TOP-10 relativa ai software nocivi maggiormente presenti nei flussi di posta elettronica mondiali è andata nuovamente ad appannaggio del programma Trojan classificato dagli esperti di sicurezza IT con la denominazione di Trojan-Spy.HTML.Fraud.gen. Rispetto al mese precedente, è risultato sensibilmente diminuito, all'interno del rating del malware da noi stilato, il numero dei software nocivi riconducibili alla famiglia Bublik; la TOP-10 relativa allo scorso mese di aprile annoverava, in effetti, ben 8 programmi dannosi appartenenti alla famigerata famiglia in questione, mentre nel mese di maggio 2014, la presenza di questi ultimi all'interno della speciale graduatoria si è ridotta a "sole" cinque unità.

In maggio, come abbiamo visto in precedenza, la classifica relativa alle organizzazioni (suddivise in apposite categorie) rimaste vittima con maggior frequenza degli assalti portati dai phisher non ha subito sostanziali variazioni rispetto all’analogo rating del mese precedente. La TOP-100 di maggio 2014 dedicata all'analisi del fenomeno phishing è risultata nuovamente capeggiata dalla categoria denominata «Portali di posta elettronica e ricerca», con una quota pari al 32,3%. Così come nel mese precedente, la seconda posizione del rating è andata ad appannaggio dei social network (23,9%), mentre la categoria "Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari" si è collocata al terzo posto della speciale graduatoria elaborata dai nostri analisti di spam (12,8%).