Lo spam nel primo trimestre del 2014

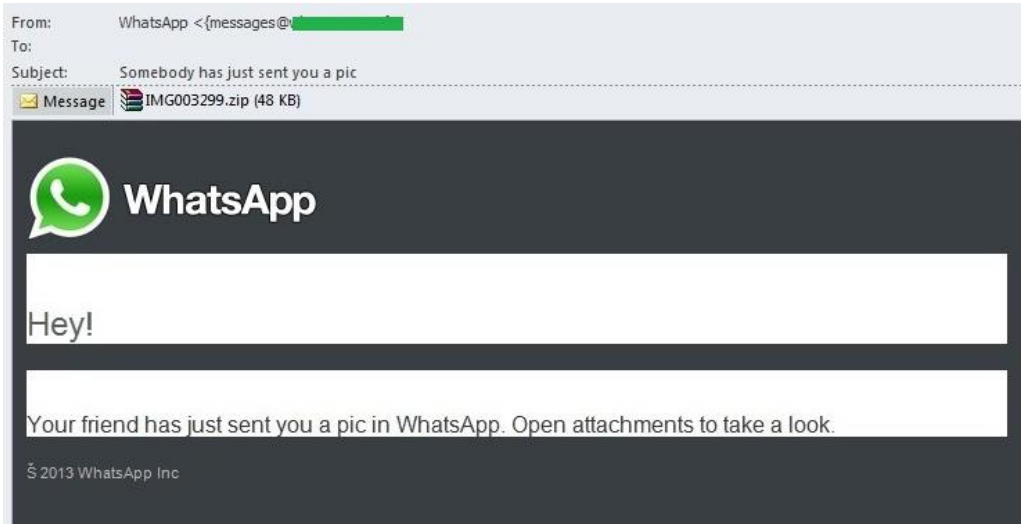
Sommario

Messaggi di spam camuffati sotto forma di notifiche inviate attraverso applicazioni mobile

Con la crescente ed ormai capillare diffusione dei dispositivi mobile, sta iniziando a comparire, all'interno del traffico di posta elettronica globale, lo spam specificamente indirizzato agli utenti di smartphone e tablet. Recentemente, avevamo già riferito in merito ad alcuni mailing di massa contenenti programmi maligni appositamente sviluppati dai virus writer per colpire il sistema operativo mobile Android. La presenza di tali software nocivi nel panorama mondiale dello spam risulta, per il momento, piuttosto contenuta, anche se gli spammer effettuano già la distribuzione di malware mobile con notevole regolarità. Nel corso del trimestre oggetto del presente report è stata da noi osservata un'ulteriore specifica tendenza, ovvero la presenza, all'interno dei flussi di posta, di un considerevole numero di e-mail di spam mascherate sotto forma di notifiche e comunicazioni provenienti (in apparenza) da alcune delle più celebri applicazioni per dispositivi mobile. Nella maggior parte dei casi, nell'ambito di tali mailing di massa, gli spammer hanno sfruttato l'elevato livello di popolarità ormai raggiunto su scala mondiale da WhatsApp, la famosa applicazione di messaggistica mobile multi-piattaforma: le e-mail contraffatte, camuffate da notifiche e messaggi inviati attraverso WhatsApp, sono state utilizzate dagli spammer sia per distribuire temibili software nocivi nelle caselle di posta elettronica degli utenti, sia per reclamizzare prodotti e servizi di vario genere.

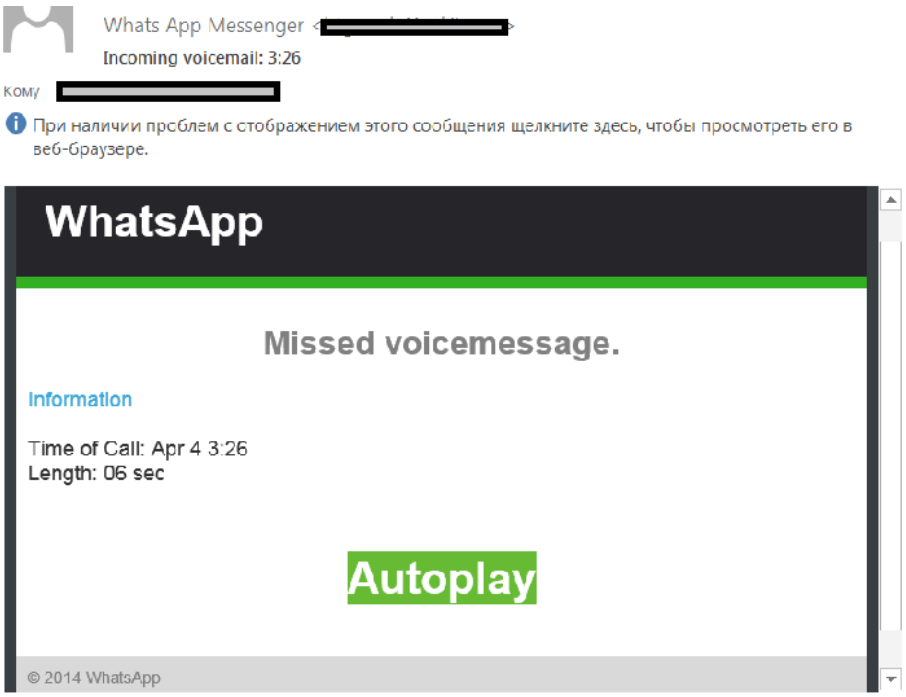
Nello scorso mese di gennaio, ad esempio, abbiamo individuato, nel traffico e-mail, una singolare campagna di spam messa a punto per recapitare messaggi in cui si comunicava che un non ben precisato mittente aveva provveduto ad inviare una foto al destinatario dell'e-mail, proprio attraverso l'applicazione mobile WhatsApp. Ovviamente, ogni utente esperto ed accorto si sarebbe subito chiesto il motivo per cui un messaggio del genere veniva insolitamente recapitato tramite posta elettronica, visto che gli account WhatsApp non sono in alcun modo direttamente collegati alle e-mail box degli utenti del noto servizio di messaggistica mobile. Bisogna però tener conto del fatto che sono davvero in molti sia

coloro che abitualmente sincronizzano i propri contatti, sia coloro che sono a conoscenza di come, attraverso la posta elettronica, possano comunque essere ricevuti messaggi provenienti da app mobile; sono queste le ragioni per cui, un messaggio del genere, tutto sommato, non era di per se stesso destinato ad allarmare in maniera particolare la maggior parte degli utenti che lo avrebbero ricevuto.



In realtà, l'archivio compresso allegato al messaggio di posta elettronica qui sopra raffigurato conteneva un pericoloso programma malware, rilevato dalle soluzioni antivirus di Kaspersky Lab come Backdoor.Win32.Androm.bjkd. Si tratta di un noto programma backdoor, la cui principale funzionalità consiste nel generare il download di ulteriori software nocivi sul computer-vittima sottoposto ad attacco.

Nel mese di marzo, poi, ci siamo imbattuti in un ulteriore mailing di massa, anch'essa volta a sfruttare l'ampia popolarità di cui gode l'applicazione mobile in questione. Attraverso tali messaggi si comunicava al destinatario l'esistenza di un messaggio vocale di WhatsApp non ancora ascoltato da parte di quest'ultimo; nella circostanza, per «porre rimedio» alla situazione, il potenziale utente-vittima avrebbe dovuto semplicemente cliccare sull'apposito link inserito nel corpo dell'e-mail.



Il pulsante «Autoplay», tuttavia, anziché far ascoltare il messaggio mancante, avrebbe condotto l'ignaro utente verso un sito legittimo compromesso, contenente il seguente codice Javascript:

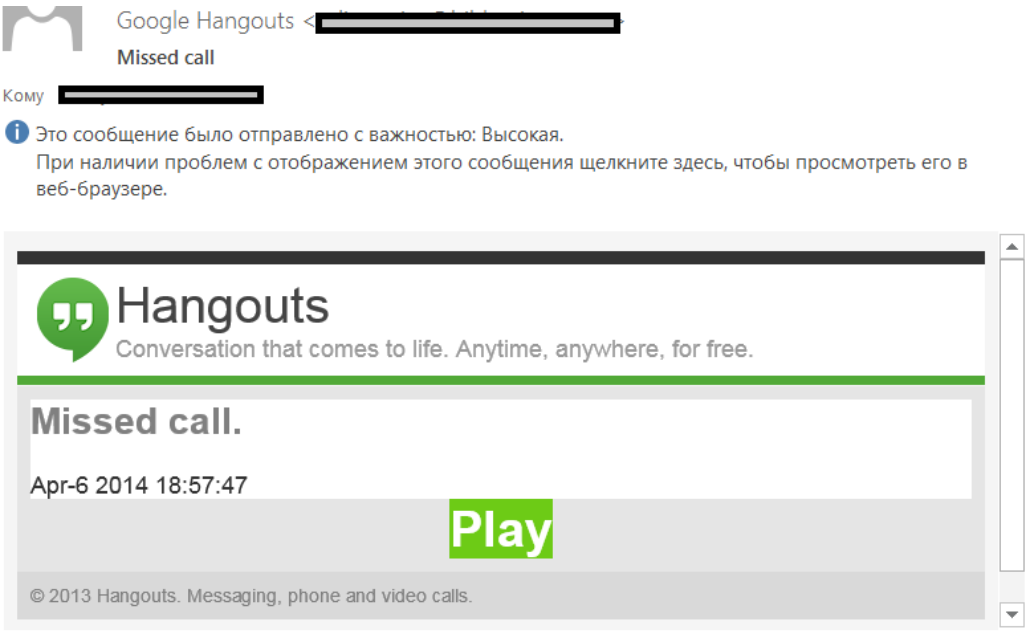
```
<html>
<body>
  <script type="text/javascript">
        rxat1 = "\x30";
        wazze2 =
        "\x68\x74\x74\x70\x3A\x2F\x2F\x74\x68\x65\x70\x69\x6C\x6
        C\x6D\x65\x64\x69\x63\x61\x6C\x2E\x63\x6F\x6D";
        setTimeout("\x77\x69\x6E\x64\x6F\x77\x2E\x74\x6F\x70\x2E\
        x6C\x6F\x63\x61\x74\x69\x6F\x6E\x2E\x68\x72\x65\x66\x3D\
        x77\x61\x7A\x7A\x65\x32\x3B", rxat1);
  </script>
</body>
</html>
```

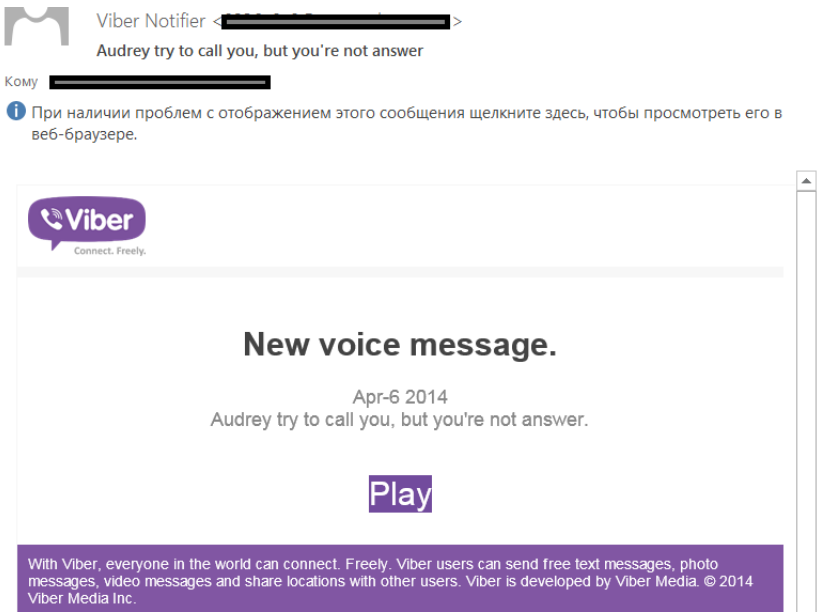
Se trasformiamo i caratteri esadecimali sopra rappresentati in caratteri letterali, otteniamo quanto segue:

```
<html>
<body>
  <script type="text/javascript">
    rxat1 = "0";
    wazze2 = "http://***pillmedical.com";
    setTimeout("window.top.location.href=wazze2", rxat1);
  </script>
</body>
</html>
```

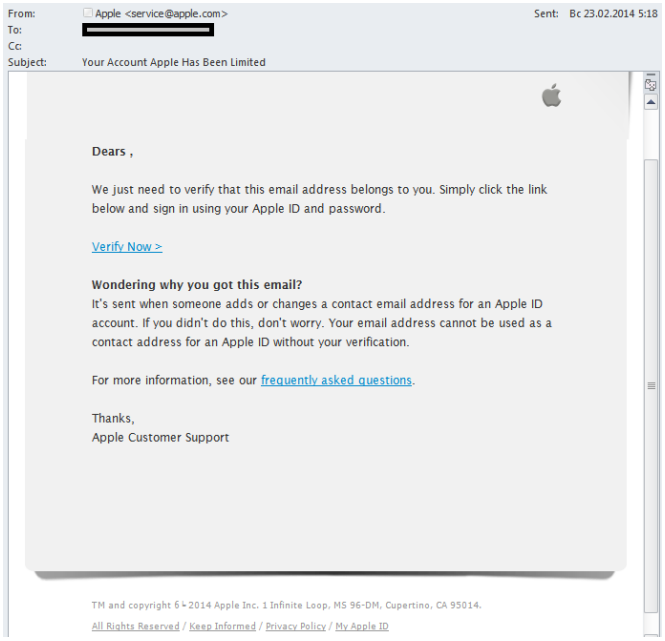
Nella fattispecie, il sito web violato agiva in funzione di redirector, indirizzando l'utente verso un altro sito Internet, appositamente allestito per pubblicizzare viagra e prodotti affini.

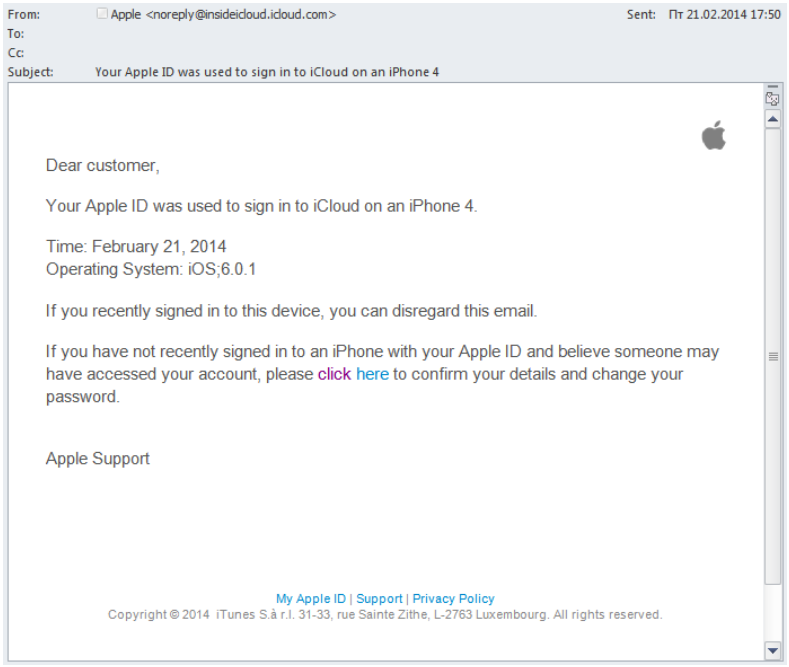
Nell'ambito di tale schema, gli spammer si avvalevano non soltanto dei messaggi contraffatti apparentemente provenienti dal client WhatsApp, ma anche di e-mail camuffate sotto forma di notifiche inviate attraverso altri popolari software di messaggistica mobile, quali Viber e Google Hangouts.





Nel quadro generale del sempre più crescente interesse nutrito dagli utenti nei confronti dei dispositivi mobile, spiccano ugualmente i frequenti attacchi di phishing che si prefiggono di realizzare il furto degli ID Apple:





Nel primo trimestre del 2014, la società Apple è andata di fatto ad occupare il 17° posto nell'ambito della speciale graduatoria riservata alle organizzazioni maggiormente sottoposte agli attacchi portati dai phisher.

I temi caldi dello spam: i Giochi Olimpici

Dal 7 al 23 febbraio 2014 si è svolta a Sochi, nella Federazione Russa, la XXII° edizione dei Giochi Olimpici Invernali. Un simile avvenimento internazionale, naturalmente, non poteva passare inosservato agli occhi degli spammer che in effetti, hanno approfittato della situazione per allestire varie mailing di massa, sebbene le azioni a cura degli spammer in occasione dell'evento olimpico non si siano rivelate di vastissima portata, come era invece lecito attendersi. Vari imprenditori cinesi, tramite i consueti messaggi di spam pubblicitario, hanno offerto prodotti di vario genere appositamente decorati con i simboli delle Olimpiadi di Sochi; i cosiddetti truffatori «nigeriani», da parte loro, hanno invece sfruttato le tematiche connesse alla manifestazione olimpica dello scorso febbraio per cercare di sottrarre

cospicue somme di denaro agli utenti della Rete. Allo stesso modo, all'interno dei flussi di spam che hanno caratterizzato il primo trimestre dell'anno 2014, è stata da noi individuata la conduzione di alcuni estese mailing di massa volte a reclamizzare repliche di "orologi per il viaggio alle Olimpiadi", oppure determinati servizi offerti da un elicottero privato nella città di Sochi.

Desideriamo con l'occasione sottolineare come non sia affatto la prima volta che rileviamo un livello di attività piuttosto contenuto, da parte degli spammer, nei confronti d tale eclatante avvenimento sportivo. Nell'estate del 2012, ad esempio, durante lo svolgimento dei Giochi Olimpici di Londra, sono state principalmente individuate, all'interno dei flussi e-mail globali, campagne di spam fraudolento dedicate ad improbabili vincite realizzate in fantomatiche lotterie «olimpiche». La precedente edizione dei Giochi Olimpici Invernali, svoltasi a Vancouver nel mese di febbraio del 2010, da parte sua, non aveva quasi per nulla attirato le losche attenzioni dei cybercriminali. E' tuttavia interessante rilevare come, in genere, durante i Campionati del Mondo di calcio, si osservi invece un numero sempre crescente di campagne di spam collegate alle tematiche suggerite da tale evento, di indubbia portata planetaria.

Nel corso del primo trimestre dell'anno, oltre al tema delle Olimpiadi invernali di Sochi 2014, gli spammer (ed in particolar modo i truffatori «nigeriani») hanno ugualmente fatto ricorso ad argomentazioni ispirate alle principali news internazionali del momento, quali, ad esempio, la notizia relativa alla morte di Ariel Sharon, l'ex primo ministro israeliano. I truffatori della Rete, inoltre, continuano imperterriti ad allestire un consistente numero di mailing di massa «nigeriani», volti a distribuire - nelle caselle di posta elettronica degli utenti - fiumi di messaggi di spam fraudolento mascherati sotto forma di e-mail provenienti (in apparenza) da familiari e collaboratori di Nelson Mandela, ex-presidente della Repubblica Sudafricana, deceduto nello scorso mese di dicembre.

Metodi e trucchi adottati dagli spammer: «inquinamento» del codice HTML

Come è noto, allo scopo di rendere in qualche modo «unico» ogni singolo messaggio di spam facente parte di un esteso mailing di massa, gli spammer ricorrono spesso ad una sorta di «imbrattamento» del testo, ovvero all'aggiunta, all'interno di quest'ultimo, di caratteri, parole o frammenti di testo del tutto casuali. Naturalmente, dopo il «trattamento» ricevuto, il messaggio in questione evidenzia un aspetto decisamente meno accurato del solito - per non dire che, a volte, ne viene addirittura compromessa la leggibilità - suscitando in tal modo, inevitabilmente, minor interesse ed attenzione da parte dei destinatari dell'e-mail. E' per tale motivo che gli spammer, in genere, cercano in ogni modo di nascondere, agli occhi dell'utente, il testo casuale da essi inserito. Metodi ormai piuttosto datati - quali l'immissione di testo di colore bianco su sfondo della medesima tonalità, oppure la semplice separazione del testo «spazzatura» dal contenuto principale dell'e-mail mediante l'inserimento di un elevato numero di interruzioni di riga - vengono tuttora ampiamente utilizzati da coloro che si dilettano a riempire le caselle di posta elettronica degli utenti di ogni genere di e-mail indesiderate, nonostante trucchi del genere siano in pratica «coetanei» della nascita dello stesso fenomeno spam.

Alcuni spammer, ad ogni caso, applicano metodi decisamente più sofisticati ed avanzati. Uno di essi consiste nell'«imbrattamento» dei messaggi di spam mediante l'aggiunta di specifici tag HTML. La caratteristica fondamentale di un simile trucco è rappresentata dal fatto che, in sostanza, il destinatario dell'e-mail «spazzatura», una volta ricevuto il messaggio, non si accorgerà di nulla di strano, ovvero leggerà esclusivamente il contenuto principale dello stesso (ciò che lo spammer, in sostanza, desidera

sia letto), mentre, contemporaneamente, agli «occhi» dei filtri antispam ogni messaggio del genere apparirà come «unico».

Lo screenshot esemplificativo qui sotto inserito mostra come un'e-mail di spam riconducibile alla tipologia sopra descritta sarà visualizzata dall'utente tramite il proprio client di posta elettronica:

A livello di codice sorgente, il corpo del messaggio di spam qui sopra raffigurato appare nel modo seguente:

```
<html><body><br><style><span dir=3D"theoretically"><big></big></span><span
title=3D"dues"><big><font color=3D"corroborated"><span></style><font lang=
=3D"softwares"></span><small></font><span></span></big></font></small></span>=
<font size=3D"quickens"></font><a href=3D"HtTp://=EF=BB=BFa=EF=BB=BFl=EF=
=BB=BFgeri=EF=BB=BFedz.=EF=BB=BFb=EF=BB=BFiz=EF=BB=BF/eskra/R0u8xTqHlEuAQi3=
vxH2WtqujVRY31/XQVTQEpsatAamV4qw.B"><small><font size=3D"maximized"></small>=
</font><style></style><style class=3D"brokers"><span dir=3D"dumbest"></style>=
</span><span face=3D"cornmeal"></span><span color=3D"attainment"></span>=
<style class=3D"Hurwitz"></style><img src=3D"HTtP://algeriedz.=EF=BB=BFbi=
=EF=BB=BFz/loisel/TrmU4rv8KKPSpTzRVSHjnVPKtuvBn/ga5i0NUpxLlyiG7qctk"><style
title=3D"scrumptious"><span></style><font dir=3D"handful"></font></span><style
face=3D"crimsoning"></style></a><span title=3D"detaches"></span><span>=
</span><font dir=3D"muscle"></font><style id=3D"survivals"></style><style>=
<span lang=3D"refugee"></style></span><small></small><font title=3D"curiosity"><font
class=3D"personnel"></font></font><style></style><font></font></body></html>
```

L'intero testo in linguaggio HTML, a parte i link evidenziati in rosso e le relative immagini, sembra, a prima vista, assolutamente privo di senso. Analizzando in dettaglio il codice qui riprodotto traspare in maniera netta come all'interno di esso si incontri, di frequente, il tag provvisto di vari attributi. Si

tratta, più precisamente, di un tag contenitore, utilizzato in particolar modo per formattare specifici elementi di una pagina web e/o per assegnare un identificatore univoco ad un determinato frammento di testo. Nel caso da noi esaminato, tra il tag di apertura ed il relativo tag di chiusura non è stato inserito alcun testo reale ed effettivo; in altre parole, i tag in questione sono stati introdotti semplicemente per «inquinare» il codice HTML di cui si compone il messaggio e-mail di spam.

Nella circostanza, merita una particolare e specifica attenzione il collegamento ipertestuale - anch'esso «imbrattato» - presente nel corpo del messaggio, link da noi evidenziato con il colore rosso. Una dettagliata analisi dello stesso ci permette di notare come gli spammer abbiano più volte aggiunto, alle normali lettere che compongono il collegamento in questione, peraltro in posizioni del tutto casuali, la sequenza «=EF=BB=BF». Attraverso tale specifica sequenza, nell'ambito del sistema esadecimale, viene identificato un determinato carattere UTF-8, utilizzato per indicare l'ordine dei byte che compongono un file di testo. Questo, tuttavia, risulta valido nel caso in cui il suddetto carattere venga impiegato per l'effettivo scopo al quale è preposto e sia quindi posizionato all'inizio del testo. Secondo le specifiche Unicode, tale carattere, una volta inserito a metà di un flusso di dati, deve essere interpretato come uno «spazio di larghezza zero non spezzabile» (in inglese «Zero-width no-break space»); si tratta pertanto, in sostanza, di un carattere nullo. Ciò significa che il client di posta elettronica, semplicemente, ignorerà la sequenza sopra indicata e procederà quindi facilmente all'apertura del link o al caricamento dell'immagine. Per i filtri antispam, tuttavia, ognuno di tali link risulterà come unico. Oltre a ciò, anche la parte finale del collegamento ipertestuale (evidenziata in arancione) è, in pratica, del tutto casuale.

Il codice sorgente qui analizzato, una volta «disinquinato» dagli elementi di disturbo, avrebbe il seguente aspetto:

```
<html><body><br><a href=3D"http://algeriedz.biz/eskra/"><img
src=3D"http://algeriedz.biz/loisel/"></a></body></html>
```

Come si può vedere, complessivamente, la parte «spazzatura» di cui si compone il codice HTML in causa supera considerevolmente, per estensione, la parte di messaggio riservata al contenuto vero e proprio da trasmettere al destinatario dell'e-mail. Tutta questa «spazzatura» viene generata in maniera casuale e risulta essere, di fatto, del tutto «unica» per ogni singolo messaggio di posta elettronica facente parte del mailing di spam qui esaminato. Il destinatario dell'e-mail, tuttavia, procedendo all'apertura del messaggio attraverso il proprio client di posta elettronica, visualizzerà, nella circostanza, soltanto un'e-mail elaborata in maniera particolarmente accurata, priva della benché minima traccia di qualsiasi trucco, espediente o sotterfugio applicato nell'occasione dagli spammer.

Le statistiche del primo trimestre 2014

Quota di spam nel traffico di posta elettronica

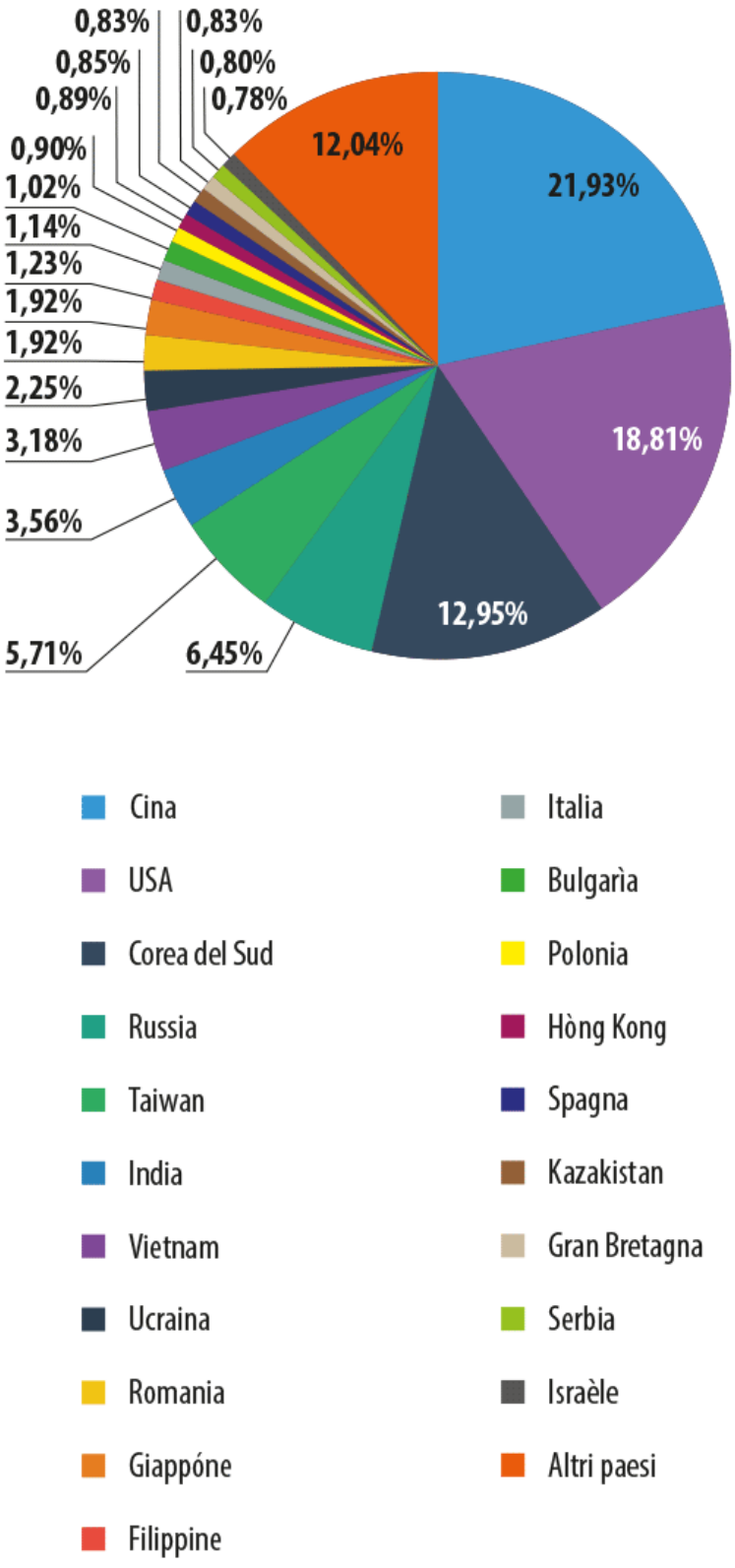
Nel primo trimestre del 2014, la quota relativa ai messaggi di spam presenti all'interno dei flussi di posta elettronica globali si è attestata su un valore medio pari al 66,34% del volume totale dei messaggi e-mail circolanti in Rete. Tale significativo indice ha fatto registrare un sensibile decremento (- 6,43%) rispetto al trimestre precedente. Tuttavia, se effettuiamo un debito confronto con l'analogo valore complessivamente riscontrato nei primi tre mesi del 2013, notiamo come la quota media di spam rilevata nel traffico e-mail nel corso del primo trimestre del 2014 sia diminuita in maniera quasi impercettibile rispetto allo stesso periodo di un anno fa (- 0,16%).

Quote di spam rilevate settimanalmente nel traffico e-mail nel corso del primo trimestre del 2014

Il grafico qui sopra evidenzia in maniera netta come, lungo tutto l'arco del trimestre oggetto del presente report, la quota inerente ai messaggi «spazzatura» rilevati nel traffico globale di posta elettronica abbia presentato forti oscillazioni, facendo peraltro segnare il valore più contenuto (61%) proprio nell'ultima settimana del trimestre qui analizzato.

Geografia delle fonti di spam

La speciale graduatoria relativa alla distribuzione geografica delle fonti dei messaggi di spam giunti nelle caselle di posta elettronica degli utenti della Rete non presenta variazioni di rilievo rispetto all’analogo rating da noi stilato riguardo al trimestre precedente.



Ripartizione geografica delle fonti di spam rilevate nel primo trimestre del 2014 - Suddivisione per paesi

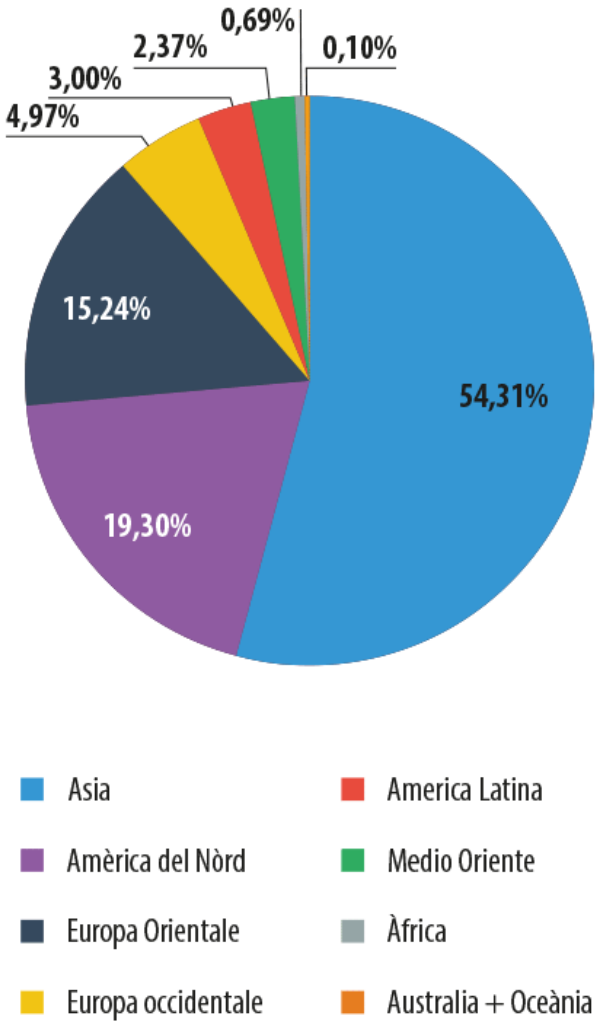
Le prime tre posizioni della TOP-20 da noi stilata sono andate ad appannaggio, rispettivamente, di Cina (- 0,34%), USA (+ 1,23%) e Corea del Sud (- 0,91%). La Russia, da parte sua - per ciò che riguarda la quantità complessiva di e-mail indesiderate distribuite in Rete, verso tutti e cinque i continenti - ha sopravanzato Taiwan ed è andata ad occupare il quarto posto della classifica qui sopra riportata;

rispetto al trimestre precedente, la Federazione Russa ha quindi «guadagnato» una posizione all'interno del ranking relativo alle fonti geografiche dello spam «mondiale» (+ 0,34%).

Riguardo alle rimanenti posizioni della TOP-10 inerente al primo trimestre dell'anno in corso, osserviamo come la situazione si sia mantenuta sostanzialmente stabile e non presenti, quindi, significative variazioni rispetto allo scorso trimestre.

Nella seconda metà della graduatoria in questione sono invece intervenuti cambiamenti di maggior rilievo. Le Filippine (+ 0,67%), ad esempio, sono passate dal 20° all' 11° posto del ranking qui esaminato, mentre la quota percentuale attribuibile al Kazakhstan ha fatto registrare una diminuzione pari allo 0,76%; il paese dell'Asia Centrale è in tal modo sceso dall'undicesima alla diciassettesima piazza della TOP-20. Il Canada, infine, decimo nel rating relativo al trimestre precedente, è addirittura precipitato al 27° posto della speciale classifica da noi stilata. Nel primo trimestre del 2014, l'indice ascrivibile al paese nordamericano è diminuito di oltre tre volte rispetto all'analogo valore riscontrato nell'ultimo trimestre dell'anno passato; nel breve volgere di tre mesi, la quota riconducibile ai messaggi di spam distribuiti nelle caselle di posta elettronica degli utenti della Rete di ogni angolo del globo dagli spammer insediati entro i confini del territorio canadese è di fatto scesa dall' 1,73% allo 0,49%.

Ripartizione delle fonti di spam per regioni geografiche

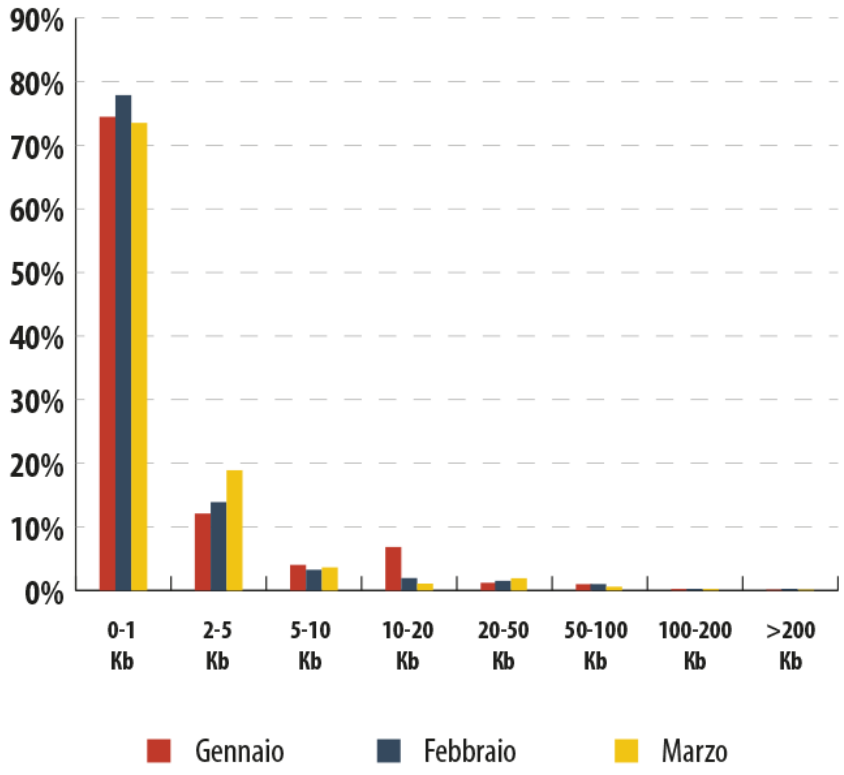


Suddivisione delle fonti di spam per macro-aree geografiche mondiali - Situazione relativa al primo trimestre del 2014

La graduatoria relativa alla ripartizione delle fonti di spam per macro-regioni geografiche mondiali risulta, anch'essa, sostanzialmente invariata rispetto al trimestre precedente. La leadership della speciale classifica «regionale» dello spam è quindi nuovamente andata ad appannaggio del continente asiatico, con un notevole margine percentuale rispetto alle altre macro-regioni del globo, anche se la quota attribuibile all'Asia ha evidenziato una lieve flessione (- 3,2%). Continuando la nostra analisi, rileviamo come l'indice percentuale relativo all'America Settentrionale sia rimasto in pratica immutato (- 0,01%), mentre le quote riguardanti le rimanenti macro-aree mondiali risultano leggermente aumentate.

Dimensioni dei messaggi di spam

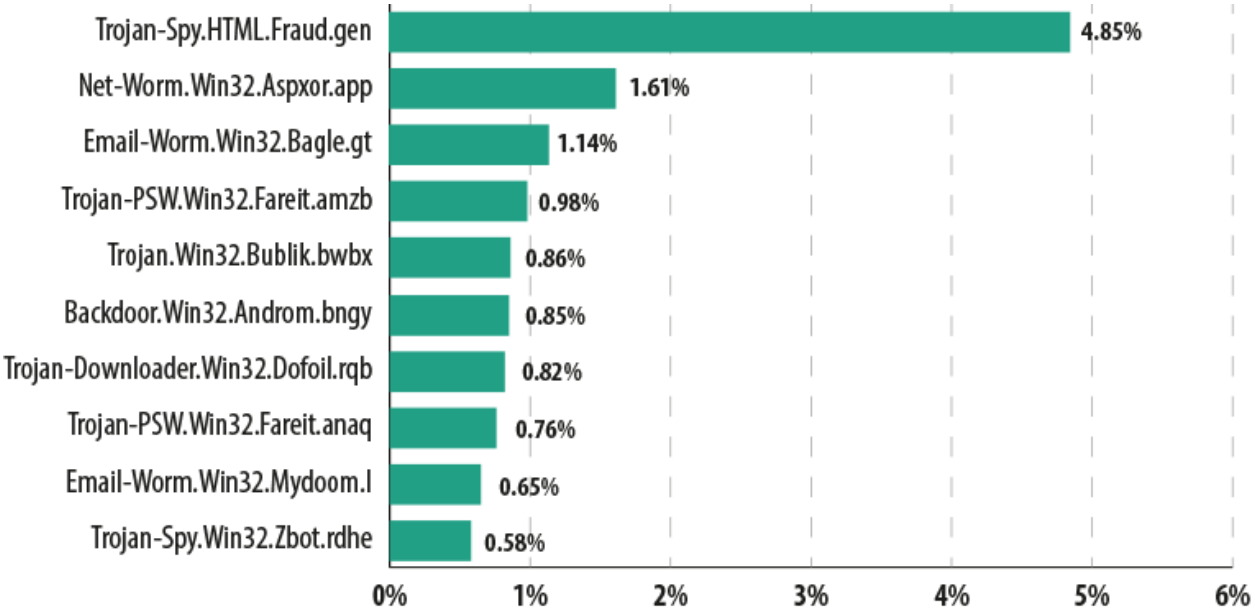
Così come in precedenza, all'interno dei flussi di spam risulta particolarmente elevato il numero dei messaggi e-mail «spazzatura» aventi dimensioni estremamente contenute (1 Kb o addirittura meno di un kilobyte). Il grafico qui sotto riportato evidenzia in maniera netta il predominio - lungo tutto l'arco del trimestre qui analizzato - dei messaggi di spam «super-brevi» rispetto alle e-mail di maggiori dimensioni.



Dimensioni delle e-mail di spam - Quadro relativo al primo trimestre del 2014

Sottolineiamo, ad ogni caso, come nel traffico di posta elettronica globale dello scorso mese di gennaio si sia registrato un significativo incremento del numero dei messaggi e-mail indesiderati con dimensioni comprese nel range 10 - 20 Kb. Probabilmente, tale specifica situazione è stata generata dall'allestimento, da parte degli spammer, dei tradizionali mailing di massa riconducibili al cosiddetto spam «festivo», volto a promuovere prodotti e servizi di ogni genere, tramite appositi messaggi e-mail ispirati alle tematiche suggerite dalle più importanti ricorrenze stagionali. Nella circostanza, come è noto, coloro che si «dilettano» a distribuire in rete vere e proprie montagne di e-mail di spam, elaborano messaggi di posta particolarmente curati dal punto di vista cromatico, ricchi di immagini, simboli e decorazioni, nel più classico stile «festivo».

Allegati maligni rilevati nel traffico di posta elettronica



TOP-10 relativa ai programmi maligni maggiormente diffusi nel traffico di posta elettronica - Situazione riguardante il primo trimestre del 2014

La prima posizione della speciale graduatoria da noi stilata relativamente ai programmi nocivi rilevati con maggior frequenza dal nostro antivirus e-mail all'interno del traffico di posta elettronica globale risulta nuovamente occupata dal malware classificato con la denominazione di Trojan-Spy.HTML.Fraud.gen, peraltro con un cospicuo margine percentuale rispetto ai diretti «concorrenti». Il software nocivo in questione viene abitualmente diffuso tramite le e-mail di phishing e costituisce, tuttora, uno dei principali metodi di attacco presenti nel sempre nutrito «arsenale» dei phisher. Ricordiamo, a tal proposito, come il suddetto programma trojan sia stato elaborato dai suoi autori sotto forma di una pagina HTML in grado di riprodurre i form di registrazione di determinati servizi di Internet banking, sistemi di pagamento online o altri servizi erogati nel World Wide Web. I cybercriminali di turno utilizzano poi i dati di registrazione illegalmente carpiti, inseriti dall'utente in tali «form» fasulli, per impadronirsi delle somme di denaro depositate nei conti bancari violati.

La seconda e la settima posizione della TOP-10 qui analizzata risultano occupate da due varianti del noto worm di rete denominato Asprox (Net-Worm.Win32.Aspxor). I programmi nocivi appartenenti a tale famiglia di malware, ormai ampiamente nota agli esperti di sicurezza IT, sono in grado di ricercare automaticamente, in Rete, i siti web vulnerabili, i quali vengono in seguito infettati in maniera massiccia, allo scopo di alimentare il processo di diffusione del bot. I net-worm in questione sono inoltre provvisti di ulteriori temibili funzionalità dannose; in effetti, essi sono stati appositamente creati dai virus writer anche con il preciso intento di effettuare il download ed avviare l'esecuzione di altri software nocivi, raccogliere preziose informazioni sensibili all'interno del computer-vittima sottoposto ad attacco (quali, ad esempio, le password custodite nella macchina infetta, così come i dati utilizzati per ottenere l'accesso agli account relativi ai programmi di posta elettronica ed ai client FTP), nonché inviare elevate quantità di messaggi di spam.

Il terzo gradino del «podio» virtuale è andato ad appannaggio del worm di posta elettronica classificato dagli esperti ed analisti di malware come Email-Worm.Win32.Bagle.gt, anch'esso un «habitué» della classifica qui esaminata. La principale funzionalità di cui sono dotati tutti gli e-mail worm consiste nel

raccogliere illecitamente gli indirizzi di posta presenti nei computer-vittima contagiati e realizzare il successivo processo di auto-diffusione in Rete, condotto tramite gli account di posta elettronica sottratti. I worm riconducibili alla famiglia Bagle, tuttavia, in aggiunta alla funzionalità standard qui sopra illustrata, risultano provvisti di ulteriore potenziale nocivo: essi sono difatti in grado di connettersi ed interagire da remoto con il centro di controllo allestito dai cybercriminali, e di ricevere quindi da quest'ultimo appositi comandi volti a generare il download e la successiva installazione di altri software maligni sui computer-vittima infettati.

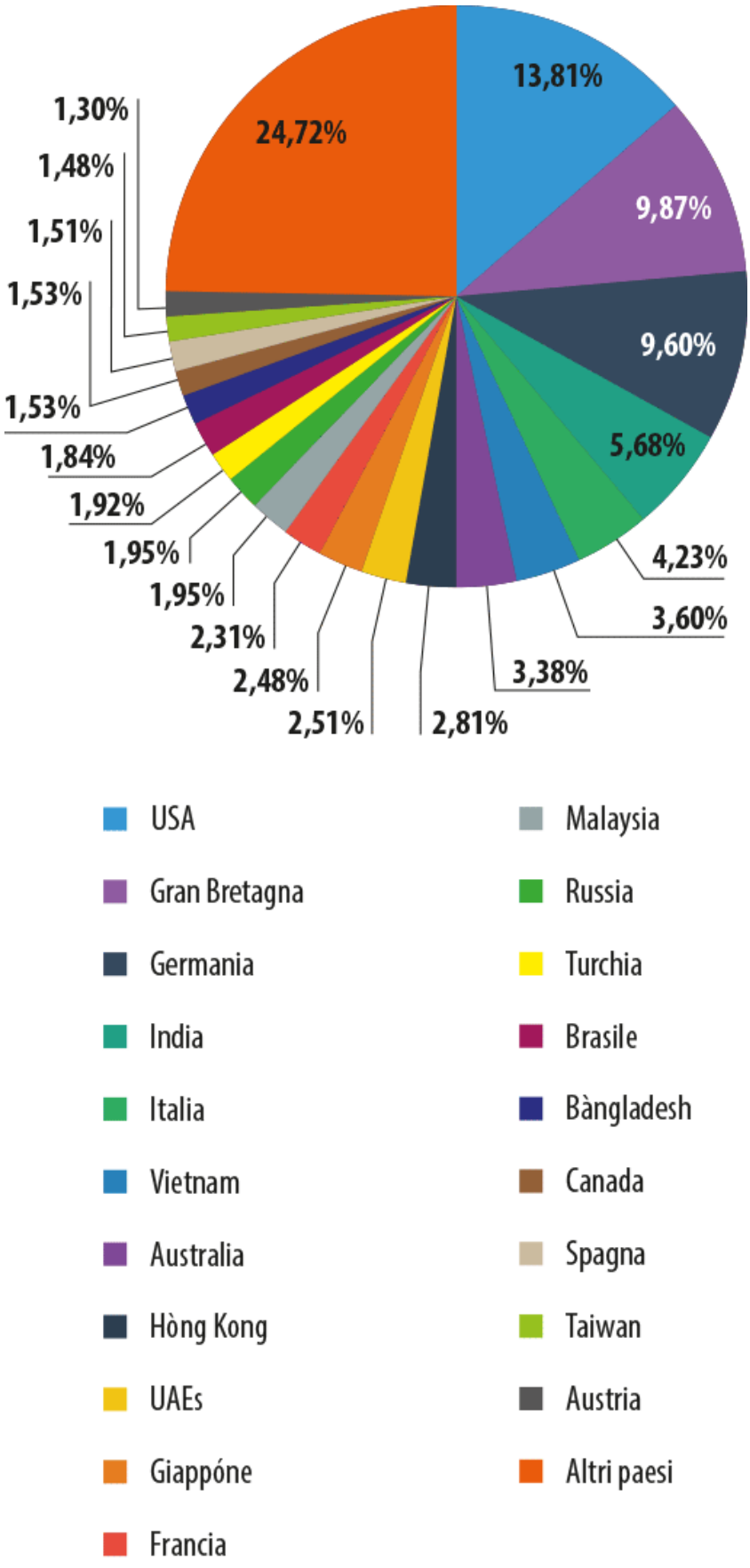
Al quarto e all'ottavo posto della TOP-10 qui sopra riportata si sono collocati due programmi Trojan appartenenti alla famiglia di malware denominata Fareit; tali software nocivi sono stati diffusi in maniera particolarmente attiva, attraverso la posta elettronica, durante lo scorso mese di gennaio. Si tratta, nella fattispecie, di programmi nocivi in grado di compiere il furto delle password di cui si avvalgono gli utenti per accedere ai propri account, così come di realizzare pericolosi ed insistiti attacchi DDoS (Distributed Denial of Service), generare il download ed avviare l'esecuzione di software arbitrario nel sistema informatico preso d'assalto. Allo stesso modo, i due «rappresentanti» della suddetta famiglia di malware, entrati a far parte del rating da noi stilato relativamente al primo trimestre dell'anno 2014, provvedono ad effettuare il download dei famigerati programmi Trojan appartenenti alla famiglia Zbot, i quali vengono poi lanciati ed eseguiti sul computer-vittima. Inoltre, i programmi malware riconducibili alla famiglia Fareit sono ugualmente specializzati nel furto dei «wallet» utilizzati nell'ambito del sistema Bitcoin (si tratta, nello specifico, dei «portafogli» virtuali nei quali vengono custoditi, sul computer dell'utente o in altri luoghi virtuali, i Bitcoin generati) e di altre criptovalute (in totale, circa 30 diverse valute digitali).

La quinta piazza della speciale graduatoria relativa ai malware più diffusi all'interno dei flussi e-mail mondiali risulta occupata dal software nocivo rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Trojan.Win32.Bublik.bwbx; tale programma dannoso è in grado di realizzare il download di ulteriori software maligni sul computer dell'utente, ed in particolar modo dei malware che compongono la temibile famiglia Zbot.

La sesta posizione del ranking analizzato nel presente capitolo del nostro consueto report trimestrale dedicato all'evoluzione del fenomeno spam è andata ad appannaggio del programma nocivo classificato con la denominazione di Backdoor.Win32.Androm.bngy. I software maligni riconducibili alla famiglia Androm 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.

Al nono posto della graduatoria troviamo poi una «vecchia conoscenza» nell'ambito della TOP-10 in questione, ovvero il worm di posta elettronica denominato Email-Worm.Win32.Mydoom.l.

L'ultima posizione della classifica da noi elaborata annovera infine la presenza di un noto Trojan-spy appartenente alla famiglia di malware conosciuta con l'appellativo di Zbot. Come è noto, tale famiglia - formata da pericolosi software nocivi - risulta altamente specializzata nel furto delle informazioni confidenziali custodite nei computer degli utenti sottoposti ad attacco. Oltre a ciò, il suddetto programma Trojan è ugualmente in grado di generare l'installazione di Cryptolocker sul computer preso di mira, un programma malware «estorsore» che richiede all'utente-vittima una certa somma di denaro per effettuare la decodifica dei dati precedentemente criptati.

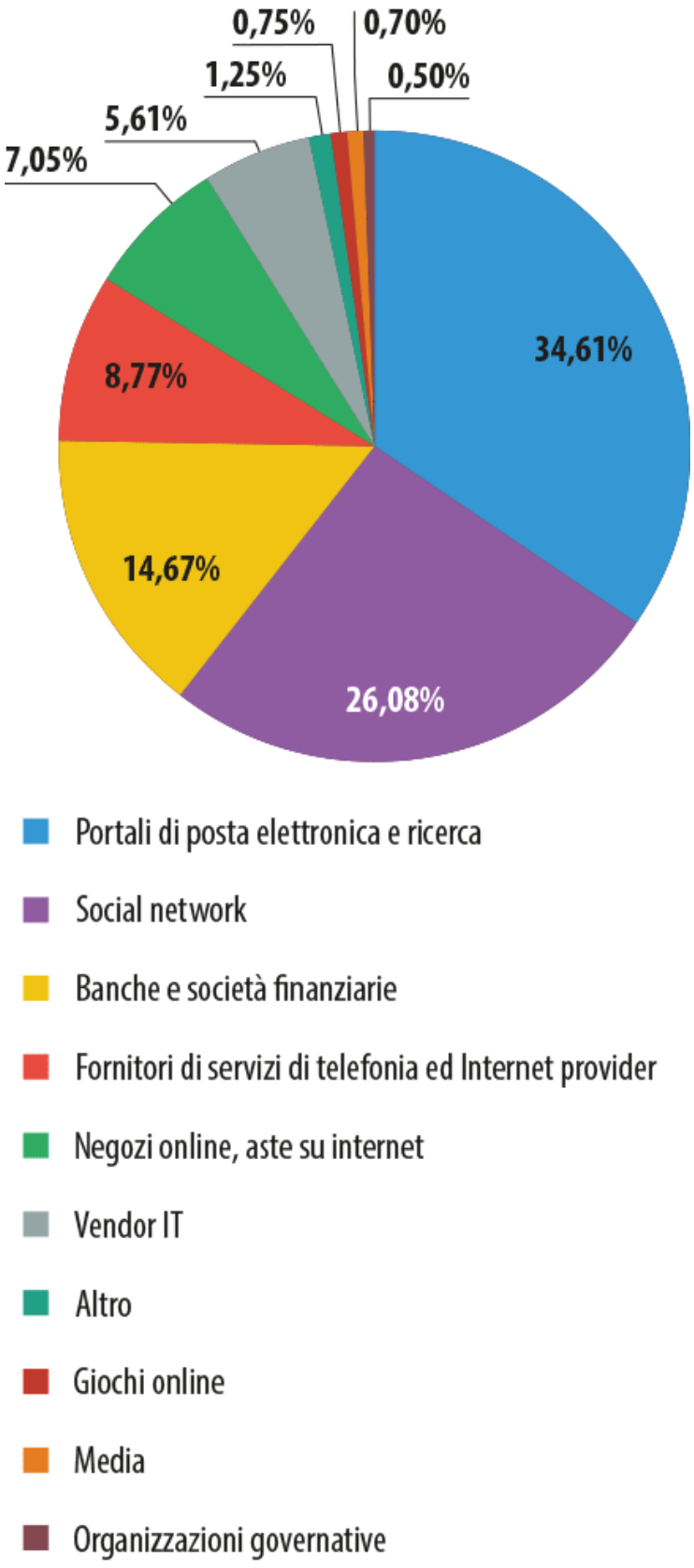


Suddivisione per paesi dei rilevamenti effettuati dal modulo antivirus e-mail nel corso del primo trimestre del 2014

La speciale TOP-20 da noi stilata - relativa ai 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 - evidenzia come, rispetto al trimestre precedente, sia sensibilmente aumentata la quota percentuale attribuibile agli Stati Uniti (+ 3,68%), mentre, al tempo stesso, hanno fatto registrare una significativa flessione gli indici riguardanti, rispettivamente, Gran Bretagna (- 2,27%), Germania (- 1,34%) ed Hong Kong (- 2,73%). In tal modo, gli USA, che nello scorso trimestre occupavano «soltanto» il terzo posto del ranking, si sono nuovamente collocati sul gradino più alto del «podio» virtuale, nell'ambito della graduatoria riservata ai paesi verso i quali è stata inviata la maggior quantità di messaggi di spam contenenti allegati maligni. Concludiamo la nostra breve rassegna osservando come gli indici percentuali relativi agli altri paesi presenti in classifica evidenzino solo lievi variazioni rispetto agli analoghi valori riscontrati nell'ultimo trimestre dello scorso anno.

Phishing

A partire dal trimestre oggetto del presente report abbiamo deciso di unire due delle principali categorie da noi precedentemente definite per ciò che riguarda, nello specifico, le organizzazioni sottoposte con maggior frequenza agli attacchi portati dai phisher. In effetti, i raggruppamenti «Posta elettronica, programmi di instant messaging» e «Motori di ricerca» sono stati in pratica fusi in un'unica, nuova categoria, denominata «Portali di posta elettronica e ricerca». Il fatto è che tali portali mettono spesso a disposizione dei propri utenti un unico account generale, il quale può essere utilizzato da questi ultimi per effettuare le necessarie impostazioni, per la cronologia delle ricerche eseguite, nonché in qualità di account di posta elettronica; oltre a ciò, mediante l'account unico si può ugualmente accedere ai servizi in-the-cloud, oppure usufruire di ulteriori opportunità previste nell'ambito delle attività svolte dal portale.



TOP-100 relativa alle organizzazioni maggiormente sottoposte agli attacchi di phishing* nel corso del primo trimestre del 2014 - Suddivisione per categorie dei rilevamenti eseguiti dal modulo «Anti-phishing»

* La classifica delle 100 organizzazioni (divise 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.

Come era lecito attendersi, la nuova categoria «Portali di posta elettronica e ricerca» è andata subito ad occupare la prima posizione della speciale TOP-100 del phishing da noi elaborata. Nonostante gli account attualmente disponibili sui portali e-mail e di ricerca offrano un ampio ventaglio di opportunità ai propri utenti, la maggior parte degli attacchi organizzati dai phisher nei confronti di tali siti web risulta essere esclusivamente orientata al furto dei dati sensibili che consentono l'accesso alla casella di posta elettronica dell'utente. E' di particolare importanza porre in risalto come, oltre ad utilizzare l'e-mail box violata per i propri fini, i malintenzionati abbiano, nella circostanza, anche la possibilità di controllare il contenuto della casella di posta dell'utente-vittima, allo scopo di verificare la presenza di ulteriori login e password. Inoltre, come è noto, numerosi siti web utilizzano spesso proprio l'account di posta elettronica dell'utente per le operazioni di recupero della password eventualmente dimenticata. Il fatto è che, mentre alcuni siti, nell'occasione, inviano all'utente esclusivamente un link per poter generare la nuova password, altre risorse web inseriscono invece tale password direttamente nel messaggio inoltrato via e-mail. Vari siti Internet, infine, una volta completate le procedure di registrazione, inviano ai propri utenti un messaggio di posta elettronica contenente login e password per accedere all'account appena creato. Per prevenire la perdita di dati confidenziali, gli attuali sistemi di posta offrono spesso il metodo di autenticazione a due fattori: ciò significa, in pratica, che, per ottenere l'accesso, oltre a login e password, l'utente dovrà necessariamente inserire un codice segreto, precedentemente inviato tramite SMS. Un ulteriore metodo, di indubbia efficacia, consiste nel rimuovere semplicemente, dalla propria e-mail box, tutti i messaggi contenenti informazioni di natura confidenziale o sensibile.

Come evidenzia il grafico qui sopra riportato, gli account relativi ai social network continuano ad essere uno dei bersagli prediletti dai phisher; le reti sociali occupano infatti la seconda posizione della speciale graduatoria riservata alle organizzazioni maggiormente sottoposte agli attacchi di phishing. Rispetto al trimestre precedente, tuttavia, la quota attribuibile alla suddetta categoria, nell'ambito della TOP-100 qui esaminata, ha presentato una flessione pari all' 1,44%.

Per contro, è cresciuto in maniera sensibile (+ 2,47%) l'indice percentuale relativo al raggruppamento che riunisce i negozi Internet e le aste online. Tale specifica situazione è stata in primo luogo determinata dagli insistiti attacchi condotti nei confronti dei servizi web adibiti alla distribuzione di coupon sconto, così come dalle numerose campagne di phishing allestite a scapito delle agenzie specializzate nella vendita online di biglietti per eventi e manifestazioni di vario genere.

Ha fatto inoltre registrare una significativa diminuzione (- 2,46%) la quota ascrivibile agli attacchi condotti nei confronti della categoria che raggruppa i vendor IT; non sono state invece riscontrate variazioni di rilievo relativamente alla ripartizione degli indici percentuali attribuibili alle rimanenti categorie facenti parte del rating in questione.

Conclusioni

Ormai quasi tutti, al giorno d'oggi, possiedono uno o più dispositivi mobile «intelligenti», mentre, in pratica, la quasi totalità delle risorse Internet che godono di maggiore popolarità presso il vasto pubblico degli utenti della Rete è dotata di apposite versioni mobile, per facilitare la navigazione tramite smartphone o tablet. Spicca inoltre, all'interno del panorama «mobile», la presenza di varie applicazioni

che riscuotono un successo davvero enorme presso gli utenti di ogni angolo del globo. L'ampia popolarità raggiunta da tali applicazioni viene purtroppo già sfruttata da una nutrita schiera di malfattori intenti a distribuire nelle e-mail box del pubblico della Rete un considerevole numero di messaggi di spam mascherati sotto forma di notifiche e comunicazioni inviate (in apparenza!) attraverso alcune tra le più celebri app mobile del momento. Con il passare del tempo, la quantità di simili messaggi e-mail contraffatti, all'interno dei flussi di spam, è destinata inevitabilmente ad accrescersi. Allo stesso modo, è lecito prevedere un sensibile aumento del numero delle campagne di phishing che si prefiggono di carpire, come obiettivo principale, proprio le password utilizzate per gli account relativi alle applicazioni mobile.

Vengono attualmente già diffusi, attraverso la posta elettronica, i programmi malware appositamente sviluppati dai virus writer per colpire il sistema operativo mobile Android; il loro numero, tuttavia, risulta ancora piuttosto contenuto. E' ad ogni caso prevedibile, all'interno del traffico e-mail globale, un significativo aumento della quantità di software nocivi specificamente creati per attaccare le piattaforme mobile.

Il principale obiettivo della maggior parte dei programmi maligni distribuiti attraverso i flussi di posta elettronica è indubbiamente rappresentato dal furto dei dati confidenziali custoditi dall'utente sul proprio computer. Nel corso del trimestre oggetto del presente report, tuttavia, sono risultati particolarmente popolari, presso gli ambienti cybercriminali, anche i software nocivi in grado di inviare elevate quantità di messaggi di spam e di realizzare insistiti attacchi DDoS. Desideriamo sottolineare, nella circostanza, come la maggior parte dei malware più diffusi nell'ambito dell'attuale traffico di posta mondiale possieda caratteristiche di spiccata multifunzionalità: tali software dannosi possono in effetti sottrarre dati sensibili dal computer dell'utente-vittima, così come asservire il computer sottoposto ad attacco ad un'estesa botnet, oppure generare il download e la successiva installazione di ulteriori programmi malware.

Per cercare di eludere l'azione svolta dai filtri antispam, gli spammer hanno continuato a far uso di trucchi di vario genere. Uno dei metodi più sofisticati ed avanzati di cui si avvalgono attualmente gli spammer è rappresentato dall'«imbrattamento» dei messaggi e-mail mediante l'aggiunta di specifici tag HTML; coloro che si dilettano a riempire le caselle di posta elettronica degli utenti della Rete di ogni genere di e-mail spazzatura ricorrono di frequente, oltre che all'«inquinamento» del codice HTML, anche all'offuscamento dei link di volta in volta inseriti nei messaggi di spam. A tal proposito, uno degli ultimi trucchi adottati consiste nell'aggiungere al collegamento ipertestuale un carattere UTF-8, il quale, nel caso in cui non risulti collocato all'inizio del testo, viene poi interpretato come un carattere nullo. Di fatto, la codifica UTF-8 può presentare un numero piuttosto considerevole di «astuzie» del genere, le quali vengono periodicamente utilizzate anche da malintenzionati.

La maggior parte degli attacchi di phishing individuati e neutralizzati nel corso del trimestre qui esaminato è risultata essere indirizzata nei confronti degli account utilizzati per accedere ai servizi di posta elettronica. Desideriamo con l'occasione sottolineare una volta di più come, spesso, gli utenti non adottino le necessarie cautele nel far uso del proprio client e-mail; molte persone, in effetti, continuano tuttora a servirsi di login e password particolarmente semplici. Ricordiamo, nella circostanza, come una e-mail box violata possa di fatto fornire ai malintenzionati un comodo accesso a tutte le informazioni in essa custodite, incluso login e password utilizzati per operare con ulteriori account. Raccomandiamo pertanto, a tutti gli utenti, di far uso di password particolarmente solide e complesse per ciò che riguarda l'accesso alle proprie caselle di posta elettronica e, qualora sia possibile, di avvalersi di un sistema di autenticazione a doppio fattore.