

# Lo spam nel mese di Marzo 2014

---

Tat'jana Šerbakova

Marija Vergelis

## Sommario

Le peculiarità del mese .....	1
Spam e festività .....	1
Lo spam linguistico .....	3
Telefonia.....	4
Le statistiche.....	6
Quota di spam nel traffico di posta elettronica .....	6
Ripartizione geografica delle fonti di spam.....	6
Allegati dannosi rilevati nel traffico e-mail .....	12
Peculiarità e tratti caratteristici dello spam nocivo di marzo .....	15
Phishing .....	17
Conclusioni .....	20

## Le peculiarità del mese

Lungo tutto l'arco del mese di marzo 2014, gli spammer hanno condotto non soltanto i tradizionali mailing di massa riconducibili al cosiddetto spam "festivo", volto a reclamizzare prodotti e servizi di ogni genere, ma hanno cercato di carpire le informazioni personali degli utenti di noti social network, tramite appositi messaggi e-mail ispirati alle tematiche suggerite da alcune delle più importanti ricorrenze stagionali.

Nell'ambito dello spam pubblicitario che ha contraddistinto il mese oggetto del presente report spiccano, in particolar modo, le campagne organizzate per recapitare nelle e-mail box degli utenti offerte commerciali di varia natura, relative a prodotti per automobilisti, proprietà immobiliari in Crimea, servizi linguistici e servizi per ottimizzare i costi e l'efficienza delle comunicazioni telefoniche aziendali. Molti di tali mailing di massa sono stati individuati dai nostri esperti non solo nel segmento di lingua russa di Internet, ma anche in altri segmenti della Rete, frequentati da utenti che parlano lingue diverse.

## Spam e festività

Come è noto, nell'anno 2014 le date previste per la celebrazione della Pasqua ortodossa e della Pasqua cattolica coincidono, visto che in entrambi i casi la festività in questione cade il giorno 20 aprile. Alla vigilia di tale importante ricorrenza religiosa, come al solito, all'interno dei flussi di spam che convogliano messaggi e-mail elaborati in lingua inglese, è stato dato ampio spazio alle consuete

pubblicità di articoli di lusso contraffatti ed articoli da regalo concepiti sotto forma di prodotti dolciari, pubblicità realizzate sfruttando le tradizionali tematiche pasquali.

From: [redacted] To: [redacted] Cc: [redacted] Subject: That TIME of week

From: [redacted] To: [redacted] Cc: [redacted] Subject: A Dozen Ways to Say Happy Easter

**The only 100% Identical Replicas in the WORLD**  
**Easter Orders must be in by April 12th**

**ORDER BEFORE APRIL 12TH**  
**&**  
**USE COUPON CODE**  
**asgood**


**WE USE 100% IDENTICAL**  
**Metals**  
**Materials**  
**Labeling**  
**Hand Movements**

**Rolex Explorer II**  
**\$71.20** [www.\[redacted\].com](http://www.[redacted].com)

Did you know the Easter bunny is coming soon?  
Then Mother's day, then Father's Day.  
*They will never know the difference, it will be our little secret.*

**Note:**  
The above image file contains more information about our product.  
There is also a coupon which is valid to use on any order before April 12th.  
Orders placed before this day will also ensure item availability at that time.

**CHERRY MOON FARMS®**  
Fruit Baskets • Gift Baskets • Spa Gifts




Easter Chocolates  
New Secret Garden Cookies With Bear  
Easter Basket  
Easter Chocolates Covered Sampler  
New Easter Cookie Assortment  
Children's Easter Basket  
New Gingerbread Birdhouse  
3 Easter Cake Pops & Half Dozen  
30 Easter Cookies

Anche i messaggi di spam pubblicitario composti in lingua russa, dedicati alla celebrazione della Pasqua, hanno ampiamente reclamizzato prodotti dolciari e souvenir decorati con i classici temi e simboli pasquali.

From: [redacted] on behalf of [redacted]  
To: [redacted]  
Cc: [redacted]  
Subject: Пасхальные подарки и сувениры для Ваших коллег и сотрудников

**ПОДАРКИ**

**Подарки на Пасху**

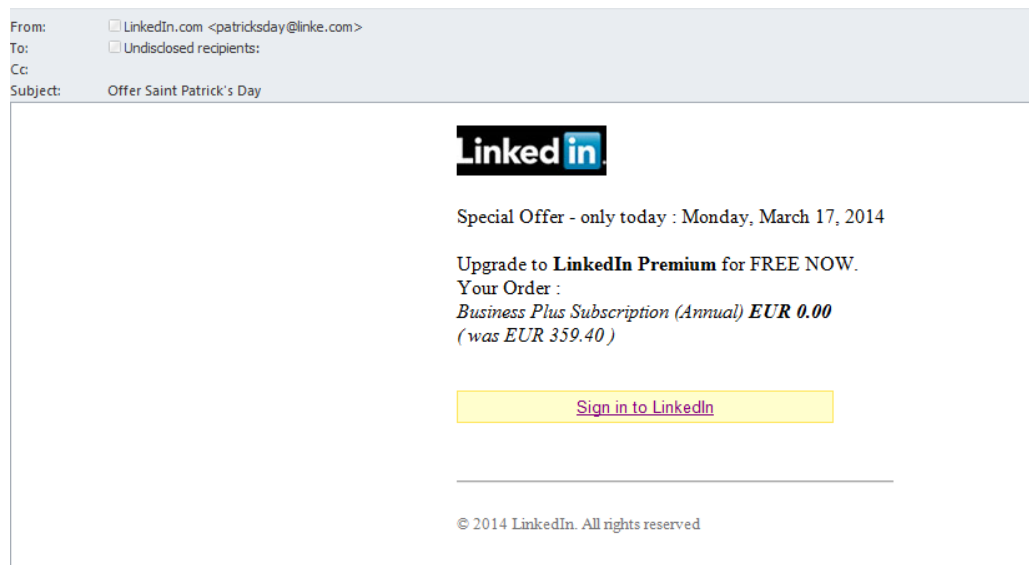


**Уважаемые клиенты!**  
Вы задумывались над корпоративным подарком на Пасху для родных, друзей, коллег или клиентов? Обратите внимание

Desideriamo sottolineare come nel mese di marzo il volume complessivo dello spam dedicato alle festività di Pasqua sia risultato piuttosto contenuto; naturalmente, per ciò che riguarda il successivo mese di aprile, è logico attendersi un considerevole aumento del numero dei messaggi e-mail di spam ispirati a tale tematica.

Segnaliamo, inoltre, come i malintenzionati abbiano fatto ricorso al tema del Giorno di San Patrizio, importante ricorrenza celebrata il 17 marzo di ogni anno, per cercare di realizzare il furto di login e password relativi agli account aperti dagli utenti della Rete presso LinkedIn, il popolare social network professionale. Tramite un apposito mailing di massa nocivo, "dedicato" alla suddetta festività, è stato in effetti proposto, ai destinatari dei messaggi di spam, di usufruire di un account premium nell'ambito di

tale rete sociale. Per poter accedere all'account personale così generosamente messo a disposizione, i "fortunati" utenti avrebbero dovuto semplicemente cliccare sul link inserito nella parte conclusiva del messaggio. Il collegamento ipertestuale in questione, tuttavia, non conduceva verso il sito web ufficiale del social network LinkedIn, bensì ad un'insidiosa pagina di phishing, per cui, nella circostanza, tutti i dati inseriti nell'apposito form predisposto dai malfattori sarebbero stati poi trasmessi ai truffatori di turno. Come evidenzia lo screenshot inserito di seguito, per conferire all'e-mail un aspetto di credibilità e legittimità, i malintenzionati hanno utilizzato il logo del celebre social network, nonché una firma automatica. Inoltre, l'indirizzo del mittente appariva alquanto plausibile, nonostante fosse stato inserito, da parte dei cybercriminali, un nome di dominio in forma abbreviata, ovvero <linke.com>, invece del nome di dominio ufficiale che identifica la suddetta società, <linkedin.com>.



## Lo spam linguistico

Nel mese di marzo 2014, i flussi dello spam "di lingua russa" sono stati ugualmente caratterizzati da un elevato numero di messaggi e-mail recanti proposte per lo studio delle lingue straniere mediante l'utilizzo dei più disparati metodi di apprendimento. Ai destinatari di tali e-mail è stata ad esempio offerta l'opportunità di poter imparare una lingua straniera in soli 10 giorni... con la promessa di svelare chissà quale recondito segreto linguistico. Nel campo <From>, al posto del nome del mittente, i messaggi di spam in questione presentavano, nella maggior parte dei casi, la dicitura «Language Learning». Inoltre, i domini di posta elettronica inseriti dagli spammer al posto di indirizzo del mittente variavano da un messaggio all'altro; si trattava, nella circostanza, di domini di recente creazione. I messaggi contenevano dei link particolarmente estesi, i quali, dopo una serie di reindirizzamenti, convogliavano gli utenti verso un sito web pubblicitario, in cui si proponevano allettanti sconti per l'acquisto di un set di cd per l'apprendimento della lingua straniera preferita in base ad una specifica metodologia di studio. Al momento di inviare l'ordine, l'utente avrebbe potuto poi scegliere di effettuare l'acquisto mediante il sistema di pagamento più comodo.

From: Language Learning <Aval.LW93@...>  
 To:  
 Cc:  
 Subject: Discover the ability of the [redacted] Approach to help you learn a new language quickly.

**Approach**

**Its Almost Ridiculous.**  
 Learning A Second Language Leads To SHOCKING Stories!

It's almost ridiculous how many incredible stories come from learning a second language.

Amazing stories continue to pour in from language learners of all ages. They're shocked at how effective the [redacted] Approach program is!

*"My colleagues were astonished"*

*"My fellow personnel looked on in utter amazement"*

*"It's absolutely brilliant. I'm impressed."*

**Astonished, amazed, flabbergasted, brilliant. These are just a few of the words our customers have used to describe their experience with the [redacted] Approach program.**

You can have an amazing story to tell, too. Find out how learning another language can bring you closer to your family, allow you to travel with ease, or even save a life!

**Check out these real customer testimonials:**

From: [redacted] <[redacted]@lozfebrfs.us>  
 To:  
 Cc:  
 Subject: Language learning made quick & easy

**Learn any Foreign Language in 10 Days!**

**The trick for your brain to learn a new language fast**

Discover how you can rapidly learn any new language in just 10 days using this sneaky linguistic secret...

**Free Presentation: Click Here.**

From: [redacted] Approach Language Learning <[redacted]@lozfebrfs.us>  
 To:  
 Cc:  
 Subject: 1 Sneaky Linguistic Secret to Learn a Foreign Language in just 10 Days Revealed

**Sneaky Linguistic Secret to Learn a Foreign Language in just 10 Days Revealed**

From: [redacted] Approach Language Learning <[redacted]@lozfebrfs.us>  
 To:  
 Cc:  
 Subject: 1 Sneaky Linguistic Secret to Learn a Foreign Language in just 10 Days Revealed

**Uncover the trick for your brain to learn a new language fast**

Hanno presentato tematiche di natura linguistica anche i messaggi di spam riconducibili ad un'altra tipologia di mailing di massa, ovvero i mailing allestiti da numerose agenzie di traduzione allo scopo di pubblicizzare i servizi offerti. All'interno del traffico di posta elettronica del mese di marzo, è stato da noi individuato un considerevole numero di campagne di spam del genere, peraltro condotte in varie lingue: inglese, tedesco, francese, spagnolo, olandese. Talvolta lo stesso messaggio di spam conteneva il medesimo testo in molteplici lingue. Le e-mail in questione illustravano l'elenco delle lingue di lavoro proposte dalle varie agenzie, le combinazioni linguistiche offerte, così come un elenco completo dei servizi effettuati (interpretariato, traduzioni scritte, generi di traduzione più richiesti). Per contattare le agenzie in causa, i destinatari dei messaggi avrebbero potuto avvalersi degli appositi link inseriti per condurre ai siti web delle varie società, oppure usufruire dei numeri telefonici indicati, o degli indirizzi di posta elettronica specificati dai responsabili delle agenzie di traduzione.

<p>From: Lore Gillebert &lt;[redacted]&gt;          To:          Cc:          Subject: Vertaaldienst tot 31 talen</p> <p>Geachte klant,</p> <p>Wij bieden professionele vertalingen m.b.t. alle onderwerpen aan. Volgende talen zijn momenteel beschikbaar:</p> <p>Duits          Italiaans          Frans          Engels          Spaans          Russisch          Tjechisch          Hongaars          Sloveens          Kroatisch          Pools          Portugees          Deens          Zweeds          Fins          Nederlands          Noors          Slovaaks          Turks          Japans          Chinees          Arabisch          Roemeens          Grieks          Oekraïens</p> <p>U kunt de gewenste tekst via <a href="#">Colist</a> in We kijken uit naar uw bestelling</p> <p>Mvg.          Uw vertaalteam</p>	<p>From: Mareike Burz &lt;[redacted]@bersetzungen.com&gt;          To:          Cc:          Subject: Übersetzungen ( alle Sprachen )</p> <p>Sehr geehrte Damen und Herren,</p> <p>auf diesem Wege wollten wir uns gern erkundigen, ob wir Ihnen per Übersetzungsservice zuschicken dürfen?</p> <p>Wir bieten alle gängigen Sprachenkombinationen zu günstigen Preisen.</p> <p>Wir würden uns freuen, von Ihnen zu hören.</p>	<p>From: Zoe Abalmon &lt;[redacted]@ubunt-message.org&gt;          To:          Cc:          Subject: Aanbieding van vertalingen door native speakers</p> <p>Geachte dames en heren,</p> <p>Wij zijn een Europese onderneming en bieden vertalingen tot 25 talen aan m.b.t. alle onderwerpen. Onze vertalers zijn uitsluitend native speakers.</p> <p>Via <a href="#">Colist</a> kunt u de kosten voor de gewenste tekst berekenen.</p> <p>Wanneer de prijs met uw voorstellingen overeenkomt, verzoeken wij u de aanvraag te bevestigen en ontvangt u op korte termijn de gewenste vertaling.</p>
<p>From: [redacted] France &lt;[redacted]&gt;          To:          Cc:          Subject: Vertaling Traduction</p> <p>Bonjour,</p> <p>Notre métier est de traduire vos documents dans 70 couples de langues. Nos références</p> <p>Nous pouvons recevoir tous types de format de document (Suite Microsoft, PDF, Indesign ou autres)</p> <p>Vous avez besoin d'une traduction de qualité, d'une agence réactive et qui respecte vos délais?</p> <p>Envoyez-nous par retour vos documents pour obtenir un devis gratuit en moins de 24 heures. Nos traducteurs assermentés ou non et interprètes sont tous des professionnels diplômés qui exercent depuis plus de dix ans.</p> <p>Pour traduire votre site internet vous pouvez nous mettre en relation avec votre Webmaster ou l'agence de communication qui a créé votre site. Nous envisagerons avec eux la meilleure solution technique pour traduire votre site internet (-)</p>	<p>From: [redacted] &lt;[redacted]@gmail.com&gt;          To:          Cc:          Subject: La traducción que necesitas</p> <p><b>¡Hola! ¿Cómo estas?</b></p> <p><b>No ponemos a tus ordenes para apoyarte en el proyecto de traducción que necesitas.</b></p> <p>Traducciones INGLES-ESPAÑOL, ESPAÑOL-INGLES)</p>	<p>From: [redacted] &lt;[redacted]&gt;          To:          Cc:          Subject: Onze vertaaldiensten - Nos services de traduction - Unsere Übersetzungsdienste</p> <p><a href="#">Frans</a> <a href="#">Nederlands</a> <a href="#">Deutsch</a></p> <p>Madame, Monsieur,</p> <p>Nous avons découvert vos activités dans des annuaires professionnels. Nous sommes une entreprise située à Bruxelles et notre activité est centrée sur la traduction.</p> <p>Nous pouvons vous fournir des documents dans plus de 93 couples de langues, avec une garantie de qualité maximale et à des prix très compétitifs.</p> <p>En espérant pouvoir vous y inscrire bientôt, nous vous invitons à consulter la liste de nos clients à l'adresse <a href="http://www.[redacted].fr/references.htm">http://www.[redacted].fr/references.htm</a></p>

## Telefonia

Nel corso del mese oggetto del presente report gli spammer hanno ugualmente provveduto a reclamizzare in maniera particolarmente attiva vari metodi e sistemi appositamente sviluppati per


ridurre i costi della telefonia aziendale. La maggior parte dei messaggi di spam riconducibili a tale tematica è risultata essere rivolta ad imprese e società di considerevoli dimensioni. Nella circostanza, ai destinatari delle e-mail è stato ad esempio proposto di migliorare la qualità delle comunicazioni da telefono fisso, collegare i telefoni aziendali con determinati codici, effettuare chiamate internazionali illimitate, da qualsiasi città, con l'applicazione di tariffe estremamente convenienti.

From: Telephone [redacted]@social-email.biz>  
To:  
Cc:  
Subject: Save up to 60% on your telephone system

From: Telephone [redacted]@lead-mail.biz>  
To:  
Cc:  
Subject: Save up to 60% on your telephone system

**market**  
Compare Telephone Systems

Manage customers and costs more effectively with a telephone system



**Why do I need a Telephone System?**

The importance of a **reliable business telephone system** cannot be underestimated by companies of any shape or size. It is vital to have a telephone system that has all the specific functions your business requires and can cope with the demands your business.

They are central to maintaining both internal communications between colleagues and a providing a consistent external line for customers.

**Advantages of a telephone system within a business**

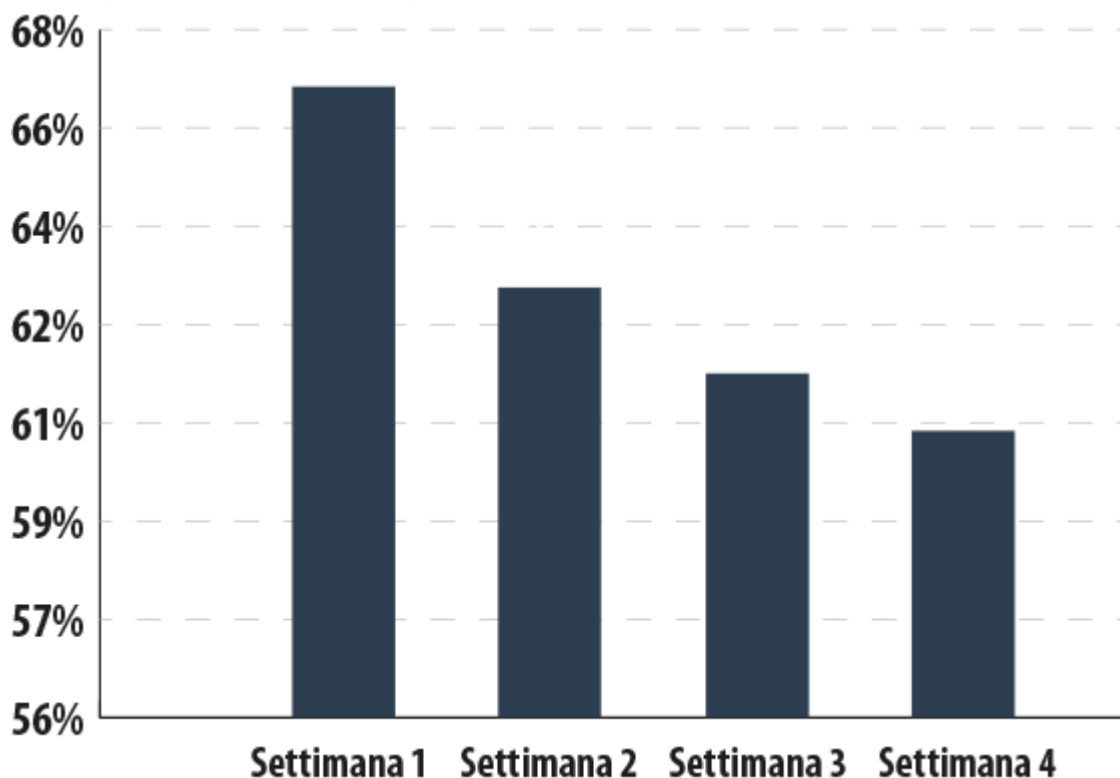
- ✓ Intercom System
- ✓ Unified messaging
- ✓ Wireless IP Capability
- ✓ Video Conferencing

[Compare Prices Now](#)

I messaggi e-mail in questione sono stati principalmente spediti da indirizzi di posta elettronica riconducibili a domini di recente creazione, appositamente allestiti per l'occasione, domini che mutavano di volta in volta. I link inseriti in tali messaggi erano destinati a convogliare l'utente verso un sito web provvisto di un mini-formulario in veste di sondaggio, grazie al quale, previa indicazione di alcuni specifici criteri ed elementi, sarebbe risultato possibile scegliere la soluzione di telefonia più vantaggiosa per la propria impresa. In sostanza, tutto quanto, alla fin fine, sfociava in pagine di pubblicità web appositamente allestite da alcuni fornitori di servizi di telefonia aziendale.

## Le statistiche

### Quota di spam nel traffico di posta elettronica

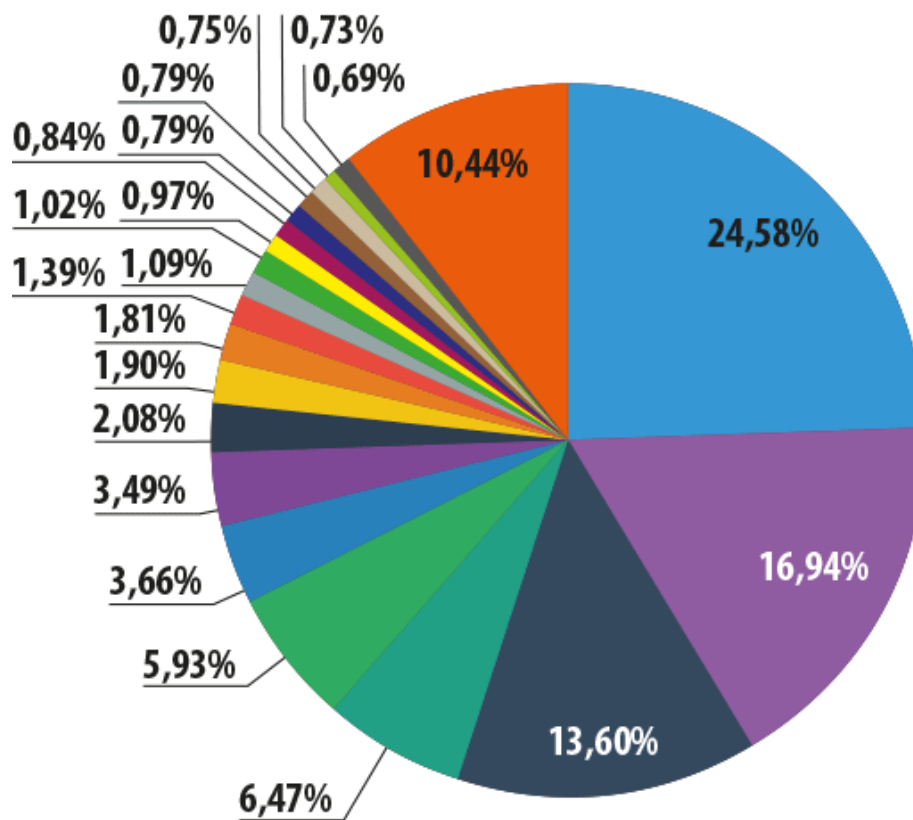


**Quote di spam rilevate settimanalmente all'interno del traffico di posta elettronica**

Nel mese oggetto del presente report, la quota relativa allo spam presente nel traffico di posta elettronica globale ha fatto registrare un valore medio pari al 63,5% del volume complessivo di messaggi e-mail circolanti in Rete. L'indice percentuale più elevato è stato osservato nella prima settimana di marzo (67,3%); in seguito, la quota di spam rilevata all'interno dei flussi e-mail mondiali è progressivamente diminuita.

### Ripartizione geografica delle fonti di spam

La speciale graduatoria "globale" delle fonti di spam - relativa ai paesi dal cui territorio, nel mese di marzo 2014, sono state distribuite in Rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura" - si presenta nella maniera seguente.



- |   |   |
|---|---|
| <span style="color: blue;">■</span> Cina              | <span style="color: gray;">■</span> Gran Bretagna |
| <span style="color: purple;">■</span> USA             | <span style="color: green;">■</span> Bulgaria     |
| <span style="color: darkblue;">■</span> Corea del Sud | <span style="color: yellow;">■</span> Italia      |
| <span style="color: teal;">■</span> Russia            | <span style="color: maroon;">■</span> Polonia     |
| <span style="color: green;">■</span> Taiwan           | <span style="color: darkblue;">■</span> Serbia    |
| <span style="color: blue;">■</span> India             | <span style="color: brown;">■</span> Spagna       |
| <span style="color: purple;">■</span> Vietnam         | <span style="color: tan;">■</span> Kazakistan     |
| <span style="color: darkblue;">■</span> Ucraina       | <span style="color: lightgreen;">■</span> Israele |
| <span style="color: yellow;">■</span> Giappone        | <span style="color: gray;">■</span> Hông Kong     |
| <span style="color: orange;">■</span> Romania         | <span style="color: orange;">■</span> Altri paesi |
| <span style="color: red;">■</span> Filippine          |   |

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

La leadership della classifica analizzata nel presente capitolo del nostro report mensile dedicato al fenomeno spam è andata nuovamente ad appannaggio della Cina (24,6%); la quota ascrivibile al "colosso" dell'Estremo Oriente è aumentata di 1,7 punti percentuali rispetto all'analogo indice rilevato riguardo alla Repubblica Popolare Cinese nello scorso mese di febbraio. Il secondo gradino del "podio" virtuale di marzo 2014 risulta occupato dagli USA: l'indice relativo ai messaggi e-mail indesiderati provenienti dal territorio degli Stati Uniti d'America ha tuttavia presentato un decremento del 2% rispetto al mese precedente; nonostante ciò, gli USA hanno mantenuto la seconda posizione nell'ambito della graduatoria sopra riportata, facendo complessivamente segnare una quota percentuale media pari al 17%. La terza piazza del rating di marzo 2014 risulta occupata - così come nel mese scorso - dalla Corea del Sud (13,6%); la quota ascrivibile ai flussi di spam generati entro i confini del paese asiatico ha fatto registrare un lieve incremento (+ 0,8%) rispetto all'analogo valore riscontrato nel precedente mese di febbraio. Complessivamente, nel periodo analizzato nel presente report, oltre la metà del volume complessivo dei messaggi di posta elettronica "spazzatura" diffusi su scala mondiale è stato inoltrato verso le e-mail box degli utenti dal territorio dei tre suddetti paesi.

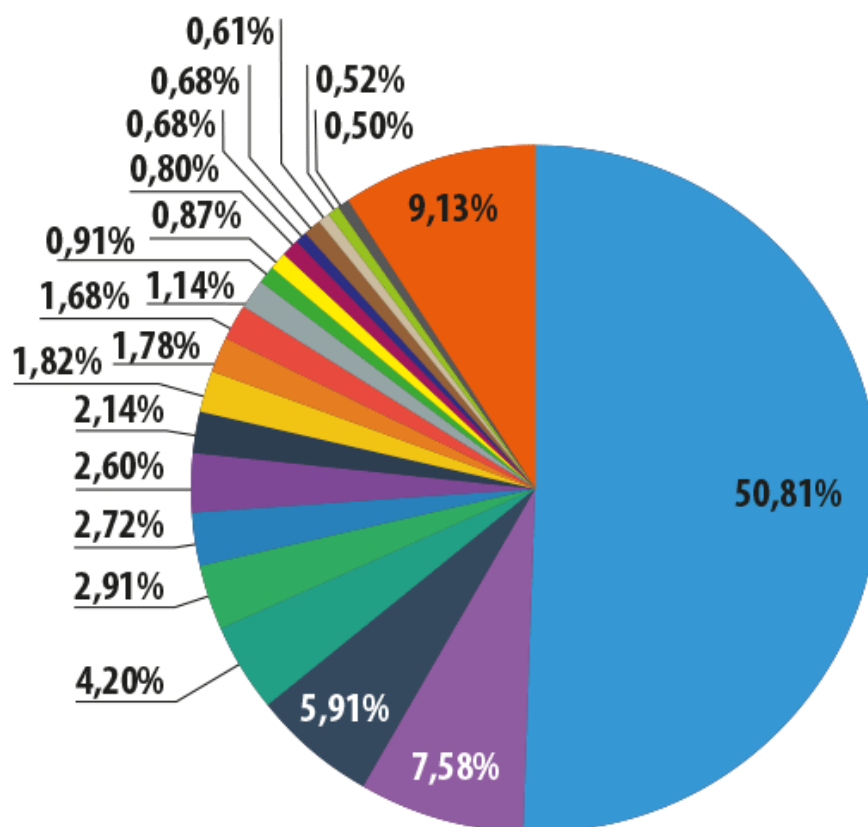
Così come un mese fa, al quarto posto della speciale graduatoria da noi elaborata troviamo la Federazione Russa (6,5%); la quota ad essa riconducibile ha tuttavia evidenziato una leggera diminuzione (- 0,5%) rispetto al mese scorso.

Risultano poi invariate le posizioni occupate in classifica dai seguenti paesi: Taiwan (6%), India (3,7%), Vietnam (3,5%), Ukraina (2%). Nell'arco di un mese gli indici relativi a tali paesi non hanno subito significative variazioni percentuali.

Il Giappone (1,9%), da parte sua, ha visto aumentare la propria quota soltanto dello 0,15%; ciò si è ad ogni caso rivelato sufficiente per "guadagnare" una posizione in graduatoria. Il Paese del Sol Levante è in effetti passato dalla decima alla nona posizione della speciale classifica da noi stilata, relativa alla geografia delle fonti dello spam "mondiale". L'ultima posizione della TOP-10 di marzo 2014 risulta infine occupata dalla Romania (1,8%).

E' di particolare interesse osservare come, nel corso del mese oggetto della nostra analisi, si siano ugualmente intensificate, seppure non in maniera particolarmente marcata, le attività condotte dagli spammer entro i confini del territorio della Gran Bretagna (1%). Rispetto allo scorso mese di febbraio il Regno Unito ha in tal modo "scalato" ben 8 posizioni all'interno del rating qui sopra riportato, andando a collocarsi al dodicesimo posto del ranking.





- |   |   |
|---|---|
| <span style="color: blue;">■</span> Corea del Sud   | <span style="color: gray;">■</span> Malaysia      |
| <span style="color: purple;">■</span> USA           | <span style="color: green;">■</span> Polonia      |
| <span style="color: darkblue;">■</span> Taiwan      | <span style="color: yellow;">■</span> Italia      |
| <span style="color: teal;">■</span> Russia          | <span style="color: maroon;">■</span> Kazakistan  |
| <span style="color: green;">■</span> Cina           | <span style="color: blue;">■</span> Bulgaria      |
| <span style="color: blue;">■</span> Vietnam         | <span style="color: brown;">■</span> Germania     |
| <span style="color: purple;">■</span> India         | <span style="color: tan;">■</span> Spagna         |
| <span style="color: darkblue;">■</span> Hòng Kong   | <span style="color: lightgreen;">■</span> Francia |
| <span style="color: yellow;">■</span> Ucraina       | <span style="color: gray;">■</span> Tailandia     |
| <span style="color: orange;">■</span> Gran Bretagna | <span style="color: orange;">■</span> Altri paesi |
| <span style="color: red;">■</span> Romania          |   |

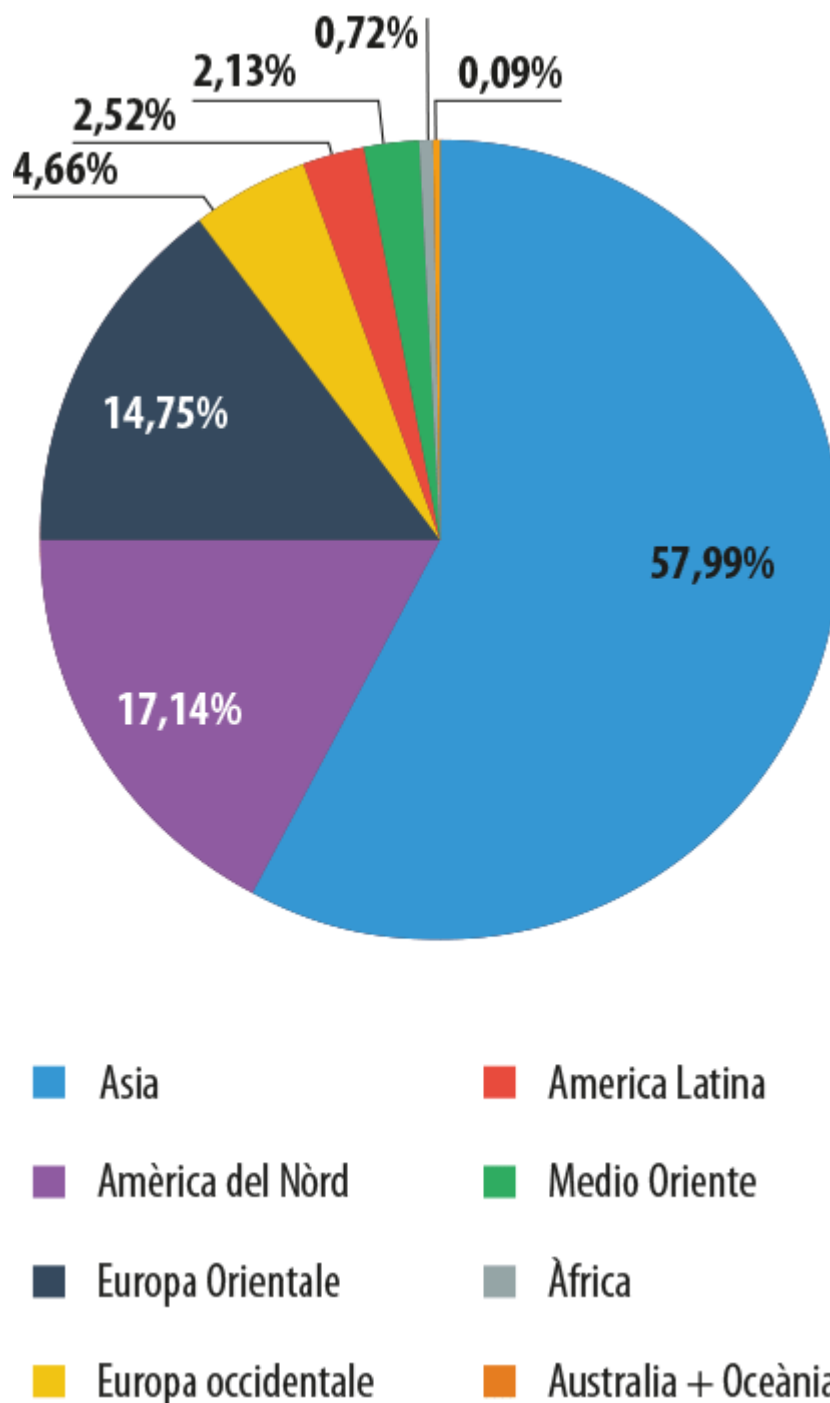
**Geografia delle fonti di spam rilevate nel mese di marzo 2014 relativamente ai messaggi e-mail indesiderati inviati agli utenti della Rete situati sul territorio di paesi europei**

Così come in precedenza, anche nel mese di Marzo 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 della Corea del Sud (50,8%). Rispetto a quanto riscontrato per il mese di febbraio 2014, la quota attribuibile al paese dell'Estremo Oriente ha fatto segnare un ulteriore incremento di 1,2 punti percentuali, attestandosi quindi ancora una volta su un valore complessivo indubbiamente molto elevato. L'indice relativo ai messaggi e-mail indesiderati provenienti dal territorio degli Stati Uniti d'America (7,6%) - e diretti verso gli utenti ubicati in Europa - ha presentato un significativo decremento rispetto al mese precedente, pari all' 1,4%; gli USA hanno tuttavia mantenuto la loro posizione all'interno della speciale classifica "regionale" delle fonti di spam, collocandosi sul secondo gradino del "podio" virtuale di marzo 2014. La terza piazza del rating qui analizzato è andata nuovamente ad appannaggio di Taiwan (6%); la quota ascrivibile ai flussi di spam generati entro i confini del paese situato nell'Estremo Oriente insulare ha fatto registrare un lieve aumento (+ 0,5%) rispetto all'analogo valore riscontrato nel precedente mese di febbraio.

Così come un mese fa, al quarto posto della graduatoria da noi elaborata troviamo la Russia (4,2%), la cui quota risulta diminuita di 0,8 punti percentuali.

Rispetto al rating di febbraio 2014 è stata ugualmente rilevata una significativa diminuzione degli indici relativi a Cina (2,9%), Ukraina (1,8%) e Germania (0,7%), quantificabile, rispettivamente, in un valore pari all' 1%, 0,5% e 0,7%. E' stato poi osservato, allo stesso tempo, un aumento delle quote percentuali inerenti a Vietnam (2,7%), India (2,6%) e Gran Bretagna (1,8%). Proprio il Regno Unito - come evidenzia il grafico qui sopra riportato - chiude la speciale TOP-10 relativa alle fonti dello spam distribuito nelle caselle di posta elettronica degli utenti della Rete ubicati sul continente europeo.

E' infine interessante notare come, nel mese di marzo, si siano intensificati, anche se non in maniera particolarmente marcata, i flussi dello spam "europeo" provenienti da Francia e Thailandia; ciò ha "consentito" a tali paesi di entrare a far parte della graduatoria in questione, con un indice pari - per entrambi - allo 0,5%.

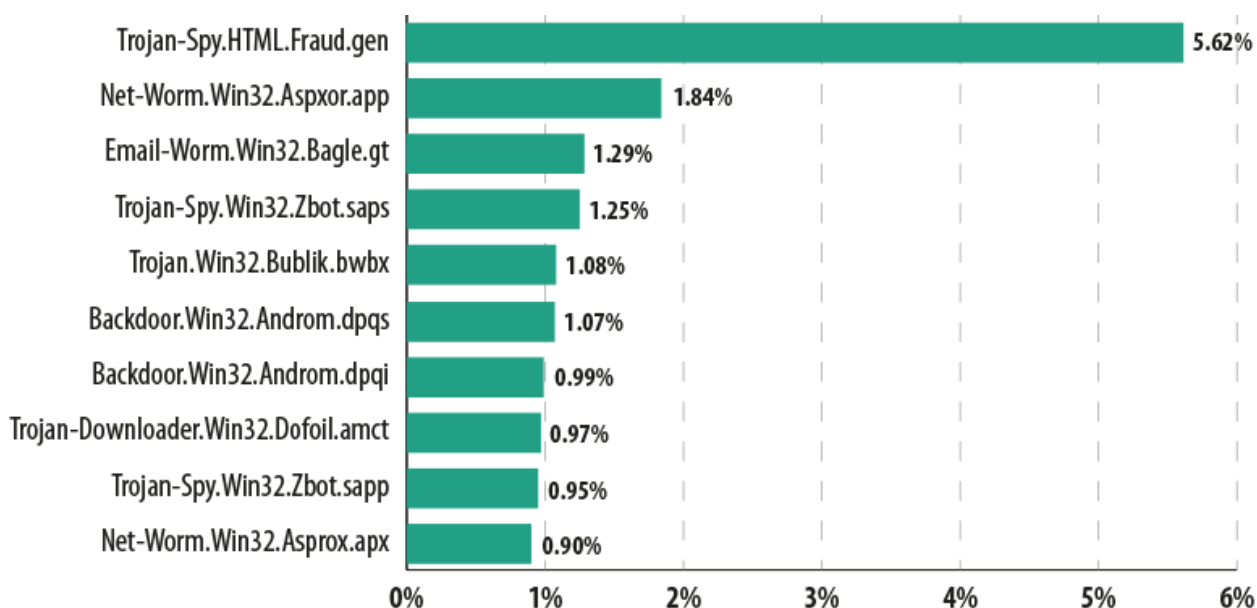


**Suddivisione per macro-regioni geografiche delle fonti di spam rilevate nel mese di marzo 2014**

La graduatoria relativa alla ripartizione delle fonti di spam per macro-regioni geografiche mondiali risulta ancora una volta dominata dall'Asia, con una quota pari al 58%; nel mese di marzo 2014, l'indice complessivamente attribuibile al continente asiatico ha fatto registrare un incremento di ben 4 punti percentuali rispetto all'analogo valore riscontrato nel mese precedente. Così come nel rating dello scorso mese di febbraio, il secondo e il terzo gradino del "podio" virtuale risultano occupati da America Settentrionale (17%) ed Europa Orientale (15%). Gli indici attribuibili a tali macro-aree geografiche hanno tuttavia fatto segnare un decremento pari, rispettivamente, al 2,6% e all' 1,4%. Le quote percentuali riconducibili alle rimanenti regioni del globo sono invece rimaste sostanzialmente invariate rispetto ad un mese fa.

## Allegati nocivi rilevati nel traffico e-mail

La TOP-10 del mese di marzo 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 marzo 2014**

La TOP-10 del mese di marzo 2014 relativa ai software nocivi maggiormente presenti nei flussi di posta elettronica globali risulta capeggiata, così come nel mese precedente, dal malware classificato con la denominazione di Trojan-Spy.HTML.Fraud.gen (5,6%); sottolineiamo, nell'occasione, come la quota attribuibile a tale programma nocivo abbia fatto registrare un aumento di quasi 1,3 punti percentuali rispetto all'analogo indice rilevato in febbraio. Ricordiamo, nella circostanza, come il suddetto 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 World Wide 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.

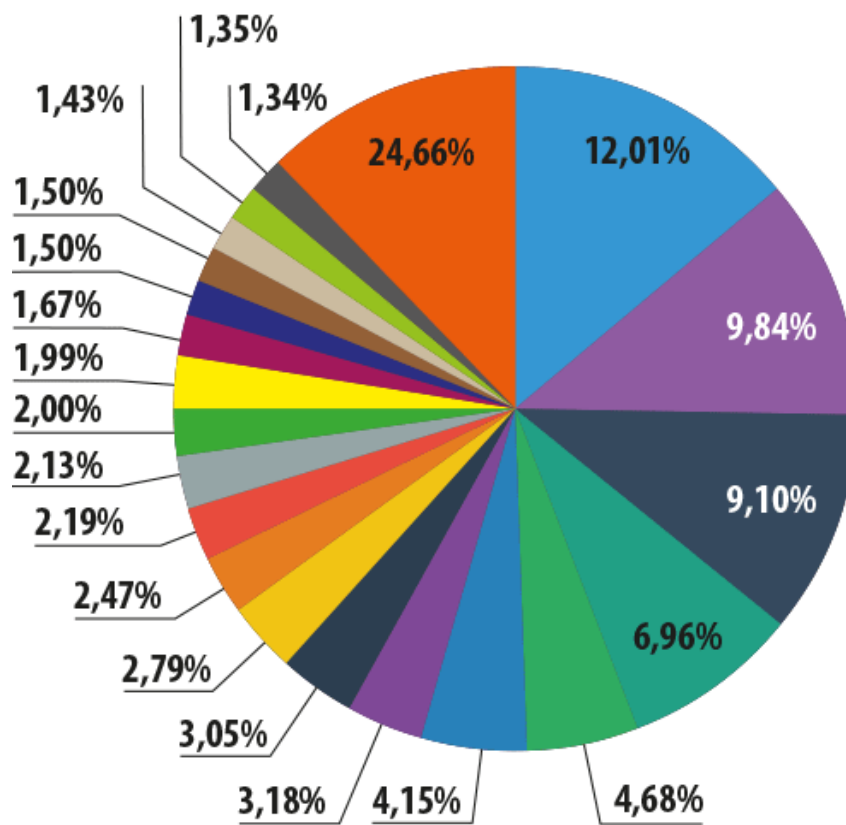
La seconda e la decima posizione della speciale graduatoria da noi stilata risultano occupate da due software nocivi appartenenti ad una famiglia di malware ampiamente nota; si tratta, più precisamente, di due varianti del famigerato worm di rete denominato Asprox, abitualmente preposto all'invio di messaggi di spam. I net-worm in questione sono in grado di infettare automaticamente i siti web presi di mira, effettuare il download ed avviare l'esecuzione di ulteriori software dannosi, 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.

Alla terzo posto del rating si è poi collocato il malware rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Email-Worm.Win32.Bagle.gt. Si tratta, come è noto, di un worm di posta elettronica preposto a raccogliere gli indirizzi e-mail presenti nei computer-vittima contagiati, e più precisamente negli elenchi dei contatti, per poi auto-diffondersi in Rete tramite gli account di posta illecitamente carpiri. Tale programma nocivo risulta inoltre provvisto di ulteriori funzionalità: esso è stato appositamente creato dai virus writer per interagire con specifici siti web allestiti dai cybercriminali, al fine di scaricare dalla Rete ulteriori file dannosi sui computer sottoposti ad attacco, all'insaputa degli utenti-vittima. Per realizzare l'invio dei messaggi infetti, Email-Worm.Win32.Bagle.gt utilizza la propria libreria SMTP.

Il quarto ed il nono posto della graduatoria qui analizzata sono andati ad appannaggio, rispettivamente, delle varianti di malware classificate come Trojan-Spy.Win32.Zbot.saps e Trojan-Spy.Win32.Zbot.sapp. Come è noto, Zbot è un programma Trojan altamente specializzato nel furto delle informazioni confidenziali custodite nei computer degli utenti sottoposti ad attacco. La variante Zbot.saps, in aggiunta alla funzionalità principale abitualmente espletata, provvede ugualmente ad installare sul computer-vittima il malware denominato dagli esperti di sicurezza IT come Rootkit.Win32.Necurs (oppure, in alternativa, Rootkit.Win64.Necurs). Il rootkit in causa, una volta installato con successo sui computer presi di mira, interferisce con il lavoro svolto da vari anti-virus ed altre soluzioni di sicurezza eventualmente presenti sulle macchine sottoposte a contagio informatico.

Al quinto posto della TOP-10 da noi stilata si è insediato un temibile rappresentante della famiglia di malware denominata Bublik. Le principali funzionalità di cui sono provvisti tali programmi dannosi consistono nel download e nella successiva installazione sul computer-vittima di nuove versioni di programmi nocivi, a totale insaputa dell'utente. Una volta portato a termine il proprio compito, i programmi malware riconducibili alla famiglia Bublik non rimangono allo stato attivo, anche se provvedono a realizzare una copia di se stessi all'interno della cartella <%temp%>. Riteniamo infine di particolare utilità sottolineare come i trojan-downloader Bublik siano soliti camuffarsi sotto forma di applicazioni o documenti Adobe.

Il sesto ed il settimo posto della graduatoria in questione risultano occupati dai malware classificati, rispettivamente, come Backdoor.Win32.Androm.dpqs e Backdoor.Win32.Androm.dqpi. 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 dannosi 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.



- USA
- Gran Bretagna
- Germania
- India
- Italia
- Vietnam
- Hòng Kong
- UAEs
- Francia
- Australia
- Malaysia
- Giappòne
- Brasile
- Turchia
- Taiwan
- Russia
- Bàngladesh
- Àustria
- Cina
- Indonèsia
- Altri paesi

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

Il primo posto della classifica qui sopra riportata - riguardante i paesi nei quali, durante il mese di marzo 2014, il nostro modulo antivirus dedicato alla posta elettronica ha eseguito il maggior numero di rilevamenti volti a neutralizzare i programmi malware distribuiti attraverso i flussi e-mail - è andato nuovamente ad appannaggio degli Stati Uniti (- 1,02%). Sul secondo e sul terzo gradino del "podio" virtuale si sono poi collocate, rispettivamente, Gran Bretagna e Germania.

La Russia, da parte sua, è passata dalla dodicesima alla sedicesima posizione della graduatoria qui esaminata; in effetti, la quota relativa ai rilevamenti effettuati sul territorio della Federazione Russa dal modulo antivirus e-mail ha presentato una significativa diminuzione (- 0,82%). Allo stesso modo, risulta sensibilmente diminuita la quota attribuibile all'Australia (- 0,75%); il paese-continente dell'emisfero sud ha così "perso" tre posizioni in classifica, scendendo dalla settima alla decima posizione del rating da noi elaborato. Durante questo mese, gli indici relativi ai rimanenti paesi presenti in graduatoria non hanno subito significative variazioni percentuali.

### **Peculiarità e tratti caratteristici dello spam nocivo di marzo**

Lungo tutto l'arco del mese di marzo 2014, all'interno dei flussi di posta elettronica globali, è stata rilevata la presenza di un consistente numero di allegati dannosi inviati tramite messaggi di spam nocivo camuffati sotto forma di notifiche e comunicazioni provenienti (in apparenza!) da varie organizzazioni operanti nella sfera finanziaria - tutte ampiamente note - la cui attività risulta collegata alla riscossione delle imposte ed ai prelievi fiscali in genere. Più precisamente, le e-mail in questione sono giunte nelle caselle di posta degli utenti mascherate in veste di avvisi di pagamento emessi da autorità fiscali e società incaricate della riscossione dei tributi, sotto forma di richieste di pagamento di imposte di vario genere, oppure camuffate alla stregua di notifiche relative alla mancata dichiarazione dei redditi da parte del contribuente.

Spesso, in tali messaggi, venivano indicati ulteriori dati, quali, ad esempio, l'ID del soggetto di imposta, il genere di imposta per il quale si richiedeva il pagamento (nello screenshot esemplificativo qui sotto riportato, ad esempio, si parla esplicitamente di imposta sul reddito), il numero del documento di riferimento. Altre volte, invece, gli spammer comunicavano al destinatario del messaggio che la dichiarazione dei redditi presentata in precedenza da quest'ultimo si era rivelata falsa.

From: E\*TRADE SECURITIES <etrade\_tax\_mbox@...>  
 To:  
 Cc:  
 Subject: Important Tax Document  
 Message: E-Trade\_Tax\_Form2423057.zip (9 KB)

**E\*TRADE**

**Your Tax Document is Now Available**

Dear Customer,  
 Account number ending in: 0466

A tax document for your E\*TRADE Securities brokerage account shown above is now available online.  
 To view and complete your tax document now, please follow the instructions below. (Adobe Acrobat Reader required.)

Download E-Trade\_Tax\_Form2423057.zip.

---

From: HMRC <no\_reply@...>  
 To:  
 Cc:  
 Subject: HMRC Tax Notice  
 Message: PDF\_Scanned\_HMRC70DD15AAF.zip (71 KB)

The image you are requesting does not exist or is no longer available.  
 Imgur.com

**Dear**

Please be advised that one or more Tax Notices (P6, P6B) have been issued.

For the latest information on your Tax Notices (P6, P6B) please open attached report.  
 Document Reference: 9113268.

The security and confidentiality of your personal information is important for us. If you have any questions, please either call the toll-free customer service  
 2014 © All rights reserved

---

From: HM Revenue and Customs <noreply@...>  
 To:  
 Cc:  
 Subject: Notice of Underreported Income  
 Message: ufwsd-000005060685UK.zip (8 KB)

Taxpayer ID: ufwsd-000005060685UK  
 Tax Type: Income Tax  
 Issue: Unreported/Underreported Income (Fraud Application)

Please review your tax income statement on HM Revenue and Customs ( HMRC )

Please complete the attached form

HM Revenue and Customs

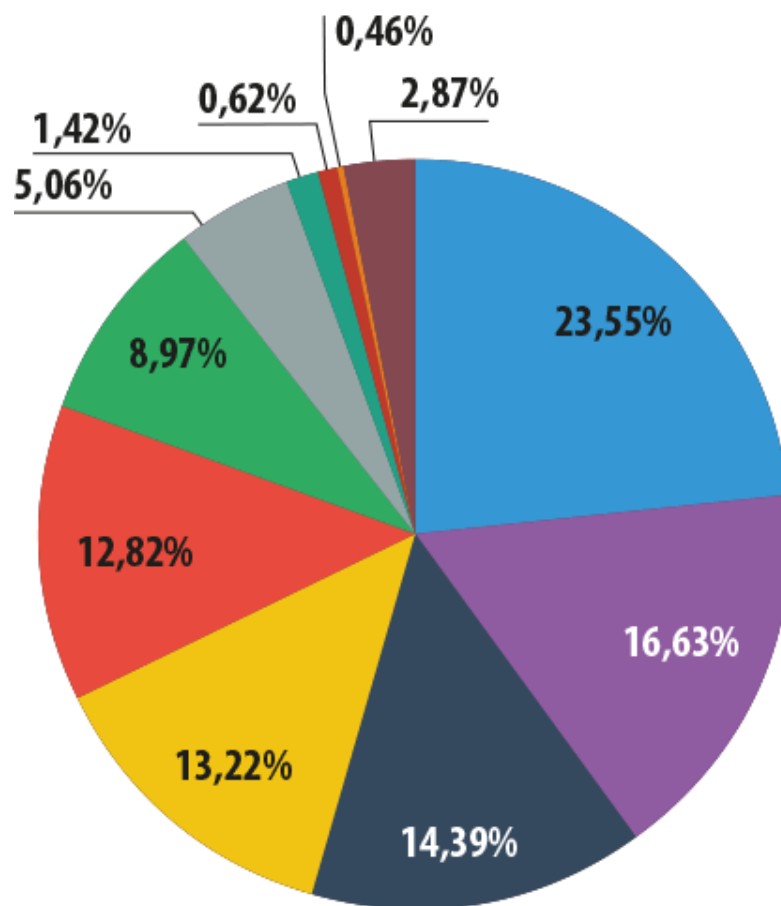
Per venire a conoscenza di tutti i dettagli relativi alla "notifica" ricevuta, il potenziale utente-vittima avrebbe dovuto aprire - su esplicito invito del mittente - il "report" allegato al messaggio nocivo. Spesso, in alternativa, si chiedeva poi al destinatario dell'e-mail di compilare l'apposito form trasmesso in allegato. Ad ogni caso - a detta degli spammer - gli "indispensabili" documenti risultavano sempre custoditi all'interno dell'archivio .zip inoltrato assieme al messaggio; in realtà, il file compresso in questione non conteneva affatto tali documenti, bensì un file eseguibile di natura nocivo.

Sono stati ad esempio da noi individuati, in qualità di allegati a messaggi e-mail del genere, due temibili programmi Trojan, rilevati dalle soluzioni anti-malware di Kaspersky Lab come Trojan-PSW.Win32.Fareit.aooe e Trojan.Win32.Bublik.buya. I software nocivi riconducibili alla prima delle due famiglie qui menzionate risultano abitualmente preposti al furto dei cookie presenti nei browser web e, allo stesso tempo, delle password utilizzate nell'ambito dei client FTP e dei programmi di posta elettronica; i dati confidenziali sottratti agli utenti-vittima vengono in seguito inoltrati al server nocivo remoto allestito dai malintenzionati. Le principali funzionalità di cui sono invece provvisti i programmi dannosi appartenenti a Bublik, la seconda famiglia di malware sopra citata, consistono nel download e nella successiva installazione sul computer-vittima di nuove versioni di software dannosi, a totale insaputa degli utenti di volta in volta sottoposti ad attacco informatico.



## Phishing

Così come nello scorso mese di febbraio, al primo posto della speciale graduatoria relativa alle organizzazioni (suddivise per categorie) rimaste vittima con maggior frequenza degli assalti portati dai phisher, troviamo i social network, con una quota pari al 23,5%; l'indice percentuale ascrivibile agli attacchi di phishing condotti nei confronti delle reti sociali ha tuttavia fatto registrare un significativo decremento rispetto ad un mese fa, quantificabile in 3,8 punti percentuali. Come evidenzia il grafico qui sotto riportato, il secondo posto del rating di marzo 2014 è andato ad appannaggio dei servizi di posta elettronica (16,6%); rispetto all'analoga graduatoria di febbraio, la quota relativa a tale categoria risulta diminuita di quasi tre punti percentuali. Nonostante ciò, il raggruppamento "Posta elettronica, programmi di instant messaging" continua a mantenersi saldamente al secondo posto della classifica dedicata al phishing da noi stilata. La categoria che raggruppa i motori di ricerca è tornata ad occupare il terzo posto della graduatoria (14,4%); rispetto ad un mese fa, l'indice attribuibile ai search engine ha tuttavia manifestato una pronunciata flessione (-2%). Nell'arco di un mese è sensibilmente diminuita anche la quota ascrivibile agli attacchi di phishing condotti a scapito della categoria che riunisce le organizzazioni finanziarie, i sistemi di pagamento online e gli istituti bancari (-3,5%); il raggruppamento in questione è in tal modo sceso al quarto posto del rating, perdendo di fatto una posizione rispetto al mese precedente. L'indice relativo ai negozi Internet ed alle aste online ha invece fatto registrare un forte aumento, pari a 8,9 punti percentuali; tale categoria ha pertanto "guadagnato" ben due posizioni in classifica rispetto allo scorso mese di febbraio, collocandosi in tal modo al quinto posto del rating qui analizzato. Risulta infine lievemente aumentata la quota percentuale riconducibile alla categoria "Fornitori di servizi di telefonia ed Internet provider"; nonostante ciò, tale raggruppamento è sceso al sesto posto della graduatoria, "perdendo" una posizione rispetto all'analogo rating di febbraio 2014.



- Social network
- Posta elettronica, messaggistica istantanea
- Motori di ricerca
- Banche e società finanziarie
- Negozi online, aste su internet
- Fornitori di servizi di telefonia ed Internet provider
- Vendor IT
- Media
- Giochi online
- Organizzazioni governative
- Altro

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

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

Le banche tedesche sono spesso uno dei bersagli preferiti dai phisher. Nel mese di marzo, all'interno dei flussi di spam, abbiamo in effetti individuato la conduzione dell'ennesima campagna fraudolenta di phishing volta a realizzare il furto dei dati sensibili di natura finanziaria appartenenti agli utenti del sistema di banking online allestito da un noto istituto bancario tedesco. Attraverso tali messaggi nocivi, inviati a nome di un sedicente funzionario della banca presa di mira dai phisher, si comunicava al destinatario dell'e-mail che il termine previsto per l'accesso online all'account di Internet banking aperto da quest'ultimo sarebbe scaduto entro breve. Per continuare ad usufruire dei servizi di banking online erogati dall'istituto bancario in questione, il potenziale utente-vittima avrebbe dovuto quindi convalidare il proprio account, cliccando sul link appositamente inserito nel messaggio; in realtà, tale collegamento ipertestuale avrebbe condotto l'ignaro utente verso un'insidiosa pagina di phishing, allestita per l'occasione dai malfattori. Una volta giunto su tale pagina web nociva, il destinatario del messaggio truffaldino avrebbe dovuto inserire non soltanto i dati confidenziali abitualmente utilizzati per accedere al sistema di banking online, ma anche informazioni di natura strettamente personale e riservata.

Come evidenzia lo screenshot qui sotto riportato, nella circostanza, la pagina contraffatta predisposta dai malintenzionati era stata realizzata in maniera decisamente accurata, e riusciva ad imitare piuttosto fedelmente la pagina web ufficiale presente all'interno del sito web della suddetta banca tedesca. L'e-mail di phishing, invece - come si può vedere - non presentava, di per se stessa, alcuna veste grafica (il logo della banca, ad esempio), né i consueti elementi di cui abitualmente si avvalgono i malintenzionati per conferire ai propri messaggi di posta elettronica un aspetto di legittimità ed autenticità (i phisher provvedono spesso, ad esempio, ad inserire una firma automatica in calce all'e-mail). E' interessante ad ogni caso rilevare come, nel campo riservato all'indirizzo del mittente, il nome di dominio del server - indicato dopo il carattere "@" - appartenesse, di fatto, al Consiglio Nazionale delle Ricerche del Canada (NRC - National Research Council Canada), istituzione ovviamente non collegata in alcun modo con l'organizzazione bancaria oggetto delle losche attenzioni dei phisher.

From: Porstner Scheuka, Allen <Allen.PorstnerScheuka@nrc-cnrc.gc.ca>  
To:  
Cc:  
Subject: Sparkasse Online-Banking

Sent: Fr 11.03.2014 14:14

Sehr geehrter Kunde,

Bitte beachten Sie, dass Ihr Online-Zugriff auf Ihr Konto in Kürze abläuft. Damit dieser Dienst ohne Unterbrechung fortzusetzen, klicken Sie auf das Symbol unten, um Ihr Konto manuell zu aktualisieren, neu zu validieren Ihrem Konto [HIER KLICKEN](#)

Nachdem Sie die Anweisungen, um Ihr Konto zu aktualisieren, wird Ihr Online-Zugang zu Ihrem Konto automatisch wiederhergestellt werden und keine weitere Aktion wird von Ihnen verlangt werden. Sie haben einen ausreichenden Kontakt mit dem Konto Abteilung für weitere Informationen über den Status Ihres Kontos.

Mit Online-Banking haben Sie alles im Griff mit einem Klick.

Die bequeme Online-Banking haben Sie einen schnellen und einfachen Zugang zu Ihrem Girokonto. Wenn Sie Online-Banking Überweisungen und Daueraufträge durch Mausclick tun. Aber Online-Banking bietet viel mehr

Die Vorteile von Online BANKING AUF EINEN BLICK:

- Ø Kontozugang rund um die Uhr
- Ø Schneller Zugriff auf das Girokonto
- Ø Online-Banking bequem von Ihrem PC
- Ø Flexibel in jeder Ecke der Welt
- Klar Ø Rechnungswesen
- Ø Hohe Sicherheitsstandards beim Online-Banking
- Ø Online-Banking in Kombination mit Telefon-Banking

Wir möchten Ihnen im Voraus danken für Ihre Mitarbeit  
Mit freundlichen Grüßen,  
Porstner Scheuka, Allen  
Customer Service Officer.  
Sparkasse Online-Banking  
Urheberrecht 2014 Sparkasse Online-Banking

Wie viel Sparpotenzial steckt in Ihrem Eigenheim?  
Jetzt Kosten senken

Online-Banking: Anmelden

Anmeldename oder E-Mailadresse

PIN

Mit dem Absenden Ihrer Anmeldeinformationen Sie die [Sicherheitshinweise](#) an

Vorname

Name

Straße

Haus Nr.

PLZ

Postleitzahl

Wohnort

Geburtsdatum

Telefon

Handy

Anmelden

## Conclusioni

Nel periodo oggetto del presente report, la quota relativa allo spam individuato nel traffico di posta elettronica globale ha fatto registrare un decremento del 6,4% rispetto allo scorso mese di febbraio, attestandosi in tal modo su un valore medio pari al 63,5% del volume complessivo di messaggi e-mail circolanti in Rete. Rispetto a quanto riscontrato nel mese precedente, risulta ugualmente diminuito, all'interno dei flussi e-mail, il numero totale dei messaggi indesiderati riconducibili al cosiddetto spam "festivo", ovvero lo spam ispirato alle tradizionali tematiche suggerite dalle più importanti ricorrenze e celebrazioni stagionali. Mentre gli spammer hanno sfruttato il rapido approssimarsi delle festività pasquali per confezionare le classiche e-mail volte a pubblicizzare prodotti di ogni genere ed una vasta gamma di articoli da regalo, il Giorno di San Patrizio - l'importante ricorrenza celebrata il 17 marzo di ogni anno in numerosi paesi del mondo - è stato invece "utilizzato" da certi malintenzionati della Rete per cercare di ottenere l'accesso agli account degli utenti di LinkedIn, il celebre social network professionale.

Inoltre, nel mese di marzo 2014, le caselle di posta elettronica degli utenti del World Wide Web sono state letteralmente invase da un'enorme quantità di proposte pubblicitarie riguardanti l'apprendimento delle lingue straniere mediante l'utilizzo dei metodi più disparati e delle tecniche più singolari ed originali. Nel corso del periodo esaminato nel nostro consueto report mensile sull'evoluzione del fenomeno spam, è stata ugualmente rilevata la conduzione di numerosi mailing di massa contenenti informazioni relative a determinati metodi da adottare per l'ottimizzazione della gestione delle comunicazioni telefoniche nell'ambito di aziende di grandi e medie dimensioni.

Le prime tre posizioni della speciale graduatoria di marzo 2014 relativa alle fonti dello spam "globale" - riguardante i paesi dal cui territorio sono state distribuite in Rete, verso tutti e cinque i continenti, le maggiori quantità di e-mail "spazzatura" - sono rimaste invariate rispetto all'analogo rating del mese precedente. Il "podio" virtuale in questione risulta pertanto composto dalle seguenti nazioni: Cina (24,6%), Stati Uniti (17%) e Corea del Sud (13,6%). Il ranking relativo alla ripartizione delle fonti di spam

per macro-regioni geografiche mondiali evidenzia ancora una volta un netto dominio da parte dell'Asia, la cui quota si è attestata su un valore complessivo pari al 58%.

Per realizzare l'invio delle abituali e-mail contenenti allegati dannosi, i cybercriminali hanno fatto ampiamente ricorso all'utilizzo di messaggi di spam nocivo camuffati sotto forma di notifiche e comunicazioni provenienti (in apparenza!) non solo da noti istituti bancari, ma anche da varie altre organizzazioni operanti nella sfera finanziaria, quali, ad esempio, le società la cui attività risulta collegata al calcolo ed alla riscossione di imposte di vario genere.

Così come negli ultimi mesi, la speciale classifica relativa alle organizzazioni rimaste vittima con maggior frequenza degli assalti portati dai phisher continua ad essere capeggiata dalla categoria "Social network". Il secondo posto del rating in questione è andato nuovamente ad appannaggio dei servizi di posta elettronica, mentre sul terzo gradino del "podio" di marzo si è collocata la categoria che raggruppa i motori di ricerca. Risulta infine sensibilmente aumentato l'indice percentuale attribuibile ai negozi online, passati dal settimo al quinto posto della speciale graduatoria del phishing da noi stilata.