Lo spam nel mese di Giugno 2014

Tat'jana Šerbakova

Marija Vergelis

Le peculiarità del mese 1
Il Campionato del Mondo di calcio 2
Spam e festività 3
L'Ukraina al centro dello spam «nigeriano» 4
Il dating online 5
Gioielli 7
Carte carburante 8
Le statistiche 9
Quota di spam nel traffico di posta elettronica 9
Ripartizione geografica delle fonti di spam 9
Allegati maligni rilevati nel traffico e-mail 11
Peculiarità e tratti caratteristici dello spam nocivo di giugno 14
Phishing 16
Conclusioni 18

Le peculiarità del mese

Nel corso del periodo oggetto del nostro consueto report mensile dedicato al sempre persistente fenomeno della diffusione dei cosiddetti messaggi "spazzatura" all'interno dei flussi e-mail globali, gli spammer hanno attivamente sfruttato alcuni tra i più eclatanti avvenimenti che si sono prodotti sulla scena mondiale, quali il Campionato del Mondo di calcio e la complessa situazione socio-politica attraversata dall'Ukraina, con il preciso intento di cercare di raggirare il maggior numero possibile di utenti Internet mediante la diffusione di messaggi e-mail fraudolenti, volti a carpire le informazioni sensibili legate alla sfera finanziaria delle potenziali vittime, e quindi sottrarre cospicue somme di denaro alle stesse.

Nell'immediata vigilia della festività musulmana del Ramadan, solennemente osservata in tutto il mondo islamico - e della Festa del Papà, ricorrenza tradizionalmente celebrata negli Stati Uniti alla metà del mese di giugno, nel vasto segmento anglofono dello spam ispirato alle principali tematiche suggerite dalle festività stagionali del momento, è stato dato ampio spazio ai messaggi appositamente allestiti per offrire prodotti e servizi strettamente "a tema". Inoltre, nell'ambito delle categorie tematiche che hanno maggiormente contraddistinto il panorama dello spam durante il mese di giugno 2014, hanno avuto

particolare rilievo le e-mail indesiderate preposte a pubblicizzare vari servizi di incontri online, al pari dei messaggi contenenti offerte di acquisto di carte carburante ed articoli di gioielleria.

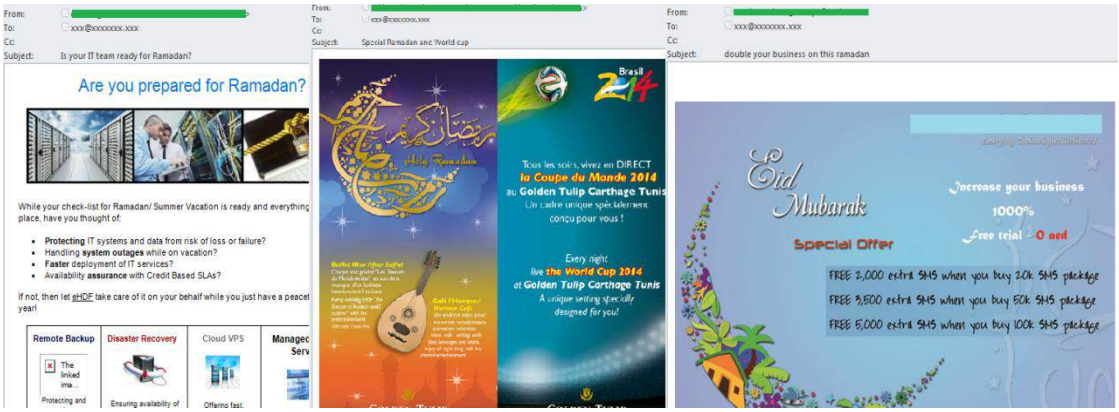
Il Campionato del Mondo di calcio

Nel mese di giugno ha avuto inizio la ventesima edizione della Coppa del Mondo FIFA; gli appassionati e i tifosi di ogni angolo del globo attendevano già impazientemente, da tempo, lo svolgimento della vera e propria festa planetaria del football. E' ampiamente noto, ormai, come gli avvenimenti sportivi che godono di maggior popolarità - dei quali fa indubbiamente parte il Mundial - attirino non soltanto l'attenzione di milioni e milioni di telespettatori in tutto il mondo, ma anche quella di spammer e phisher. A dir la verità, le prime campagne di spam di natura fraudolenta, volte a sfruttare le numerose tematiche connesse al Campionato del Mondo 2014, organizzato in Brasile, erano state individuate dai nostri esperti, all'interno del traffico di posta elettronica, già nello scorso mese di novembre, con larghissimo anticipo rispetto alla data prevista per il calcio d'inizio della prestigiosa manifestazione calcistica (lo scorso 12 giugno). Lungo tutto l'arco del mese qui analizzato, poi, i malintenzionati dello spam hanno provveduto ad inondare le e-mail box degli utenti della Rete di messaggi e-mail di phishing elaborati in lingua portoghese, contenenti proposte alquanto allettanti, come la possibilità di prendere parte ad una interessante lotteria, grazie alla quale si sarebbero potuti vincere biglietti per partecipare alla spettacolare cerimonia di apertura della Coppa del Mondo Brasil 2014, così come ambiti tagliandi per assistere a varie partite di calcio previste nel ricco programma dell'evento planetario. Per far ciò, il destinatario dell'insidiosa e-mail di phishing avrebbe dovuto cliccare sul link fraudolento subdolamente inserito dai truffatori nel corpo del messaggio, per poi introdurre i dati personali di registrazione e, soprattutto, tutte le informazioni sensibili relative alla propria carta di credito. Nella circostanza, il collegamento ipertestuale fasullo era stato posizionato dai phisher direttamente sul file grafico che avrebbe visualizzato il potenziale utente-vittima una volta aperto il messaggio di posta ricevuto. Le relative pagine web adibite al phishing erano state collocate all'interno del dominio gratuito provvisto di estensione .tk, ovvero il dominio nazionale di primo livello che identifica le remote isole Tokelau, situate nell'Oceano Pacifico del Sud e facenti parte del territorio amministrativo della Nuova Zelanda. Nel tentativo di convincere l'utente-vittima riguardo all'autenticità del messaggio e-mail in questione, gli spammer avevano appositamente inserito nel campo riservato all'indirizzo del mittente l'esplicito riferimento a domini riconducibili sia al sistema di pagamento Visa, sia alla FIFA, la Federazione Internazionale del football.

Spam e festività

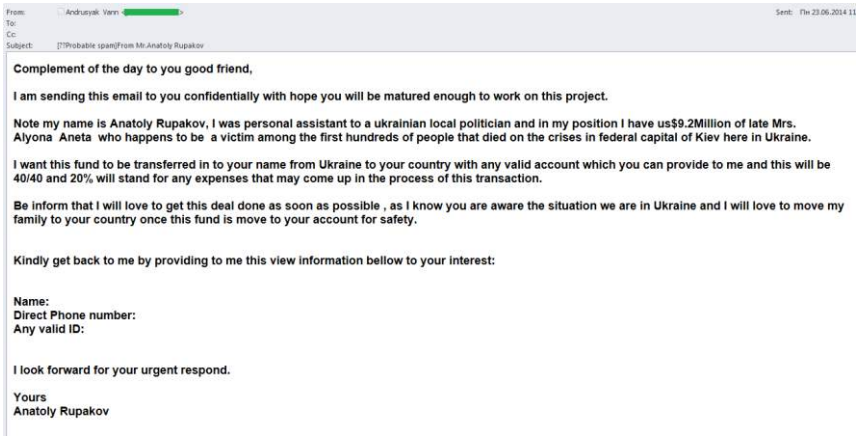
Nel mese oggetto del presente report, il cosiddetto spam "festivo" elaborato in lingua inglese è stato principalmente dedicato alla Festa del Papà, ricorrenza celebrata, negli Stati Uniti, in occasione della terza domenica di giugno. Nella circostanza, gli spammer hanno distribuito in Rete messaggi pubblicitari volti a promuovere la vendita di gadget elettronici, repliche di articoli di lusso riconducibili a prestigiosi marchi internazionali e riproduzioni di armi risalenti a varie epoche, cercando di attirare al massimo l'attenzione dei destinatari delle e-mail in causa con la promessa di sostanziosi sconti, saldi o, perlomeno, prezzi particolarmente contenuti. Per cercare di eludere l'azione di controllo svolta dai filtri antispam, gli spammer hanno inserito nella parte finale di tali messaggi una consistente porzione di testo, spesso ricavato da qualche opera letteraria, con il preciso intento di "imbrattare" l'e-mail e celarne quindi il reale contenuto pubblicitario. Al tempo stesso, gli autori dei messaggi di posta indesiderati si sono avvalsi di un popolare servizio online per la creazione di URL brevi, al fine di camuffare l'effettivo indirizzo presente nel collegamento ipertestuale e redirigere quindi gli utenti, in maniera agevole, verso il sito web appositamente allestito dagli spammer. Come si può vedere negli screenshot esemplificativi qui sotto riportati, sia nell'oggetto che nel corpo del messaggio è stato poi inserito, a più riprese, il nome della popolare e sentita festività di giugno.

Nell'ambito dello spam mondiale, le festività religiose non vengono sfruttate in maniera così ampia ed insistita come invece generalmente avviene per le feste di natura laica o civile. Ad ogni caso, sembra proprio che gli spammer non si dimentichino mai, in alcun caso, di far sì che i destinatari dei messaggi e-mail ricevano sempre offerte commerciali e pubblicitarie strettamente "a tema". E' ormai noto come, ogni anno, nel traffico di posta elettronica globale si incontrino numerosi messaggi di spam ispirati alla festività musulmana del Ramadan, il mese sacro celebrato in tutto il mondo islamico. L'anno 2014 non ha di certo rappresentato un'eccezione a quanto sopra affermato: così, nel traffico e-mail di giugno, abbiamo individuato vari messaggi di spam in cui si menzionava esplicitamente il Ramadan, volti a pubblicizzare particolari ristoranti (è singolare come, nella circostanza, sia stato abbinato anche l'invito a recarsi nel locale per assistere, allo stesso tempo, alla trasmissione televisiva degli attesi match della Coppa del Mondo di calcio). Sono stati inoltre rilevati, all'interno dei flussi e-mail di giugno, messaggi di posta in cui si proponevano vari servizi legati al mondo dell'informatica, così come appositi servizi preposti all'invio di SMS pubblicitari. Il mese sacro del Ramadan si protrarrà sino alla fine di luglio; è pertanto lecito attendersi che gli spammer continuino ad inviare nelle e-mail box degli utenti della Rete un considerevole numero di messaggi di spam volti a "sfruttare" le tematiche connesse all'importante festività islamica.



L'Ukraina al centro dello spam «nigeriano»

Nel corso del periodo qui analizzato, i delicati e complessi avvenimenti politici che hanno scosso l'Ukraina sono stati nuovamente utilizzati dai cosiddetti truffatori "nigeriani" con il preciso scopo di sottrarre significative somme di denaro a potenziali utenti-vittima, inesperti o particolarmente fiduciosi. Stavolta, l'autore dell'e-mail "nigeriana" ha assunto le vesti di un sedicente collaboratore di una personalità politica femminile dell'Ukraina, tra le prime vittime degli scontri a fuoco recentemente avvenuti nella città di Kiev. Ovviamente, come spesso recita il "genere letterario" in questione, la persona defunta ha lasciato a completa disposizione del proprio assistente un'ingente somma di denaro, pari a svariati milioni di dollari, i quali, tuttavia, vista la forte instabilità che regna a livello locale, debbono essere rapidamente trasferiti dall'Ukraina verso il conto bancario estero che il destinatario dell'e-mail dovrebbe "gentilmente" mettere a disposizione. Come ricompensa per l'aiuto prestato nell'occasione, nel concedere l'accesso al proprio conto personale, fornendone il relativo numero, i truffatori non esitano a promettere alla potenziale "vittima" del raggiro una lauta somma di denaro, e si dimostrano addirittura pronti a destinare un determinato importo a copertura di tutte le spese che inevitabilmente deriveranno dall'operazione di trasferimento dell'ingente capitale.



Complement of the day to you good friend,

I am sending this email to you confidentially with hope you will be matured enough to work on this project.

Note my name is Anatoly Rupakov, I was personal assistant to a ukrainian local politician and in my position I have us$9.2Million of late Mrs. Alyona Aneta who happens to be a victim among the first hundreds of people that died on the crises in federal capital of Kiev here in Ukraine.

I want this fund to be transferred in to your name from Ukraine to your country with any valid account which you can provide to me and this will be 40/40 and 20% will stand for any expenses that may come up in the process of this transaction.

Be inform that I will love to get this deal done as soon as possible , as I know you are aware the situation we are in Ukraine and I will love to move my family to your country once this fund is move to your account for safety.

Kindly get back to me by providing to me this view information bellow to your interest:

Name:
Direct Phone number:
Any valid ID:

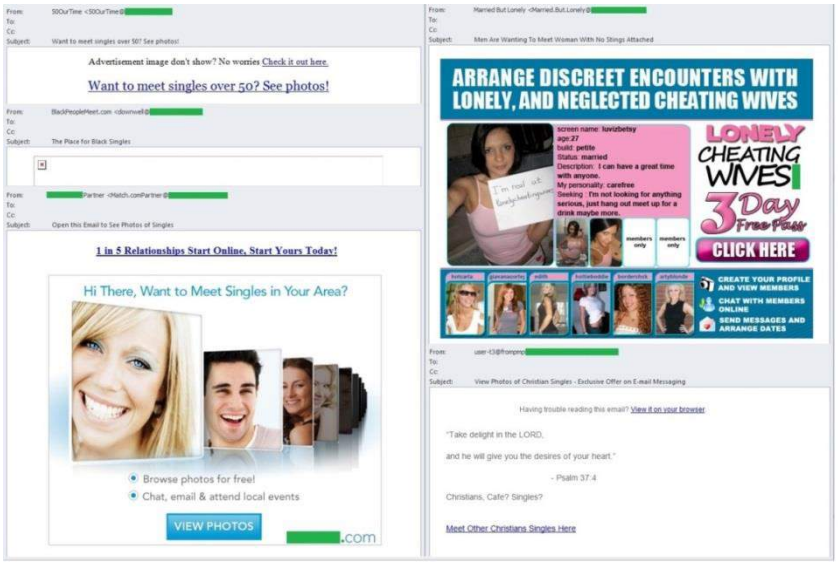
I look forward for your urgent respond.

Yours
Anatoly Rupakov

Questo stesso identico schema di truffa "nigeriana" viene costantemente utilizzato, anno dopo anno, nell'ambito dello spam fraudolento della Rete; ciò che cambia, di volta in volta, sono esclusivamente le "storie" raccontate ed i loro protagonisti; desideriamo, con l'occasione, ricordare nuovamente, a tutti gli utenti, come tali mirabolanti promesse di facile arricchimento non siano, di fatto, null'altro che un subdolo metodo adottato da truffatori senza scrupoli per cercare di sottrarre illecitamente denaro.

Il dating online

Una significativa parte dello spam di giugno è risultata composta da messaggi e-mail indesiderati volti a reclamizzare vari servizi di incontri online, orientati a gruppi sociali ben diversi tra loro: gli spammer, ad esempio, hanno pubblicizzato l'auspicata frequentazione, da parte degli utenti del web, di siti di dating online riservati a persone di colore, musulmani, cristiani, oppure a persone anziane o sposate.



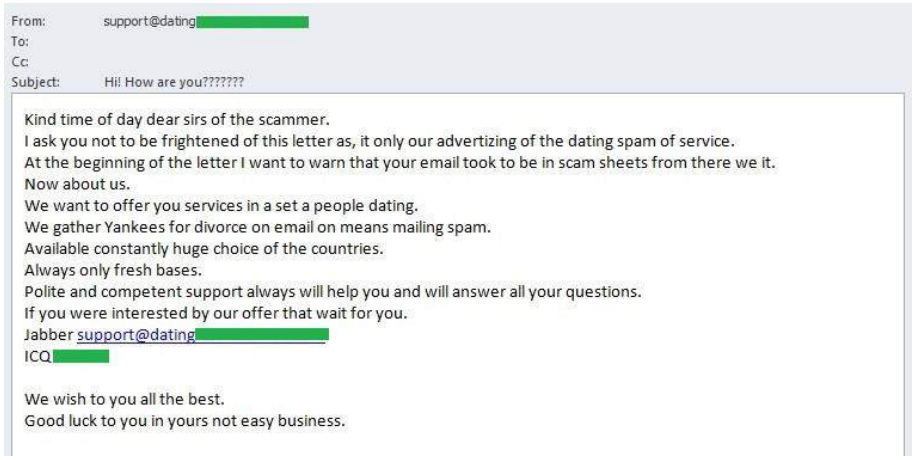
Ci siamo ugualmente imbattuti in vari mailing di massa e conseguenti messaggi di posta inviati a nome di persone desiderose di effettuare nuove conoscenze in Internet "per stabilire relazioni veramente serie o creare una famiglia". Tra l'altro, attraverso tale genere di e-mail di spam, si prospettava ugualmente la possibilità di trovare un partner non soltanto per intessere una relazione di stampo tradizionale, ma anche omosessuale. In genere, i mittenti dei messaggi in questione si premuravano di allegare la propria fotografia all'e-mail, indicando inoltre l'indirizzo di posta elettronica personale, oppure il link per condurre alla propria pagina web, situata all'interno di qualche servizio online riservato al dating (tale schema è stato ugualmente utilizzato, piuttosto di frequente, come forma di pubblicità più o meno

velata in favore del sito di incontri che si intendeva via via reclamizzare; nella circostanza, gli stessi messaggi di posta risultavano in pratica inviati a nome di utenti del tutto immaginari, alla stregua di una vera e propria allettante esca). Nel testo del messaggio, il mittente descriveva il proprio aspetto esteriore, elencava i propri hobby ed interessi, sottolineando come desiderasse intraprendere quanto prima una duratura e sincera corrispondenza. Spesso, nelle e-mail in causa, si indicava esplicitamente come il nome di contatto del destinatario fosse stato ottenuto grazie a qualche amico comune, oppure fosse stato reperito in uno dei tanti social network esistenti o in un altro sito di incontri online; ovviamente, tutto ciò non sarebbe poi risultato necessariamente vero.

Lungo tutto l'arco del mese di giugno gli spammer hanno ugualmente distribuito in Rete messaggi di spam tramite i quali si prometteva, grazie all'utilizzo di un ampio "database di anime gemelle" da essi posseduto, di poter fornire all'utente l'opportunità di formare una coppia perfetta, grazie all'applicazione di vari criteri e parametri (età, colore della pelle, interessi, etc.), e tutto questo in soli tre minuti. Per poter usufruire del servizio di matching, il destinatario del messaggio indesiderato avrebbe dovuto semplicemente indirizzare un SMS verso il numero a pagamento indicato nell'e-mail appena ricevuta. Nella circostanza, in aggiunta al denaro sottratto dall'account telefonico mobile del richiedente, gli spammer avrebbero ugualmente ottenuto l'accesso alle informazioni di contatto custodite nello smartphone di quest'ultimo, ed in particolar modo ad ulteriori numeri telefonici registrati in rubrica.

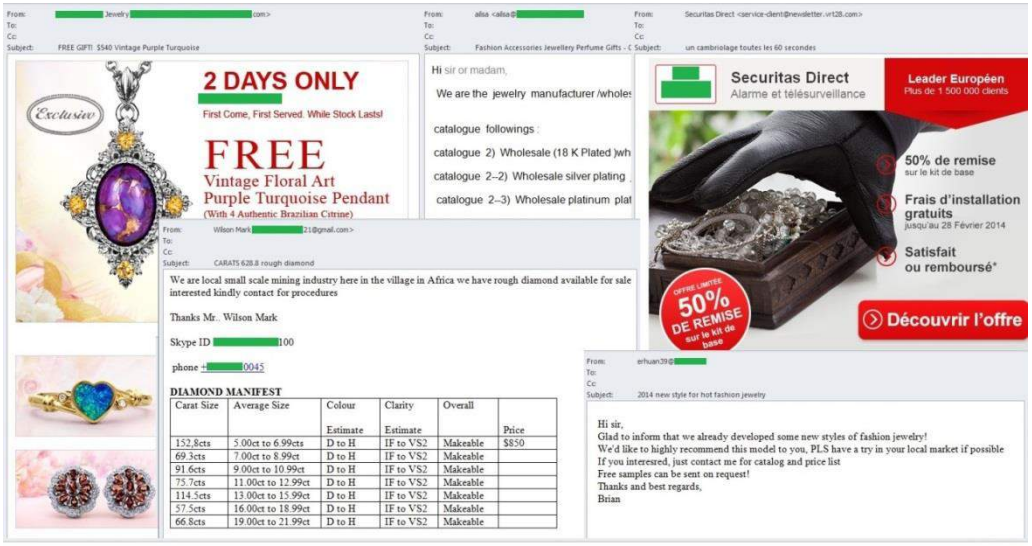
Inoltre, per coloro che non hanno particolare dimestichezza con i servizi di dating online e continuano tuttora a prediligere gli incontri "reali", gli spammer hanno proposto specifiche lezioni di seduzione delle potenziali partner femminili ("24 regole per attrarre le donne"), così come ulteriori consigli per instaurare rapporti amorosi di successo.

In uno dei mailing di massa da noi intercettati nel corso del mese di giugno 2014 abbiamo infine individuato la pubblicità di un singolare servizio di spam dating. Con l'occasione, gli spammer hanno proposto appositi servizi per la creazione e la promozione (tramite campagne di spam, ovviamente) di un nuovo sito di incontri online, con l'allettante promessa di poter attirare un vasto numero di utenti, ubicati in un gran numero di paesi. Quali informazioni di contatto, erano stati inseriti, in tali messaggi, un indirizzo di posta elettronica ed un numero ICQ.



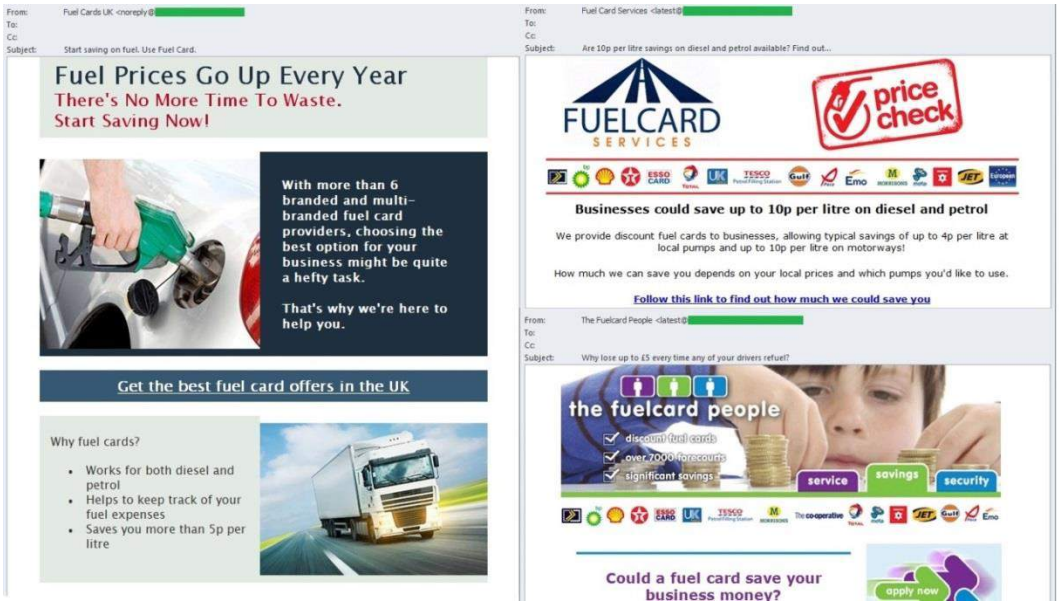
Gioielli

Nell'ambito dei mailing di spam che hanno caratterizzato il periodo oggetto della nostra consueta analisi mensile sulla diffusione delle cosiddette e-mail "spazzatura" all'interno del traffico di posta elettronica globale, ci siamo trovati di fronte ad una moltitudine di messaggi recanti proposte commerciali relative all'acquisto di articoli di gioielleria. Si è trattato, nella maggior parte dei casi, di offerte promozionali e bonus emessi da piccoli negozi di gioielleria, piccoli produttori di bigiotteria e società specializzate nel campo della produzione, taglio e finitura dei diamanti. Talvolta, si invitavano i destinatari di tali messaggi a forme di collaborazione professionale, elencando, tra l'altro, informazioni tecniche e prezzi dettagliati riguardo alla propria produzione.



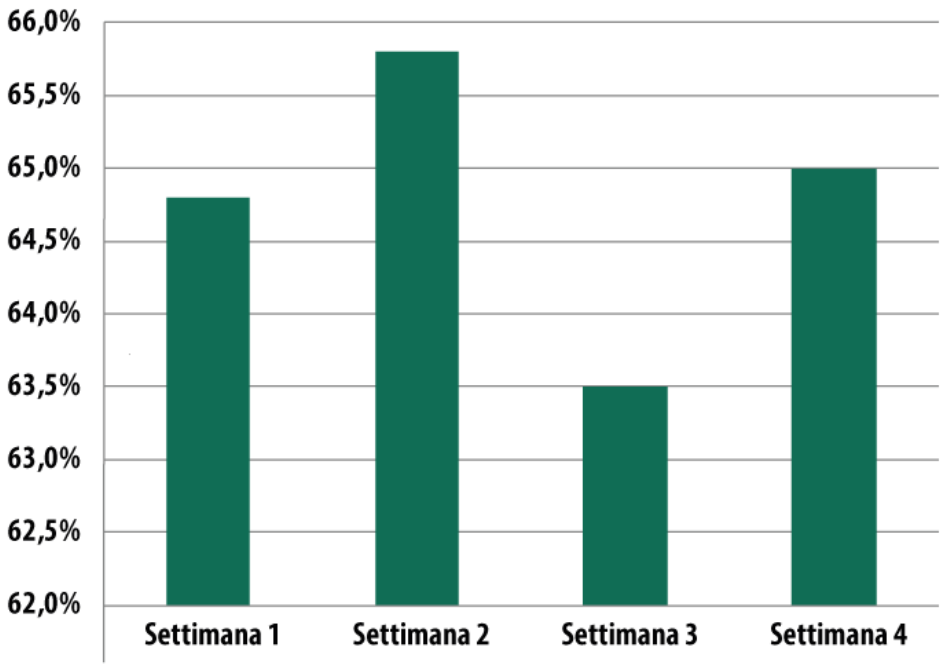
Carte carburante

Una tematica particolarmente diffusa nel quadro dei mailing di massa elaborati dagli spammer nel segmento anglofono di Internet è indubbiamente rappresentata dalla vendita delle carte carburante, strumento preposto ad automatizzare il pagamento dei rifornimenti effettuati dagli automobilisti presso i distributori di benzina. Tale sistema di pagamento del carburante acquistato risulta particolarmente conveniente soprattutto per le compagnie di trasporto provviste di un elevato numero di veicoli, adibiti alla percorrenza di numerose tratte, aziende per le quali si rivelerebbe piuttosto complesso realizzare un efficace controllo delle operazioni di rifornimento via via effettuate. Nella specifica circostanza, gli "intermediari" dello spam propongono, in genere, al destinatario del messaggio, di comparare i vari prezzi indicati riguardo ai diversi tipi di carburante disponibili e di scegliere, quindi, la compagnia più conveniente, per poi sottoscrivere il contratto necessario per l'ottenimento della speciale carta carburante. La peculiarità delle campagne di spam riconducibili a tale particolare tipologia, individuate dai nostri esperti all'interno dei flussi e-mail di giugno, risiede nel fatto che i link posizionati nel corpo delle e-mail in questione sono risultati preposti a condurre i potenziali clienti verso siti web registrati presso domini di recente creazione. Tali siti Internet si sono poi rivelati essere destinati esclusivamente al calcolo di quotazioni e preventivi in materia.



Le statistiche

Quota di spam nel traffico di posta elettronica



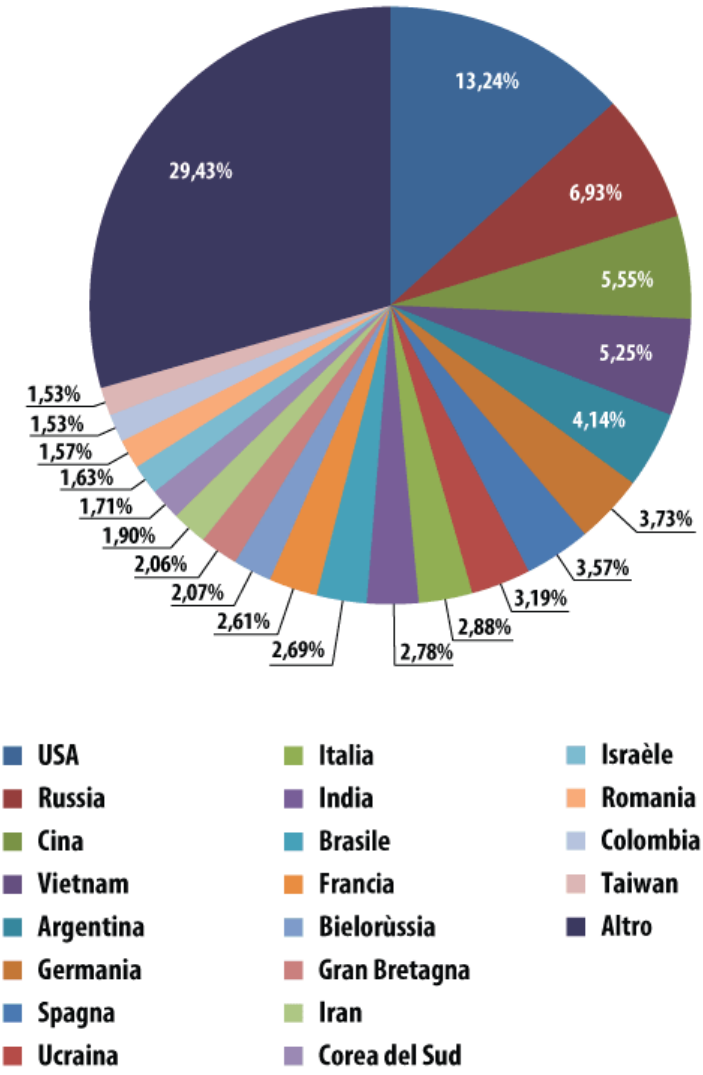
Quote di spam rilevate settimanalmente nel traffico e-mail

Nel mese oggetto del presente report, la quota inerente ai messaggi “spazzatura” rilevati nel traffico globale di posta elettronica ha fatto registrare un decremento del 5% rispetto all’analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 64,8% del volume complessivo di messaggi e-mail circolanti in Rete. L'indice percentuale più elevato è stato osservato nella seconda settimana di giugno (65,8%); la quota di spam più contenuta è stata invece rilevata, all'interno dei flussi e-mail mondiali, nella terza settimana del mese qui analizzato (63,5%).

Ripartizione geografica delle fonti di spam

In precedenza, le statistiche riguardanti la geografia delle fonti di spam, relative ai paesi dal cui territorio vengono distribuite in Rete le maggiori quantità di e-mail indesiderate, venivano elaborate dai nostri esperti sulla base dei dati ottenuti grazie alle speciali "trappole" antispam da noi allestite nei vari paesi. Di fatto, però, i messaggi "spazzatura" catturati attraverso tali "trappole" differiscono, in una certa misura, dallo spam che effettivamente giunge agli utenti reali. Ad esempio, gli speciali strumenti da noi precedentemente adottati non ricevono in alcun modo lo spam di natura mirata, di volta in volta indirizzato a società, enti ed organizzazioni ben specifici. In considerazione di ciò, abbiamo in pratica sostituito le fonti utilizzate per ricavare i dati statistici sulla geografia dello spam; attualmente, grazie al KSN (Kaspersky Security Network), la rete globale di sicurezza da noi implementata attraverso apposite infrastrutture "in-the-cloud", ricaviamo i dati statistici relativi alle fonti geografiche dello spam mondiale

direttamente sulla base dei messaggi di posta elettronica che quotidianamente giungono agli utenti dei nostri prodotti, utenti ubicati in ogni angolo del globo. Poiché questo mese i dati utilizzati per elaborare le relative statistiche sono stati ottenuti tramite una fonte diversa, risulterebbe non corretto effettuare il consueto confronto tra i risultati ricavati nel mese oggetto del report e i dati statistici relativi al precedente periodo analizzato.



Geografia delle fonti di spam rilevate - Graduatoria su scala mondiale

Come evidenzia il grafico qui sopra riportato, nel mese di giugno 2014, nelle posizioni di vertice della speciale graduatoria "globale" delle fonti di spam, relativa ai paesi dal cui territorio sono state distribuite in Rete - verso tutti e cinque i continenti - le maggiori quantità di e-mail "spazzatura", si sono rispettivamente insediati Stati Uniti (13,2%), Russia (7%) e Cina (5,6%).

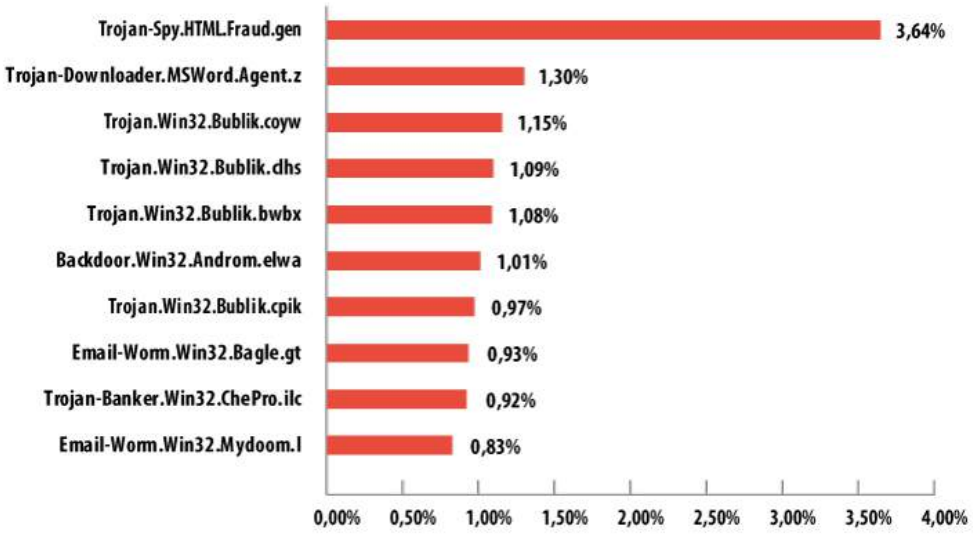
Osserviamo, inoltre, come la quarta piazza del rating di giugno risulti occupata dal Vietnam; la quota ascrivibile ai flussi di spam generati entro i confini del popoloso paese situato nel Sud-Est asiatico ha

fatto complessivamente registrare un valore pari a 5,3 punti percentuali. Segue poi, in quinta posizione, l'Argentina (4,1%). Da parte loro, Germania (3,7%), Spagna (3,6%), Ukraina (3,2%) e Italia (2,9%) sono andate rispettivamente a collocarsi al sesto, settimo, ottavo e nono posto del ranking da noi stilato.

In ultima posizione, nella TOP-10 di giugno 2014, troviamo infine l'India, dal cui territorio è stato distribuito in Rete il 2,8% dello spam mondiale.

Allegati maligni rilevati nel traffico e-mail

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



TOP-10 relativa ai programmi maligni maggiormente diffusi nel traffico di posta elettronica

Rileviamo, in primo luogo, come rispetto al mese precedente, nell'ambito della TOP-10 relativa ai software nocivi maggiormente presenti nei flussi di posta elettronica globali, sia rimasta invariata la posizione occupata dal malware classificato con la denominazione di Trojan-Spy.HTML.Fraud.gen, il temibile programma malevolo che, già da molti mesi, capeggia incontrastato la graduatoria qui sopra riportata. Ricordiamo, nella circostanza, come tale software dannoso, riconducibile alla famiglia di Trojan denominata Fraud.gen, 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.

Al secondo posto della speciale graduatoria da noi stilata, con una quota pari all' 1,30%, si è poi collocato il malware rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Trojan-Downloader.MSWord.Agent.z. Tale software nocivo è stato realizzato dai virus writer sotto forma di file provvisto di estensione *.doc, con tanto di apposita macro incorporata, scritta in VBA (Visual Basic for Applications), la quale viene automaticamente eseguita al momento dell'apertura del documento. Nella circostanza, è la stessa macro che, di fatto, provvede a generare il download e la successiva esecuzione del programma malware in causa.

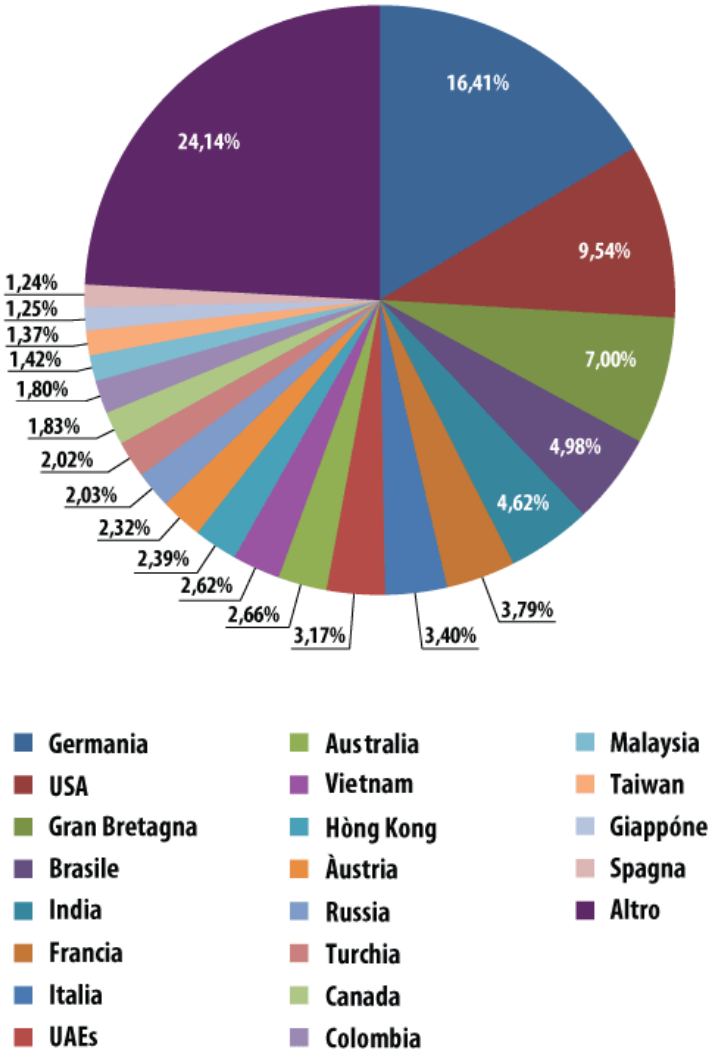
Continuando ad esaminare la composizione della TOP-10 di giugno 2014, salta immediatamente agli occhi la presenza di un cospicuo numero di programmi nocivi appartenenti alla famiglia di malware denominata Bublik, i quali sono andati a collocarsi, rispettivamente, al 3°, 4°, 5° e 7° posto del rating da noi elaborato. Come è noto, le principali funzionalità di cui sono provvisti tali programmi dannosi - riconducibili, per tipologia, alla forma più classica e diffusa di trojan-downloader - consistono, per l'appunto, nel download e nella successiva installazione sul computer-vittima di nuove versioni di programmi maligni, 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 Bublik siano soliti camuffarsi sotto forma di applicazioni o documenti Adobe.

Come evidenzia il grafico qui sopra riportato, il sesto posto del rating in questione è andato ad appannaggio del software nocivo rilevato dalle soluzioni anti-malware di Kaspersky Lab come Backdoor.Win32.Androm.elwa. Si tratta, in sostanza, di una variante del noto bot modulare universale battezzato dagli esperti di sicurezza IT con l'appellativo di Andromeda – Gamarue. In effetti, sulla base del suddetto malware risulta possibile allestire una botnet, o rete-zombie che dir si voglia, dotata delle più svariate funzionalità nocive. Peraltro, i cybercriminali sono soliti estendere tali funzionalità tramite appositi plug-in, i quali possono essere, in qualunque momento, agevolmente caricati dai malintenzionati, nelle quantità che si rivelano di volta in volta necessarie.

All'ottava piazza del ranking qui analizzato, relativo ai programmi malevoli più diffusi all'interno del traffico di posta elettronica globale, 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 carpiti. Tale software maligno 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 malevoli 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.

La nona posizione della graduatoria del malware di giugno 2014 risulta occupata dal software nocivo denominato Trojan-Banker.Win32.ChePro.ilc. Si tratta, più precisamente, di un downloader realizzato dai propri autori sotto forma di applet dotato di estensione CPL (componente del pannello di controllo), preposto a scaricare temibili programmi Trojan sul computer sottoposto ad attacco; tali programmi maligni, a loro volta, vengono in seguito utilizzati dai cybercriminali per compiere il furto delle informazioni confidenziali legate alla sfera finanziaria dell'utente-vittima. Sino ad ora, i malware riconducibili a tale specifica tipologia hanno principalmente preso di mira gli istituti bancari brasiliani e portoghesi.

Concludiamo la nostra breve rassegna riguardo ai software dannosi rilevati con maggiore frequenza all'interno dei flussi e-mail mondiali osservando come la decima piazza della speciale TOP-10 elaborata dagli esperti di Kaspersky Lab sia andata ad appannaggio del programma malevolo classificato come Email-Worm.Win32.Mydoom.l, vero e proprio "habitué" della speciale classifica qui esaminata. Ricordiamo, con l'occasione, che tale worm di rete viene abitualmente distribuito dai cybercriminali sotto forma di allegato ai messaggi di posta elettronica, nonché attraverso le reti di condivisione dei file e le risorse di rete disponibili per operazioni di scrittura. Il compito principale che si prefigge Mydoom.l è quello di effettuare la raccolta degli indirizzi e-mail custoditi nei computer sottoposti ad attacco, per poi realizzare il consueto processo di auto-diffusione in Rete tramite gli account carpiti. Il worm in questione, inoltre, fornisce ai propri "padroni" la ghiotta opportunità di poter controllare da remoto il computer precedentemente infettato.



Suddivisione per paesi dei rilevamenti effettuati dal modulo antivirus e-mail

Analizzando il grafico qui sopra inserito, notiamo immediatamente come, rispetto all'analoga graduatoria relativa allo scorso mese di maggio, la Germania abbia compiuto un più che significativo - per non dire impressionante - balzo in avanti in classifica, andando di fatto ad occupare la prima

posizione del rating di giugno 2014 riguardante i paesi nei quali il nostro modulo antivirus dedicato alla posta elettronica ha eseguito il maggior numero di rilevamenti volti a neutralizzare i programmi malware distribuiti attraverso i flussi e-mail; nel breve volgere di un mese, la quota percentuale attribuibile alla Germania è addirittura raddoppiata (+ 8,17%). La Gran Bretagna, da parte sua, leader dell'analoga classifica del mese precedente, ha "perso" ben due posizioni all'interno del rating in questione, collocandosi in tal modo sul terzo gradino del "podio" virtuale di giugno. L'indice relativo al Regno Unito si è in pratica dimezzato nell'arco di un mese, facendo registrare una diminuzione complessivamente quantificabile in 6,51 punti percentuali.

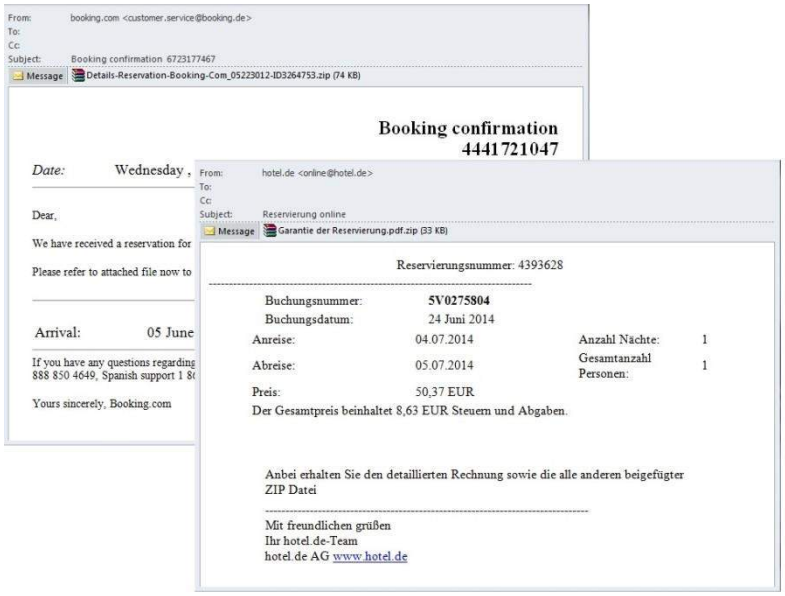
Osserviamo, inoltre, come sia entrata nuovamente a far parte della speciale TOP-20 da noi stilata la Federazione Russa; con una quota pari al 2,03% sul totale dei rilevamenti eseguiti dall'antivirus e-mail, la Russia si è di fatto collocata alla tredicesima posizione della graduatoria qui sopra illustrata.

Il rating del mese di giugno 2014 evidenzia poi come gli Emirati Arabi Uniti abbiano decisamente sopravanzato in classifica Australia, Hong Kong e Vietnam (+ 0,96%). La Svizzera, per contro, non compare più nelle prime venti posizioni del ranking relativo ai paesi che presentano gli indici percentuali più elevati riguardo ai rilevamenti effettuati dal nostro modulo antivirus operante a livello di flussi e-mail globali.

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

Peculiarità e tratti caratteristici dello spam nocivo di giugno

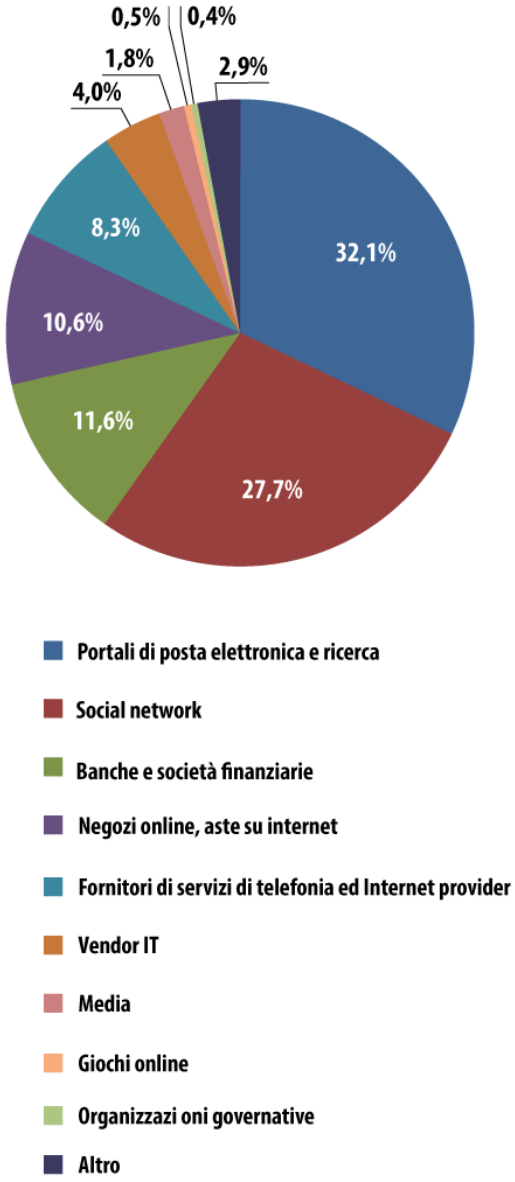
Con l'attesa stagione delle ferie e delle vacanze ormai alle porte, sono stati ovviamente in molti coloro che, durante il mese di giugno, hanno pianificato ed organizzato in ogni minimo dettaglio il proprio viaggio, oppure il soggiorno in località turistiche, occupandosi spesso in prima persona delle questioni organizzative e logistiche, così come delle relative prenotazioni di biglietti aerei e sistemazioni in hotel. Di fatto, parallelamente al tradizionale incremento stagionale del numero di messaggi di spam inerenti alle tematiche legate ai viaggi ed al turismo in generale, è stato da noi rilevato, all'interno dei flussi e-mail di giugno, un sensibile aumento dei messaggi di spam di natura fraudolenta apparentemente inviati a nome di vari servizi di prenotazione online, incluso, ovviamente, quelli più famosi a livello mondiale. Si è trattato, nella fattispecie, dei consueti messaggi e-mail fasulli camuffati sotto forma di notifiche ufficiali relative a conferme di (inesistenti) prenotazioni, infarciti, come al solito, di temibili allegati maligni, spesso mascherati in veste di fatture inerenti alla fantomatica "prenotazione" precedentemente effettuata. Come si può vedere negli screenshot esemplificativi qui sotto inseriti, le e-mail fraudolente in questione riportano costantemente numeri di ordine del tutto fittizi, nonché date fasulle di arrivo/partenza e relativi importi immaginari delle "prenotazioni" eseguite. Nel mese oggetto del presente report, uno dei programmi malware più frequentemente inseriti dai malintenzionati all'interno dei messaggi contraffatti ispirati alle suddette tematiche è risultato indubbiamente essere il software nocivo classificato dagli esperti di sicurezza informatica come Trojan-Spy.Win32.Ursnif. Si tratta, più precisamente, di un programma Trojan adibito al furto dei dati confidenziali, i quali vengono poi trasmessi al server remoto appositamente predisposto dai cybercriminali. Oltre a ciò, il Trojan in causa è perfettamente in grado di spiare il traffico di rete, generare il download e l'esecuzione di ulteriori software malevoli, nonché disabilitare alcune applicazioni di sistema, quali, ad esempio, il firewall.



Già da tempo, ormai, per realizzare la distribuzione di pericolosi programmi maligni nelle e-mail box degli utenti della Rete, i cybercriminali ricorrono non soltanto alle tradizionali notifiche fasulle provenienti (in apparenza!) dai più noti servizi di prenotazione online, da famosi istituti bancari o celebri ipermercati Internet, ma anche a messaggi inviati, a prima vista, da negozi online strettamente specializzati nella vendita di determinati prodotti ed articoli. Così, nel mese passato abbiamo ad esempio individuato, nel traffico di posta elettronica analizzato dai nostri esperti, una campagna di spam malevola volta a distribuire messaggi e-mail apparentemente provenienti da un negozio online specializzato in prodotti per animali. Come al solito, attraverso tali messaggi dannosi si invitava il destinatario dell'e-mail a scaricare e poi stampare la fattura relativa all'acquisto di prodotti per i propri animali domestici. Per ogni questione o chiarimento in merito, il potenziale utente-vittima avrebbe potuto rivolgersi al servizio di assistenza appositamente predisposto dal negozio Internet in causa tramite il proprio sito web, raggiungibile mediante il link subdolamente inserito dai malintenzionati nel corpo dell'e-mail. In realtà, l'archivio compresso allegato al messaggio non recava affatto il file PDF promesso dal mittente, con tutte le informazioni (fasulle) relative all'acquisto, bensì l'insidioso malware denominato Trojan-Banker.Win32.Shiotob.c. Si tratta, più precisamente, di un software malevolo appositamente sviluppato dai virus writer per carpire le informazioni relative al sistema sottoposto ad attacco, al pari dei nomi degli utenti e delle password utilizzate sia nell'ambito dei client FTP, sia per accedere a determinati siti Internet.

Phishing

I dati raccolti ed elaborati dai nostri esperti hanno in primo luogo evidenziato come, nel mese oggetto del presente report dedicato al fenomeno spam, la speciale classifica relativa alle organizzazioni rimaste vittima con maggior frequenza degli assalti portati dai phisher non abbia subito sostanziali variazioni rispetto all'analogo rating del mese precedente. Così come nello scorso mese di maggio, al primo posto della graduatoria da noi stilata troviamo la nuova categoria recentemente definita, denominata "Portali di posta elettronica e ricerca", con una quota pari al 32,1%; rileviamo, nella circostanza, come l'indice percentuale ascrivibile agli attacchi di phishing complessivamente condotti nei confronti di tali risorse web abbia fatto registrare un lievissimo decremento rispetto ad un mese fa, quantificabile in 0,2 punti percentuali. La seconda posizione del rating qui analizzato è andata nuovamente ad appannaggio dei social network (27,7%); il grafico qui sotto riportato evidenzia tuttavia come, nell'arco di un mese, la quota relativa alle reti sociali sia sensibilmente aumentata (+ 3,7% rispetto a maggio 2014). L'indice relativo alla categoria "Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari" (11,6%) ha evidenziato una diminuzione di 1,2 punti percentuali rispetto all'analogo rating del mese precedente. Alla quarta piazza della speciale TOP-100 dedicata al fenomeno phishing si conferma poi la categoria denominata "Negozi Internet ed aste online"; la quota riconducibile agli attacchi orditi dai phisher nei confronti dei negozi online ha ugualmente presentato un significativo decremento rispetto allo scorso mese di maggio (- 1,5%), attestandosi così su un valore medio pari al 10,6%. Terminiamo la nostra breve rassegna dedicata alla classifica del phishing di giugno 2014, osservando come, rispetto a quanto riscontrato un mese fa, l'indice percentuale relativo alle risorse web, organizzazioni e società raggruppate nella categoria "Fornitori di servizi di telefonia ed Internet provider" abbia fatto registrare una lievissima diminuzione, pari allo 0,1%. Di fatto, con una quota equivalente all' 8,30%, la suddetta categoria è andata a collocarsi al quinto posto della graduatoria qui sotto illustrata.

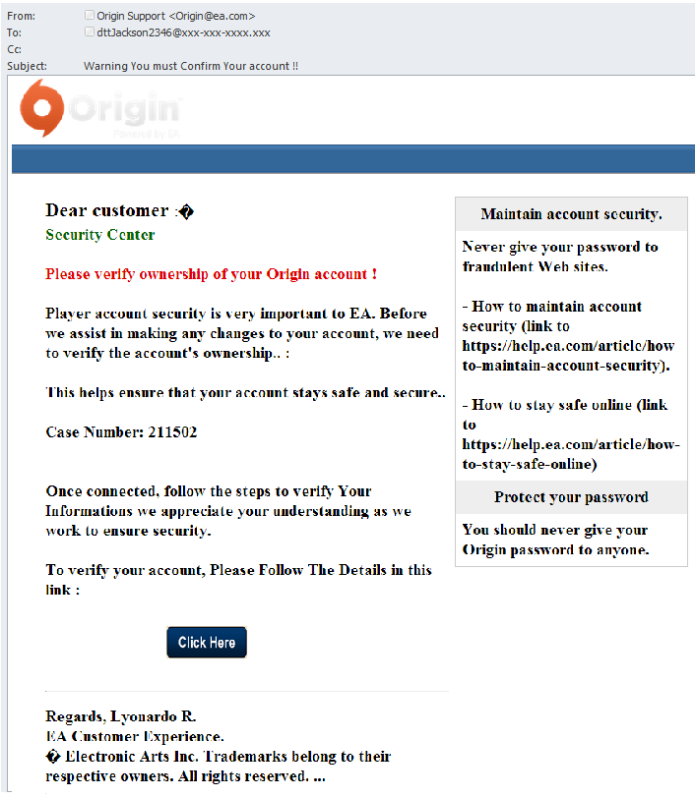


TOP-100 relativa alle organizzazioni maggiormente sottoposte agli attacchi di phishing - Suddivisione per categorie dei rilevamenti eseguiti dal modulo Anti-phishing

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 malevoli contenuti all'interno di messaggi di spam oppure link disseminati nel World Wide Web.

Durante il mese di giugno, i truffatori della Rete riconducibili alla categoria dei phisher hanno diffuso nelle caselle di posta elettronica degli utenti del web un considerevole numero di messaggi di spam mascherati sotto forma di notifiche provenienti (in apparenza) dalla corporation statunitense Electronic Arts (EA), uno dei leader mondiali relativamente allo sviluppo, pubblicazione e distribuzione su scala globale di videogiochi. Nello specifico, i phisher hanno tentato di ottenere l'accesso agli account degli

utenti di Origin, il noto store digitale di proprietà della suddetta società americana. Per cercare di raggirare le potenziali vittime i malintenzionati si sono avvalsi di un vecchio trucco, ormai ampiamente collaudato, ovvero l'invio di messaggi e-mail in cui si sollecita una pronta azione da parte dell'utente allo scopo di innalzare ulteriormente il livello di sicurezza dell'account online posseduto; nella circostanza, i phisher hanno esplicitamente invitato i destinatari delle e-mail malevole a confermare il fatto di essere gli effettivi titolari degli account via via menzionati nei singoli messaggi di phishing. Per conferire alle e-mail in questione un aspetto di ufficialità e legittimità, i phisher hanno utilizzato il logo Origin, nonché appositi link preposti a condurre i destinatari dei messaggi verso il sito ufficiale della società; non è infine mancata la consueta raccomandazione - tipica per simili messaggi fraudolenti - di non comunicare mai a nessuno, in alcun modo, la password impiegata per accedere di volta in volta al proprio account personale.


From: Origin Support <Origin@ea.com>
To: dttJackson2346@xxx-xxx-xxxx.xxx
Cc:
Subject: Warning You must Confirm Your account !!

Origin

Dear customer :
Security Center

Please verify ownership of your Origin account !

Player account security is very important to EA. Before we assist in making any changes to your account, we need to verify the account's ownership.. :

This helps ensure that your account stays safe and secure..

Case Number: 211502

Once connected, follow the steps to verify Your Informations we appreciate your understanding as we work to ensure security.

To verify your account, Please Follow The Details in this link :

Click Here

Regards, Lyonardo R.
EA Customer Experience.
Electronic Arts Inc. Trademarks belong to their respective owners. All rights reserved. ...

Maintain account security.

Never give your password to fraudulent Web sites.

- How to maintain account security (link to https://help.ea.com/article/how to-maintain-account-security).

- How to stay safe online (link to https://help.ea.com/article/how-to-stay-safe-online)

Protect your password

You should never give your Origin password to anyone.

Conclusioni

Nel mese di giugno 2014 la quota dello spam presente nel traffico di posta elettronica mondiale ha fatto registrare un decremento del 5% rispetto all'analogo indice riscontrato nel mese precedente, attestandosi in tal modo su un valore medio pari al 64,8% del volume complessivo di messaggi e-mail circolanti in Rete. Con ogni probabilità, tale significativa diminuzione percentuale riveste un carattere prettamente stagionale, visto che in estate, tradizionalmente, le attività lavorative subiscono un fisiologico rallentamento; in tal modo, viene di fatto disattivato il funzionamento di molti spam bot proprio nel periodo riservato alle ferie e alle vacanze estive, in quanto un vasto numero di computer-vittima risulta momentaneamente scollegato dalla Rete.

Lungo tutto l'arco del mese di giugno 2014, per cercare di raggirare il maggior numero possibile di utenti, i malintenzionati hanno attivamente sfruttato i più importanti avvenimenti politici e sportivi che si sono prodotti sulla scena mondiale. Alla vigilia del Campionato del Mondo di calcio, di sicuro l'evento più atteso ed in assoluto di maggior rilievo per i tifosi e gli appassionati di football di ogni angolo del

globo, i phisher hanno cercato di carpire ai destinatari dei messaggi fraudolenti, più o meno abilmente confezionati, le informazioni sensibili legate alla sfera bancaria degli stessi, con la promessa di far partecipare i potenziali utenti-vittima ad una fantomatica lotteria grazie alla quale, secondo le promesse fasulle dei malintenzionati, si sarebbe potuto guadagnare l'ambito biglietto di ingresso a determinati match previsti nel calendario della Coppa del Mondo FIFA. Da parte loro, i cosiddetti truffatori "nigeriani" hanno invece sfruttato per i loro loschi fini la complessa e delicata situazione socio-politica attualmente attraversata dall'Ukraina, rivolgendosi ai destinatari dei messaggi fraudolenti da essi elaborati con la pretenziosa e consueta richiesta di aiuto per effettuare il trasferimento di inesistenti cifre milionarie su conti bancari esteri.

In giugno, come abbiamo visto in precedenza, la classifica relativa alle organizzazioni (suddivise in apposite categorie) rimaste vittima con maggior frequenza degli assalti portati dai phisher non ha subito sostanziali variazioni rispetto all'analogo rating del mese precedente. La TOP-100 di giugno 2014 dedicata all'analisi del fenomeno phishing è risultata nuovamente capeggiata dalla categoria denominata "Portali di posta elettronica e ricerca", con una quota pari al 32,1%. Così come nel mese precedente, la seconda posizione del rating è andata ad appannaggio dei social network (27,7%); l'indice percentuale attribuibile alle reti sociali ha evidenziato un sensibile aumento (+ 3,7%). Ciò trova una logica spiegazione nel fatto che, tradizionalmente, proprio nel periodo delle vacanze estive si intensificano in maniera considerevole le attività condotte dagli studenti di ogni ordine e grado nell'ambito dei social network; naturalmente, i truffatori cercano di approfittare di tale circostanza, a loro potenzialmente favorevole. La terza posizione della speciale graduatoria elaborata dai nostri analisti di spam relativamente agli attacchi di phishing condotti in Rete nel corso del mese di giugno 2014 è andata poi ad appannaggio della categoria "Organizzazioni finanziarie, sistemi di pagamento online ed istituti bancari" (11,6%).

Sottolineiamo, infine, come la leadership della speciale TOP-10 relativa ai software nocivi maggiormente presenti nei flussi di posta elettronica mondiali sia andata per l'ennesima volta ad appannaggio del programma Trojan classificato dagli esperti di sicurezza IT con la denominazione di Trojan-Spy.HTML.Fraud.gen, da tempo dominatore incontrastato di tale significativa classifica del malware. Ricordiamo, con l'occasione, come questo temibile Trojan venga diffuso dai cybercriminali attraverso messaggi e-mail contraffatti, mascherati sotto forma di notifiche ufficiali provenienti (apparentemente!) da noti istituti bancari e famosi negozi online. Con il rapido approssimarsi delle ferie e delle vacanze estive si è di fatto registrato un sensibile aumento dei messaggi di spam di natura maligna preposti a distribuire pericolosi allegati nocivi nelle e-mail box degli utenti, messaggi inviati (in apparenza!) a nome di vari servizi di prenotazione online, incluso, ovviamente, quelli più noti su scala globale. Concludiamo le nostre osservazioni riassuntive rilevando come, nel mese di giugno, il primo posto della classifica riguardante i paesi nei quali il nostro modulo antivirus dedicato alla posta elettronica ha eseguito il maggior numero di rilevamenti volti a neutralizzare i programmi malware distribuiti attraverso i flussi e-mail - sia andato ad appannaggio della Germania (16,4%), nuovo leader della speciale graduatoria sopra menzionata.