Le cyber-minacce «finanziarie» nell'anno 2013. Parte 1: phishing

Kaspersky Lab

Introduzione: i rischi connessi all'utilizzo del denaro nel mondo multi-device

I criminali informatici specializzati nel sottrarre significative somme di denaro dagli account degli utenti dei negozi online, dei sistemi di pagamento e dei sistemi di Internet banking operano ormai da diversi anni nell'ambito del cybercrimine mondiale. Per lungo tempo, tuttavia, la portata delle losche attività condotte dai malfattori della Rete che si avvalgono di temibili minacce IT rivolte alla sfera finanziaria degli utenti del World Wide Web è risultata limitata da alcuni decisivi fattori, quali, in primo luogo, la diffusione relativamente contenuta, sino a qualche anno fa, degli strumenti specificamente adibiti alle operazioni di pagamento elettronico.

In questi ultimi anni, ad ogni caso, l'utilizzo della moneta elettronica sta assumendo un'importanza sempre più rilevante. Gli indubbi vantaggi in termini di comodità e convenienza, così come l'ormai ampia disponibilità, su scala globale, di una vasta offerta di sistemi di pagamento online e di servizi di Internet banking, attirano, in effetti, un enorme numero di utenti, in misura sempre maggiore. Da parte loro, gli organismi preposti alla regolamentazione del settore finanziario, così come gli istituti bancari di numerosi paesi del globo, stanno addirittura seriamente considerando l'eventualità di rinunciare del tutto alla circolazione di denaro contante all'interno dei propri sistemi economici nazionali, a tutto vantaggio di una progressiva ed irreversibile espansione dell'utilizzo di forme monetarie "virtuali", che non prevedano in alcun modo, in un futuro tutt'altro che remoto, l'impiego dei contanti. I dati statistici raccolti mediante un'approfondita indagine globale condotta congiuntamente, nel corso del 2013, dalla nota agenzia di marketing B2B International e dagli esperti di Kaspersky Lab, confermano in maniera inequivocabile la crescente popolarità di cui attualmente godono i sistemi di pagamento digitale presso il vasto pubblico degli utenti della Rete: il 98% di coloro che sono stati interpellati ha in effetti dichiarato di utilizzare regolarmente i propri dispositivi digitali per effettuare operazioni finanziarie nell'ambito dei servizi di banking online e dei sistemi di pagamento disponibili sul web, così come di eseguire abitualmente acquisti di e-commerce presso negozi Internet.

La specifica tendenza che prospetta il graduale passaggio verso l'utilizzo di forme di pagamento che non prevedano l'impiego di denaro contante si accompagna, al giorno d'oggi, all'inevitabile aumento del numero dei dispositivi attraverso i quali vengono condotte le transazioni finanziarie. I dati raccolti attraverso l'indagine evidenziano tuttavia come, al momento attuale, i PC ed i laptop continuino ad essere i "principali" dispositivi mediante i quali gli utenti interagiscono con i servizi online legati alla sfera finanziaria: di fatto, l' 87% degli interpellati ha affermato di eseguire operazioni con moneta elettronica avvalendosi di un computer desktop o portatile. E' risultata in ogni caso particolarmente significativa anche la quota percentuale di dispositivi mobili impiegati dagli utenti per i medesimi scopi: è in effetti emerso come, al momento attuale, le operazioni finanziarie condotte tramite l'utilizzo di tablet o smartphone vengano rispettivamente eseguite dal 22% e dal 27% degli utenti consultati.

Le tendenze, come di consueto, non sono affatto passate inosservate agli occhi dei malintenzionati. La rapida ed inarrestabile crescita del numero degli utenti che ricorrono quotidianamente all'impiego della vasta gamma dei sistemi di pagamento elettronico attualmente disponibili in Rete attira inevitabilmente le attenzioni dei malfattori dediti al cybercrimine, i quali, in misura sempre maggiore, investono consistenti risorse nell'organizzazione di sofisticati schemi fraudolenti, la cui realizzazione permette poi ai criminali informatici di ottenere, in primo luogo, l'accesso ai dati finanziari degli utenti e, in seguito, quale naturale e purtroppo ovvia conseguenza, l'accesso alle stesse risorse finanziarie di cui questi ultimi dispongono. Nonostante gli attacchi rivolti alla sfera finanziaria costituiscano una delle tipologie di assalto informatico in assoluto più complesse e costose, rappresentano indiscutibilmente una delle forme più redditizie di crimine informatico, poiché, in caso di esito positivo dell'attacco condotto, essi sono in grado di garantire l'accesso diretto al denaro posseduto dall'utente-vittima. Tutto ciò che rimane da fare - quindi - ai cybercriminali, è di sottrarre agevolmente il denaro dall'account violato, per poi convertirloin contanti, mentre, ad esempio, l'autore di programmi malware o il titolare di una botnet adibita alla conduzione di attacchi DDoS o all'invio di montagne di spam dovrà pur sempretrovare gli acquirenti interessati ai "servizi" offerti.

Kaspersky Lab, da oltre 16 anni, si occupa dell'elaborazione e dello sviluppo di strumenti in grado di proteggere gli utenti nei confronti di ogni possibile tipologia di cyber-attacco, inclusi gli attacchi informatici direttamente connessi all'ambito finanziario. Il processo di creazione e sviluppo di simili tecnologie di protezione IT non risulterebbe di fatto possibile senza una costante e dettagliata analisi dei nuovi sample di software nocivo che vanno di volta in volta a popolare il panorama del malware, così come dei metodi di ingegneria sociale e degli altri strumenti di cui è solita avvalersi ampiamente la categoria dei cybercriminali specializzati nell'allestire frodi riconducibili alla sfera finanziaria. Una delle conclusioni più evidenti che si può immediatamente trarre sulla base dei dati raccolti tramite tale analisi evidenzia come, a differenza di molte altre tipologie di assalto informatico, gli attacchi di natura finanziaria, preposti ad arrecare consistenti danni economici agli utenti-vittima, comprendano in genere un'ampia varietà di mezzi e strumenti nocivi: si va, in effetti, dall'allestimento di pagine web di phishing - volte ad imitare le pagine Internet presenti all'interno dei siti ufficiali di istituzioni finanziarie del tutto legittime - allo sfruttamento delle vulnerabilità via via individuate in applicazioni e piattaforme particolarmente diffuse, così come al dispiegamento di programmi nocivi appositamente creati "su commissione".

Data l'indubbia e comprovata complessità dei cyber-attacchi di natura finanziaria, la conseguente analisi dell'impatto da essi esercitato sul livello di sicurezza IT degli utenti della Rete richiede ogni volta un approccio particolarmente attento e composito. E' per tale specifica ragione che, nel realizzare il presente report, gli esperti di Kaspersky Lab hanno preso in considerazione non soltanto le minacce IT rivolte alle varie versioni del sistema operativo Windows, ma anche le cyber-minacce specificamente indirizzate alle piattaforme OS X e Android. Allo stesso modo, i nostri analisti hanno attentamente esaminato non solo i programmi malware "specializzati" in materia, ma anche ulteriori software, potenzialmente in grado di poter carpire i dati finanziari degli utenti. Sono stati infine debitamente analizzati, dai nostri esperti, non soltanto gli eclatanti fenomeni relativi alla distribuzione e diffusione di pericolosi programmi Trojan, ma anche i subdoli ed insistenti assalti quotidianamente portati

dai phisher. E' ben noto, in effetti, come gli attacchi di phishing possano costituire uno strumento particolarmente efficace al fine di sottrarre preziose informazioni sensibili agli utenti-vittima presi di mira, nella fattispecie i dati relativi alla sfera finanziaria di questi ultimi. Solo l'adozione di un approccio particolarmente complesso ed omnicomprensivo può consentire - secondo Kaspersky Lab - di raggiungere pienamente gli scopi che si pone questo report: fornire in primo luogo un quadro più ampio possibile riguardo al vasto panorama delle minacce informatiche appositamente create dai virus writer per cercare di sottrarre agli utenti le risorse finanziarie online di cui questi ultimi dispongono. In secondo luogo, la presente relazione si pone ugualmente l'obiettivo di fornire una valutazione complessiva ed esauriente riguardo all'entità e all'estensione del pericolo effettivamente rappresentato, al giorno d'oggi, da simili cyber-minacce.

Metodologie e criteri adottati nell'elaborazione del report

Per stilare la presente relazione sono stati utilizzati i dati ricevuti tramite gli utenti del Kaspersky Security Network, l'estesa rete globale di sicurezza da noi implementata attraverso specifiche infrastrutture "in-the-cloud", preposta ad una rapida elaborazione dei dati relativi alle minacce informatiche sulle quali, di volta in volta, si imbattono gli utenti delle soluzioni di sicurezza IT sviluppate da Kaspersky Lab. Il Kaspersky Security Network (KSN) è stato in particolar modo creato proprio con l'intento di fornire il più rapidamente possibile, agli utenti dei nostri prodotti, preziose informazioni riguardo alle minacce IT più recenti. Grazie alla rete di sicurezza in questione, l'intervallo di tempo che generalmente intercorre tra il rilevamento di una minaccia in precedenza sconosciuta e l'aggiunta della relativa firma nell'apposito database antivirus può essere davvero calcolato in termini di minuti. Un'altra significativa caratteristica del Kaspersky Security Network è rappresentata dal fatto che tale sistema di sicurezza "in-the-cloud" provvede ad elaborare in maniera del tutto anonima, priva di qualsiasi forma di personalizzazione, le statistiche relative alle minacce informatiche che cercano quotidianamente di attaccare i computer degli utenti. Inoltre, sono gli stessi utenti del KSN a fornire previamente il proprio assenso per effettuare la trasmissione di dati statistici ai nostri analisti, su base del tutto volontaria. Nella circostanza specifica, le informazioni ricevute tramite gli utenti dei nostri prodotti, attraverso il Kaspersky Security Network, hanno costituito la base per la realizzazione del presente report dedicato all'analisi del cybercrimine "finanziario".

Nell'ambito della relazione da noi stilata sono state in primo luogo considerate le informazioni relative al numero dei rilevamenti eseguiti dai componenti di sicurezza IT - implementati nei prodotti Kaspersky Lab - adibiti alla protezione degli utenti nei confronti del phishing (per quel che riguarda le piattaforme Microsoft Windows ed Apple OS X), dei programmi malware (relativamente alla piattaforma Windows) e del malware specificamente sviluppato per colpire i dispositivi mobili (riguardo alla piattaforma Google Android). Inoltre, sono stati ugualmente considerati i dati statistici relativi agli utenti sottoposti ad attacco, nel caso specifico dei sottosistemi (moduli) di protezione - facenti parte delle soluzioni di sicurezza IT di Kaspersky Lab - che offrono tale ulteriore opportunità di rilevamento. Il presente report

analizza i dati relativi alla "geografia" degli attacchi informatici di natura finanziaria condotti nel corso del 2013, così come il grado d'intensità degli stessi.

L'indagine da noi svolta abbraccia tutto l'arco dell'anno 2013; per effettuare le necessarie comparazioni statistiche, sono stati utilizzati gli analoghi dati raccolti nel corso del 2012. In qualità di oggetti specifici della ricerca condotta dagli esperti di Kaspersky Lab sono stati in primo luogo scelti i potenziali obiettivi delle campagne di phishing; si è in tal modo provveduto a considerare l'entità complessiva dei tentativi di download (opportunamente bloccati dalle nostre soluzioni di sicurezza IT) di pagine web contraffatte relative a sistemi di pagamento, servizi di banking online, negozi online ed altri possibili "bersagli" di natura finanziaria. I nostri analisti hanno inoltre selezionato alcune decine di sample di malware (si è trattato, nella fattispecie, di software nocivi appositamente progettati dai virus writer per realizzare il furto dei dati sensibili di natura finanziaria degli utenti), provvedendo ad esaminare il loro grado di diffusione globale nel corso del periodo oggetto del presente report.

Infine, vista l'estrema popolarità raggiunta nel 2013 dal Bitcoin, la celebre criptovaluta, gli esperti di Kaspersky Lab hanno inserito in una categoria a parte le minacce IT specificamente connesse al furto e alle attività di generazione di tale moneta virtuale, seguendo in dettaglio l'evoluzione delle stesse.

Principali risultati della ricerca

Sulla base dei dati ottenuti attraverso i sottosistemi di protezione implementati nei prodotti Kaspersky Lab è in primo luogo emerso che, nel corso del 2013, il numero degli attacchi informatici rivolti alla sfera finanziaria degli utenti - sia nell'ambito delle campagne di phishing che nel quadro degli attacchi condotti mediante l'utilizzo di temibili malware - è di fatto sensibilmente cresciuto.

Riassumiamo, qui di seguito, i principali dati statistici da noi raccolti ed elaborati nel corso della ricerca condotta riguardo all'attuale diffusione ed evoluzione delle cyber-minacce "finanziarie":

- Il 31,45% del volume complessivo degli attacchi di phishing organizzati dai truffatori lungo tutto l'arco del 2013 è risultato essere rivolto al settore finanziario.
- Il 22,2% del numero totale degli attacchi portati dai phisher è stato realizzato mediante pagine web fasulle volte ad imitare i siti ufficiali di numerosi istituti bancari; rispetto al 2012, la quota percentuale riconducibile al phishing "bancario" è in sostanza raddoppiata.
- Il 59,5% degli attacchi di phishing aventi quali obiettivo gli utenti delle banche ha indebitamente sfruttato i nominativi di 25 istituti bancari di primaria importanza, di assoluta caratura internazionale. La rimanente quota percentuale di attacchi "bancari" condotti dai phisher ha visto prendere di mira, complessivamente, oltre 1.000 ulteriori istituti di credito.
- Il 38,92% dei rilevamenti eseguiti grazie alle tecnologie di protezione IT appositamente sviluppate da Kaspersky Lab per i computer dotati di sistema operativo Mac è risultato riconducibile all'individuazione e alla conseguente

neutralizzazione di pagine web di phishing strettamente collegate alla sfera finanziaria degli utenti della Rete.

Nei successivi capitoli del report da noi stilato provvederemo ad esaminare in dettaglio le dinamiche degli attacchi "finanziari" che hanno maggiormente contrassegnato l'anno 2013, così come la geografia degli stessi e gli obiettivi da essi presi di mira.

Le minacce IT legate al phishing

La pratica del phishing, ovvero la creazione di copie fasulle di pagine web di siti ufficiali, allo scopo di carpire i dati confidenziali degli utenti, rappresenta indubbiamente, al giorno d'oggi, una minaccia IT assai diffusa. Ciò è principalmente dovuto al fatto che, per poter attuare e condurre una semplice campagna di phishing, il cybercriminale non deve necessariamente possedere conoscenze specifiche nel campo della programmazione; risulta in effetti sufficiente, per il truffatore, disporre esclusivamente delle minime competenze richieste per poter creare pagine web. Lo scopo principale che si prefigge il phishing è quello di cercare di convincere l'utente-vittima riguardo al fatto che quest'ultimo sia giunto su un sito web del tutto autentico, per nulla contraffatto. Spesso, purtroppo, tali tentativi hanno successo; le campagne di phishing vengono di frequente utilizzate, da parte dei truffatori, sia come principale strumento per l'ottenimento di informazioni sensibili riguardo agli utenti via via presi di mira, sia in qualità di componente indispensabile nel quadro di attacchi informatici particolarmente complessi, attraverso i quali si cerca di attirare gli utenti verso un determinato sito web nocivo, appositamente allestito per generare il download di pericolosi programmi malware sui computer-vittima sottoposti ad attacco.

In effetti, come ha ampiamente evidenziato la specifica ricerca condotta dai nostri esperti, le pagine di phishing vengono molto spesso utilizzate nell'ambito di cyber-attacchi orientati al furto dei dati finanziari degli utenti. Prima di procedere ad una dettagliata analisi di tali attacchi informatici, riteniamo opportuno fornire il quadro globale dell'evoluzione delle minacce "finanziarie" lungo tutto l'arco del 2013.

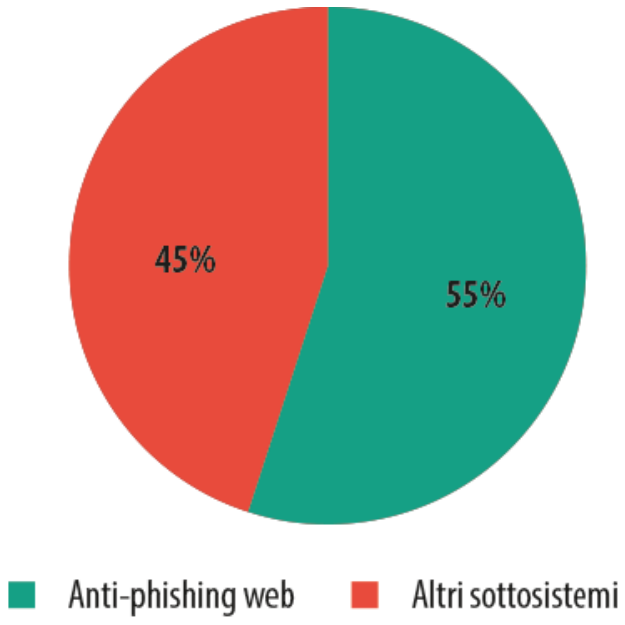
Gli attacchi nei confronti degli utenti

Per garantire un elevato livello di sicurezza nei confronti degli attacchi di phishing, i prodotti Kaspersky Lab si basano su quattro sottosistemi di protezione ben distinti tra loro. Il primo di essi è rappresentato dai database anti-phishing - simili ai database delle firme antivirus, riguardanti i file nocivi - i quali vengono custoditi sui dispositivi degli utenti e contengono l'elenco dei link di phishing più diffusi, attuali e pertinenti al momento del rilascio dei database stessi. Il secondo sottosistema è costituito dal database anti-phishing situato "in-the-cloud", al quale i prodotti Kaspersky Lab adibiti alla protezione IT si rivolgono nel caso in cui l'utente si sia imbattuto in qualche link sospetto, riguardo al quale, tuttavia, non esiste ancora alcuna specifica informazione all'interno del database anti-phishing locale. Il database collocato nella "nuvola telematica" viene ovviamente aggiornato con maggiore rapidità rispetto agli analoghi database custoditi a livello locale; la sua principale funzione consiste nel rilevare gli attacchi di phishing più recenti.

Oltre a ciò, sono stati implementati, nei prodotti Kaspersky Lab, due sistemi automatici per il rilevamento sia dei link che delle pagine Internet di phishing: si tratta, più precisamente, del

sistema anti-phishing dedicato alla posta elettronica e del sistema anti-phishing per vigilare sulla navigazione dell'utente web. Il primo di tali sistemi di sicurezza procede alla verifica dei link presenti nei messaggi e-mail ricevuti dall'utente, nel caso in cui quest'ultimo utilizzi, sul proprio computer, uno dei client di posta elettronica maggiormente diffusi (ad esempio Microsoft Outlook od altri ancora). Il sistema automatico per l'esecuzione dei rilevamenti anti-phishing a livello di World Wide Web verifica invece, da parte sua, tutto ciò che appare sul browser dell'utente, applicando, nella circostanza, un sofisticato insieme di regole euristiche; in pratica, tale sottosistema di protezione è in grado di individuare pagine web di phishing del tutto nuove, di recentissima creazione, delle quali non sussiste ancora alcuna informazione all'interno dei vari database sopra citati.

Nello stilare il presente resoconto sul fenomeno globale delle cyber-minacce finanziarie, gli esperti di Kaspersky Lab si sono avvalsi esclusivamente dei dati ottenuti attraverso il sistema di rilevamento dedicato al web, poiché, di regola, tale sistema entra in funzione soltanto nel caso in cui non risultino ancora presenti, all'interno dei database elaborati da Kaspersky Lab, informazioni relative alla nuova pagina di phishing individuata; inoltre, a differenza dei database custoditi localmente o nel cloud, il sistema anti-phishing web consente di definire esattamente l'obiettivo dell'attacco portato dai phisher. Infine, mentre i database anti-phishing sono in grado di riconoscere l'attacco dei phisher semplicemente in ragione della presenza del link nocivo all'interno del messaggio di posta elettronica o nell'ambito dei risultati della ricerca effettuata attraverso Google, il sistema automatico preposto al rilevamento sul web entra in opera nel momento in cui l'utente provvede a cliccare sul link di phishing, ovvero nel momento stesso in cui l'utente si trova già parzialmente coinvolto nello schema della truffa organizzata dai malfattori.



Quota attribuibile al sottosistema anti-phishing web in relazione al numero complessivo di rilevamenti eseguiti nel 2013

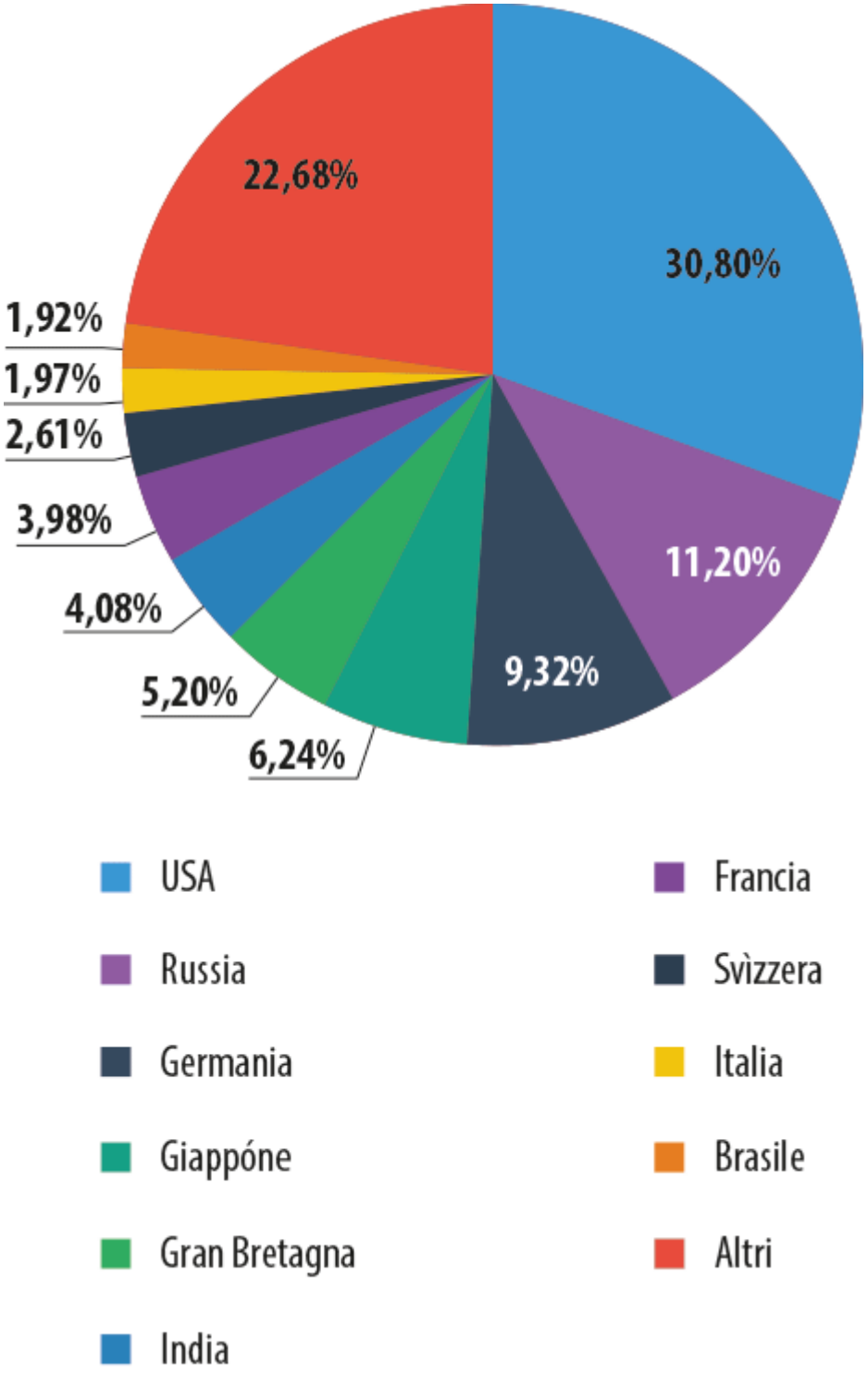
I dati raccolti ed elaborati dagli esperti di Kaspersky Lab hanno evidenziato come, nel 2013, si siano imbattuti in attacchi riconducibili al phishing **39,6 milioni** di utenti. Tale cifra risulta

leggermente superiore (+ 2,32%) rispetto all'analogo valore riscontrato riguardo all'anno 2012.

Complessivamente, da tutti i sottosistemi di protezione IT implementati nel modulo Anti-phishing di Kaspersky Lab sono stati trasmessi oltre 600 milioni di notifiche, nel preciso momento in cui i nostri utenti si sono trovati di fronte a link o pagine web adibiti al phishing. Si tratta di una cifra del tutto paragonabile a quella fatta registrare, per l'analogo parametro, nel 2012. Per contro, nel periodo preso in considerazione dal presente report, il numero degli attacchi bloccati e neutralizzati dal sistema anti-phishing web, basato su metodi euristici, è sensibilmente aumentato (+ 22,2%); si è in effetti passati dai **270 milioni** di attacchi rilevati nell'anno 2012 ai circa **330 milioni** di assalti di phishing complessivamente individuati nel corso del 2013. Tale significativo risultato è indiscutibilmente legato alle costanti migliorie apportate al sistema di rilevamento euristico implementato nelle nostre soluzioni di sicurezza.

Geografia degli attacchi di phishing

Nel corso del 2013, la maggior parte degli assalti di phishing bloccati dai prodotti Kaspersky Lab ha riguardato gli USA; in effetti, il 30,8% del volume complessivo di tali attacchi è risultato essere indirizzato proprio nei confronti di utenti della Rete entro i confini del territorio statunitense. Il secondo ed il terzo gradino del "podio" virtuale relativo alla speciale graduatoria "geografica" del phishing da noi stilata sono andati rispettivamente ad appannaggio della Federazione Russa (11,2% del numero totale di attacchi neutralizzati) e della Germania (9,32%).



TOP-10 relativa ai paesi più frequentemente sottoposti ad attacco nel corso del 2013

I dati presenti nel grafico qui sopra riportato e nei successivi capitoli del nostro report sono stati ottenuti attraverso il Kaspersky Security Network

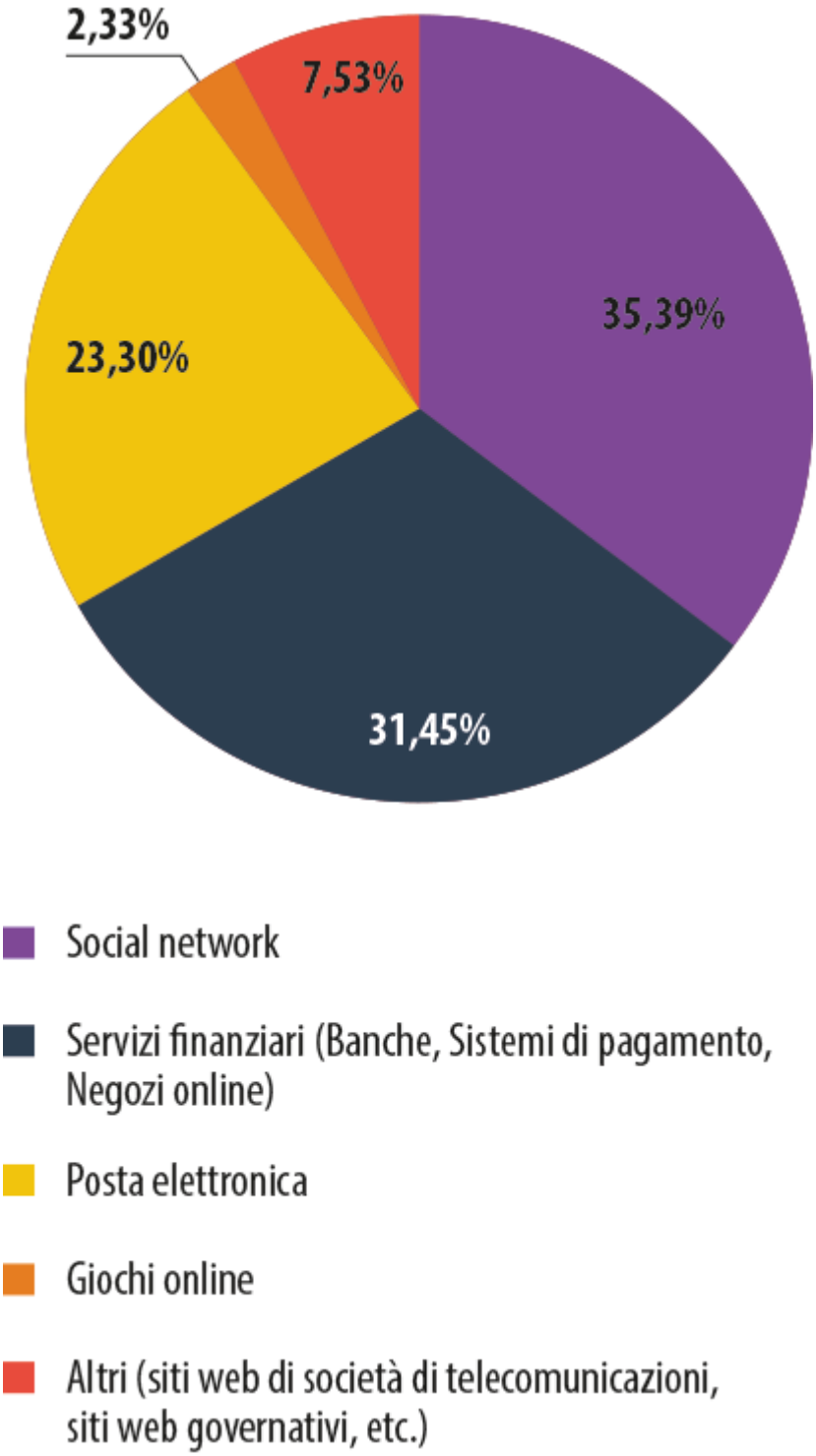
Desideriamo innanzitutto sottolineare come la TOP-10 inerente ai paesi maggiormente sottoposti agli attacchi condotti dai phisher lungo tutto l'arco del 2013 presenti significative

variazioni rispetto all'analoga situazione riscontrata riguardo all'anno 2012. Ad esempio, la quota relativa agli attacchi portati nei confronti degli utenti situati sul territorio della Federazione Russa ha fatto registrare una diminuzione di ben 9,19 punti percentuali, mentre l'indice relativo agli attacchi eseguiti a danno degli utenti ubicati sul territorio degli Stati Uniti è considerevolmente aumentato, passando dal 17,56% del 2012 al 30,8% fatto segnare nell'anno 2013. Allo stesso modo, ha presentato un incremento di 3,49 punti percentuali la quota relativa agli assalti condotti dai phisher a scapito degli utenti situati entro i confini della Germania; in un anno tale indice è in effetti salito dal 5,83% al 9,32%.

Le ragioni che hanno determinato una simile ripartizione geografica degli attacchi di phishing nel corso del 2013 possono essere innumerevoli. Nell'eseguire, negli anni precedenti, indagini analoghe, ci siamo ugualmente trovati di fronte a situazioni che vedevano una significativa diminuzione del volume degli attacchi nei confronti degli utenti di una determinata serie di paesi, mentre relativamente agli utenti di altre nazioni si era invece manifestato un evidente incremento di tale importante parametro. Un'improvvisa diminuzione del numero degli assalti di phishing può dipendere, ad esempio, da specifici fattori quali l'inasprimento delle misure adottate dalle autorità di certi paesi nella lotta contro la cybercriminalità, oppure l'aver reso particolarmente difficoltose le procedure di registrazione dei nomi di dominio, e via dicendo. Per contro, il veloce aumento del volume degli attacchi eseguiti dai phisher può essere provocato, in generale, dal "naturale" incremento del numero complessivo degli utenti Internet, così come, nello specifico, dal sempre crescente numero di utenti che, al giorno d'oggi, usufruiscono dei vari servizi disponibili online: social network, negozi di e-commerce ed altri ancora. In pratica, quanto più di frequente gli utenti di un determinato paese visualizzano sul proprio browser pagine scaricate dal web, tanto maggiore risulterà, per questi ultimi, il rischio di imbattersi in insidiose e subdole pagine Internet appositamente allestite dai phisher.

Gli obiettivi dei phisher

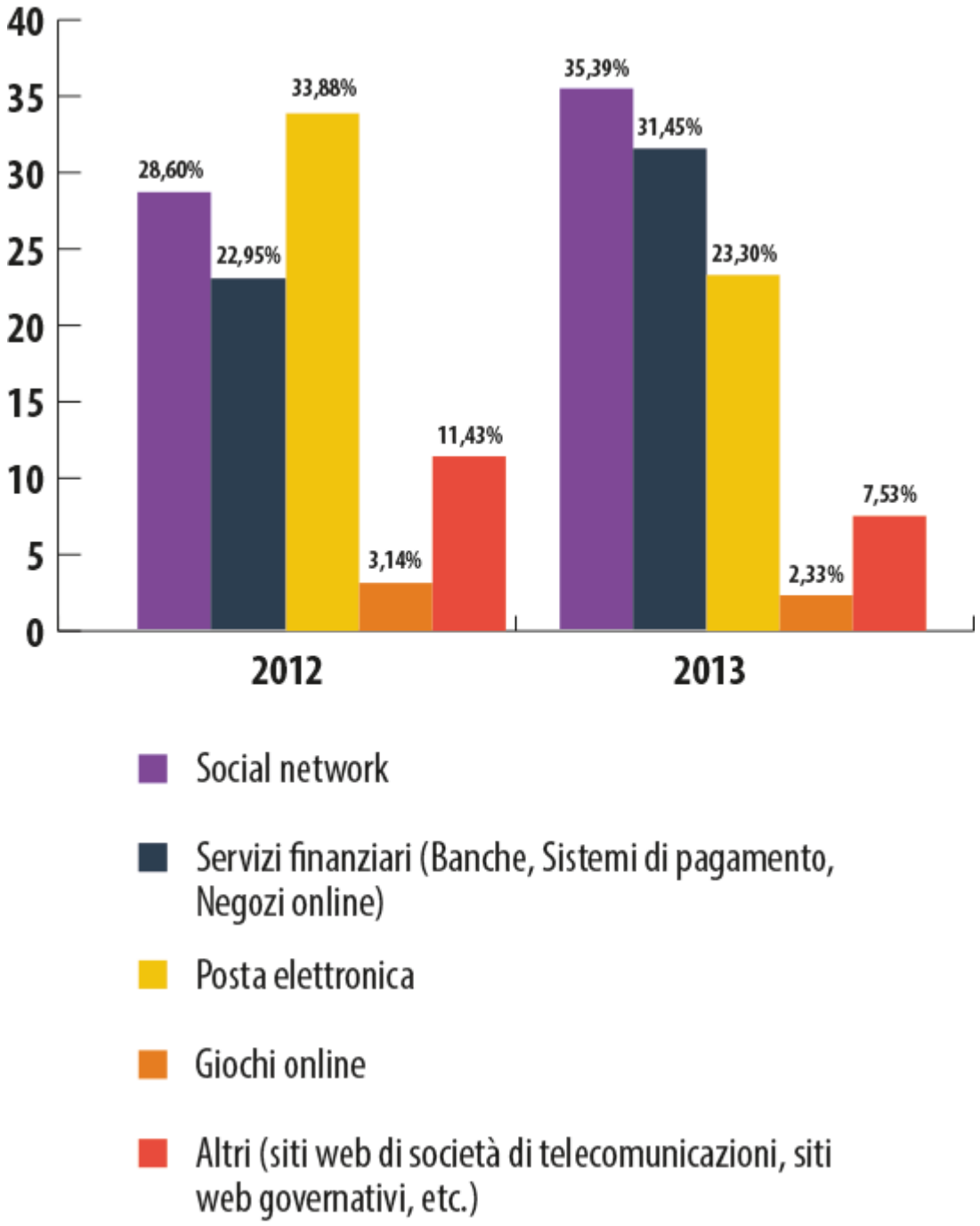
Come evidenzia il grafico qui sotto riportato, una considerevole parte degli attacchi sferrati dai phisher nel corso dell'anno oggetto del presente report ha avuto quale specifico bersaglio i social network: è risultato in effetti attribuibile a tale categoria circa il 35,4% del volume totale degli assalti neutralizzati dal nostro modulo Anti-phishing lungo tutto l'arco del 2013. Il 31,45% degli attacchi organizzati dai phisher è stato invece indirizzato proprio ad obiettivi finanziari, mediante l'allestimento di siti fasulli preposti ad imitare i siti web ufficiali di istituti bancari, sistemi di pagamento online e negozi Internet. La terza piazza della graduatoria risulta occupata dai servizi di posta elettronica, con una quota pari al 23,3% del numero complessivo di attacchi di phishing rilevati sul web.



Gli obiettivi delle campagne di phishing condotte nel 2013

E' innanzitutto interessante osservare come, rispetto al 2012, si sia assistito ad un profondo cambiamento riguardo alla ripartizione per categorie dei bersagli via via presi di mira dai phisher. La quota relativa agli attacchi mediante l'utilizzo di pagine web fasulle appartenenti, in apparenza, ai social network, ha fatto registrare un incremento di 6,79 punti percentuali,

attestandosi in tal modo su un valore pari al 35,39%. L'indice riguardante gli attacchi di phishing rivolti ad obiettivi "finanziari" ha fatto anch'esso segnare un veloce aumento (+ 8,5%), raggiungendo in tal modo una quota pari al 31,45%. E' invece sensibilmente diminuita, di ben 10,5 punti percentuali, la quota relativa agli attacchi diretti ai servizi di posta elettronica: essa si è stabilizzata su un valore medio annuale del 23,3%; allo stesso modo, anche l'indice relativo ai giochi online ha manifestato una significativa flessione, passando dal 3,14% riscontrato nell'anno 2012 al 2,33% fatto registrare nel 2013.

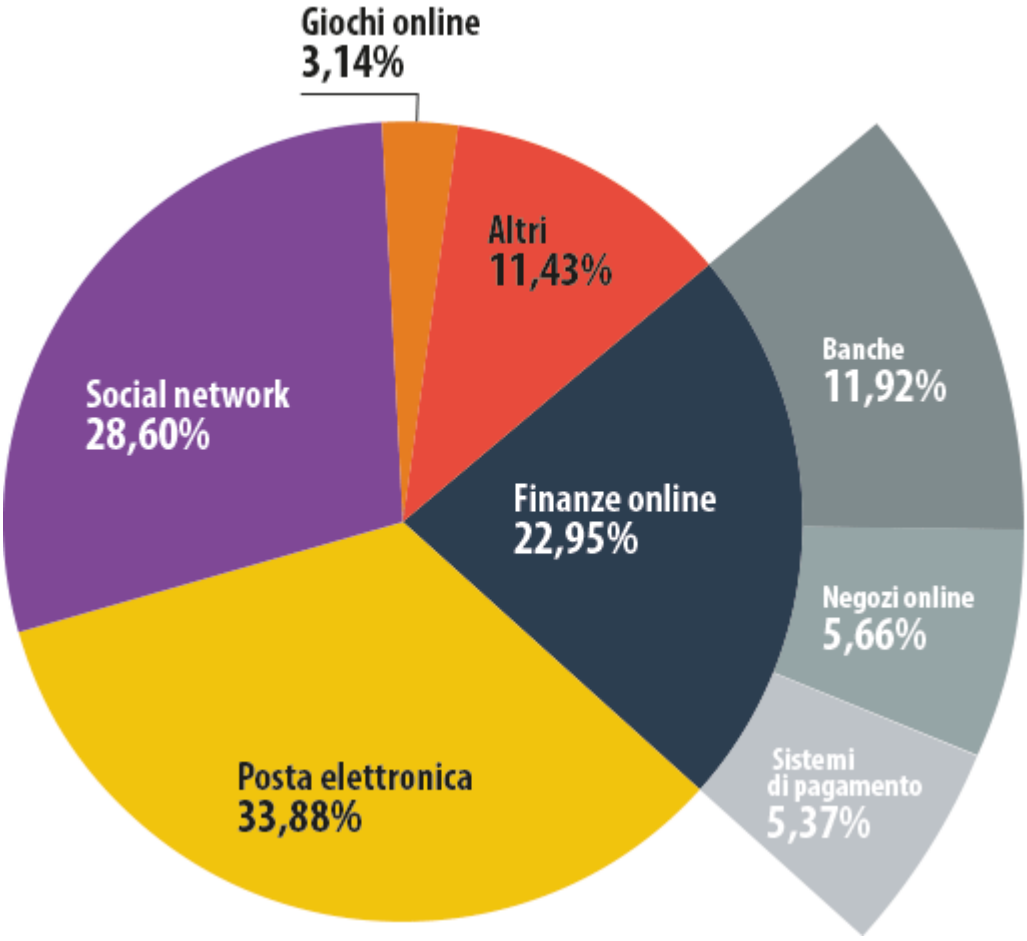


Gli obiettivi del phishing a confronto - Periodo: 2012- 2013

Prendendo come termini di riferimento i valori rilevati nel corso del 2012, traspare in tutta evidenza, dal grafico qui sopra inserito, come, nel 2013, l'aumento di quota più elevato abbia riguardato proprio la categoria degli attacchi ad orientamento prettamente "finanziario". Tale interessante elemento fornisce ovviamente lo spunto per effettuare un'analisi ancor più dettagliata ed attenta delle complesse dinamiche che hanno contraddistinto tale specifica tipologia di attacchi di phishing.

Gli attacchi "finanziari": una tendenza preoccupante

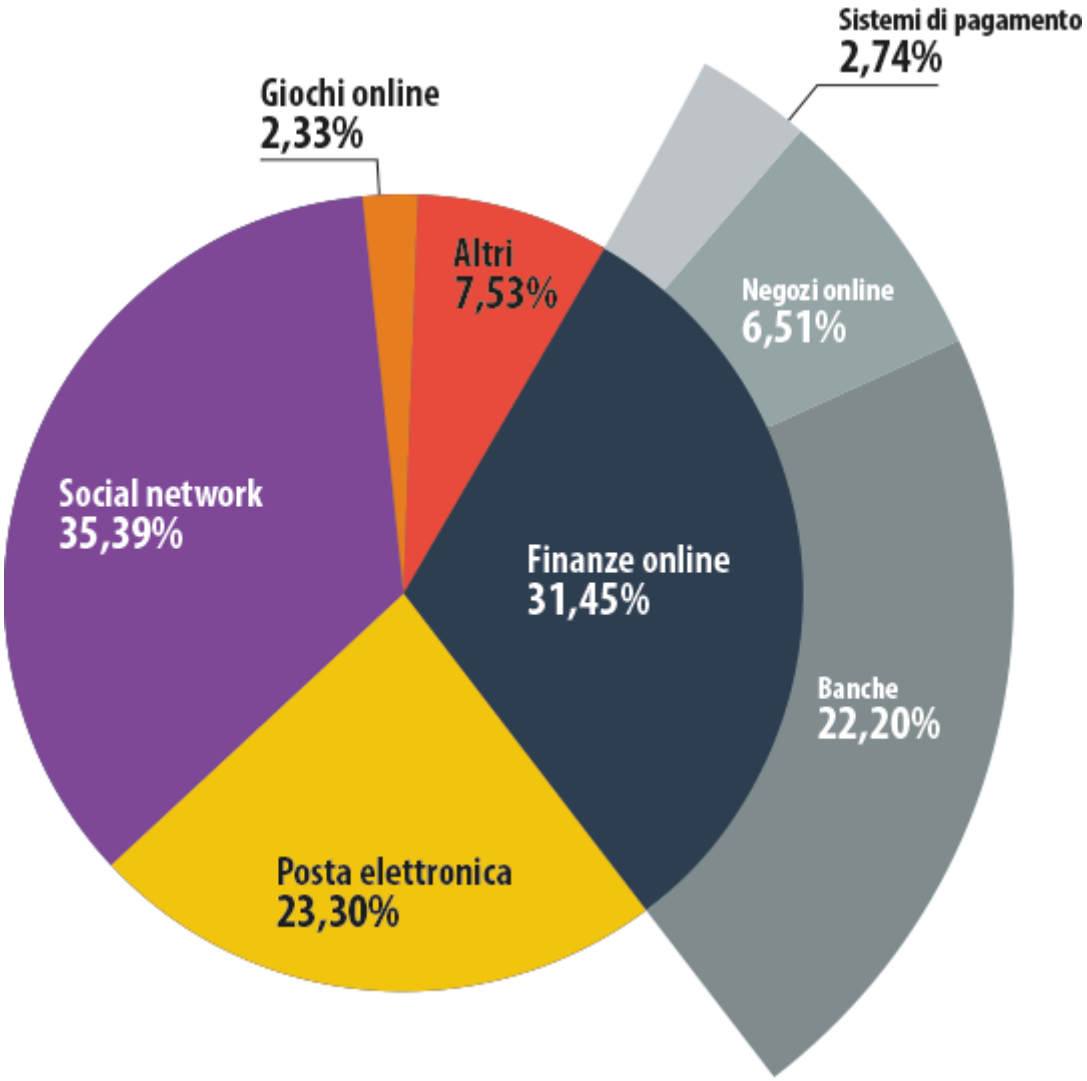
Ricordiamo in primo luogo come, nel 2012, sul 22,95% degli assalti di phishing rilevati sul web - rivolti a tutti i possibili servizi online di natura finanziaria - una quota pari all'11,92% (del volume complessivo degli attacchi allestiti dai phisher) risultasse direttamente riconducibile a siti fasulli preposti ad imitare i siti web ufficiali di istituti bancari e sistemi di banking online. Le quote relative ai siti contraffatti relativi alla categoria dei negozi online e alla categoria dei sistemi pagamento si attestavano invece, rispettivamente, su valori pari al 5,66% e al 5,37%.



Il phishing finanziario nel 2012

Nel 2013, tuttavia, sono intervenuti significativi cambiamenti riguardo alla ripartizione degli attacchi di phishing che hanno direttamente interessato la categoria "Online finance". Rispetto all'anno precedente, la quota attribuibile al phishing rivolto agli istituti bancari è in sostanza raddoppiata, ed ha in tal modo raggiunto un valore totale pari al 22,2%; da parte

sua, l'indice riguardante i negozi online ha evidenziato un lieve aumento, passando dal 5,66% al 6,51%. Per contro, risulta sensibilmente diminuita, in sostanza dimezzata (- 2,63%) la quota relativa ai sistemi di pagamento online, che si è così attestata, nel 2013, al 2,74% (sempre sul volume complessivo degli assalti di phishing neutralizzati dalle nostre soluzioni di sicurezza IT). La conclusione che si può immediatamente trarre dall'analisi della situazione descritta è più che evidente: al momento attuale, i truffatori stanno di fatto rivolgendo in misura sempre maggiore le loro attenzioni ai servizi web collegati al settore bancario. Tale tendenza emerge in maniera netta nel quadro delle cyber-minacce esplicitamente connesse alla sfera del phishing.

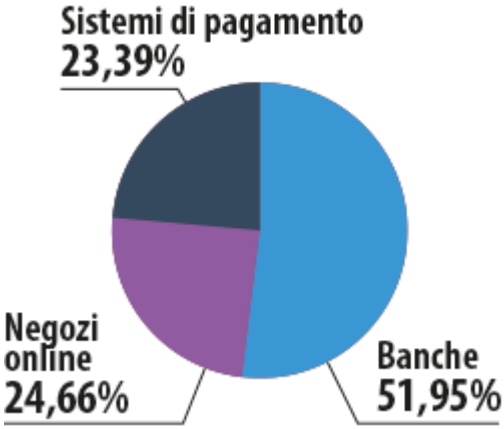


Gli obiettivi del phishing finanziario nel 2013

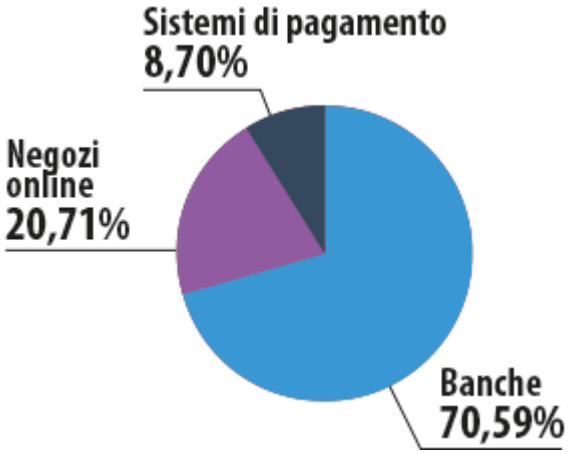
La tendenza evidenziata appare ancor più marcata qualora si vada ad esaminare il fenomeno del phishing finanziario in maniera separata rispetto a tutte le altre rimanenti categorie sottoposte agli attacchi dei phisher. Nel 2013, il 70,59% del volume complessivo

dei rilevamenti eseguiti dal sistema anti-phishing web di Kaspersky Lab relativamente alla categoria "Online Finance" ha riguardato pagine web fasulle volte ad imitare le pagine Internet ufficiali degli istituti bancari; nell'anno precedente, invece, la quota relativa al phishing di natura "bancaria" - nel quadro globale delle minacce IT ascrivibili al phishing "finanziario" - si era attestata su un valore medio pari al 51,95%.

L'indice riguardante gli attacchi condotti nei confronti dei negozi online è passato dal 24,66% fatto registrare nel 2012 al 20,71% rilevato per il 2013; da parte sua, la quota inerente agli assalti di phishing a danno dei sistemi di pagamento ha evidenziato una netta flessione, scendendo dal 23,39% all' 8,7%.



Ripartizione degli obiettivi del phishing finanziario - Situazione relativa al 2012



Ripartizione degli obiettivi del phishing finanziario - Situazione relativa al 2013

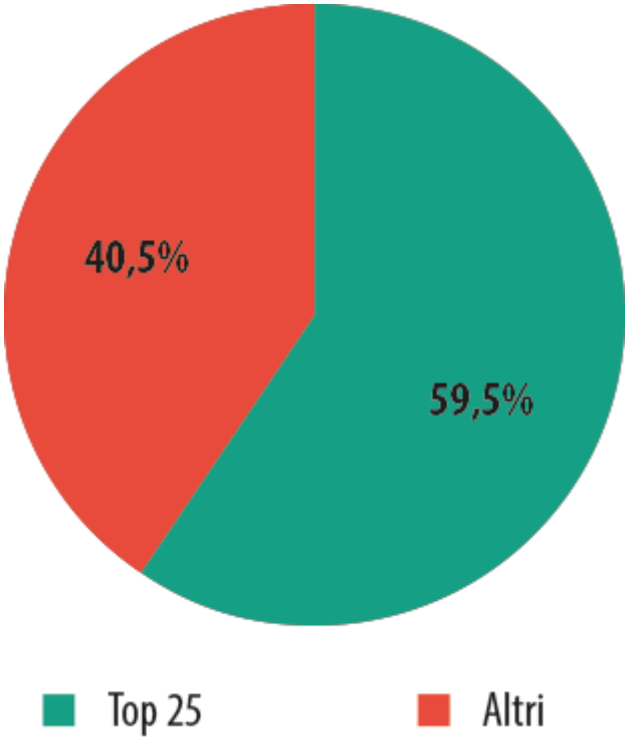
Ulteriori dettagli sugli obiettivi del phishing finanziario

Banche

Sebbene all'interno dei database anti-phishing di Kaspersky Lab siano contenuti oltre mille nominativi di istituti bancari già sottoposti, in passato, ad attacco da parte dei phisher, e di banche che, in ragione della loro popolarità, rischiano, in futuro, di essere prese di mira dai cybercriminali, è chiaramente emerso, a seguito dell'indagine condotta dai nostri esperti, come la stragrande maggioranza degli attacchi di phishing incentrati sull'utilizzo di pagine web fasulle volte a riprodurre le pagine Internet dei siti ufficiali appartenenti ad istituti bancari, abbia sfruttato esclusivamente i nominativi di 25 organizzazioni operanti nel settore bancario.

Nell'anno 2013, come evidenzia il grafico qui sotto riportato, circa il 59,5% del volume complessivo degli attacchi di phishing di natura "bancaria" neutralizzati dalle nostre soluzioni di sicurezza IT ha riguardato proprio i 25 istituti bancari sopra menzionati. Riteniamo doveroso precisare, nella circostanza, come la maggior parte delle banche presenti in tale "ristretto" elenco sia rappresentata da marchi bancari di primaria importanza, diffusi su scala internazionale ed operanti in decine e decine di paesi, in sostanza quasi in ogni angolo del globo. L'ampia diffusione e l'immediata "riconoscibilità" di un determinato brand costituisce

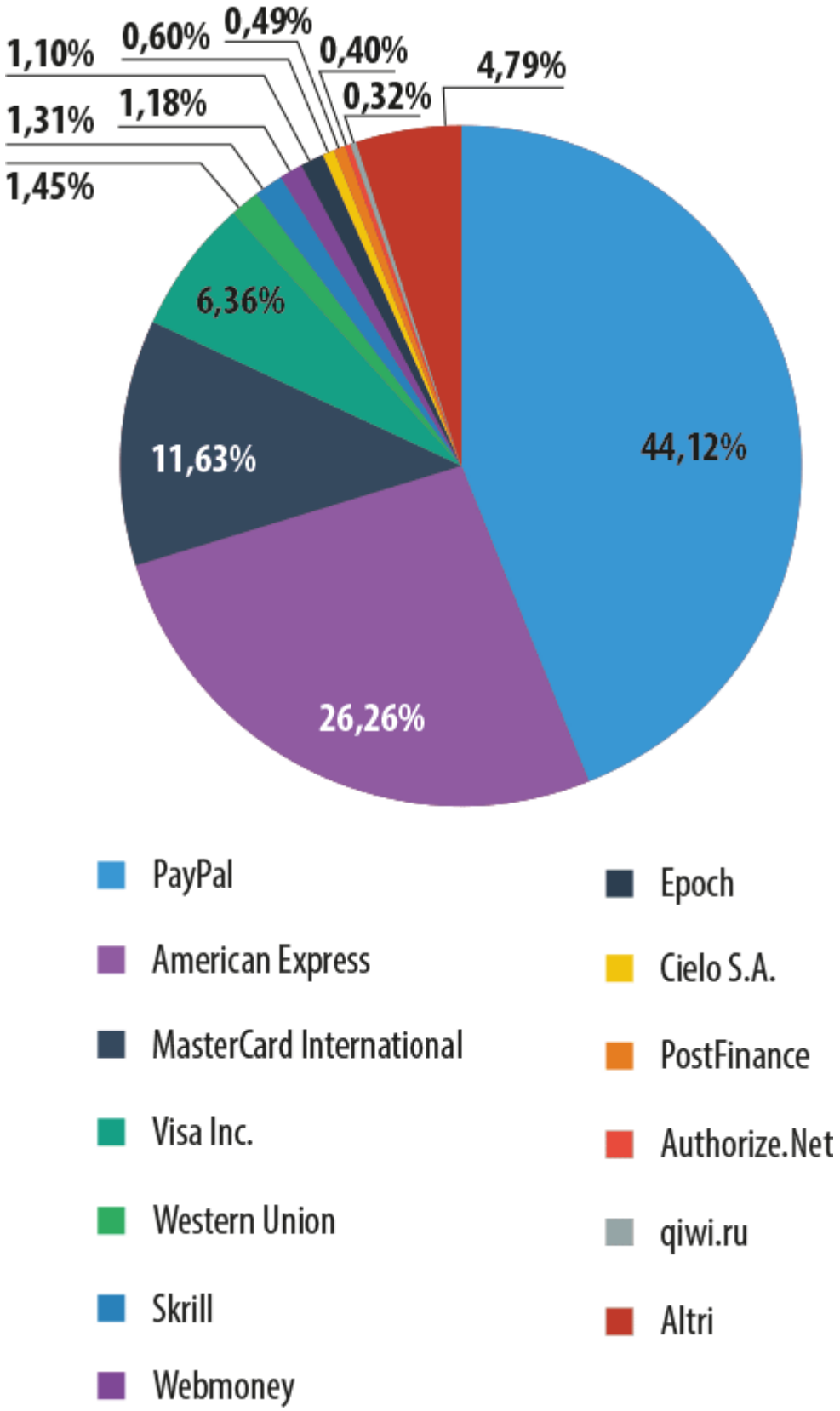
uno dei principali strumenti di cui si avvalgono, di riflesso, i truffatori specializzati nel phishing; in effetti, maggiore è la popolarità di cui gode un marchio presso il pubblico degli utenti, tanto più semplice risulterà, per i cybercriminali, attirare le potenziali vittime del raggiro verso il sito web contraffatto in cui compare tale marchio.



Ripartizione degli attacchi di phishing portati nei confronti delle banche nel corso del 2013

Sistemi di pagamento

Esattamente come nel caso degli attacchi rivolti agli istituti bancari, anche per ciò che riguarda la ripartizione degli assalti di phishing portati nei confronti dei sistemi di pagamento online, svolgono un ruolo determinante il grado di diffusione e la riconoscibilità del brand; basti pensare che quasi il 90% degli attacchi di phishing condotti a danno degli utenti dei sistemi di pagamento ha riguardato i seguenti cinque marchi di caratura internazionale: PayPal, American Express, MasterCard International, Visa e Western Union.

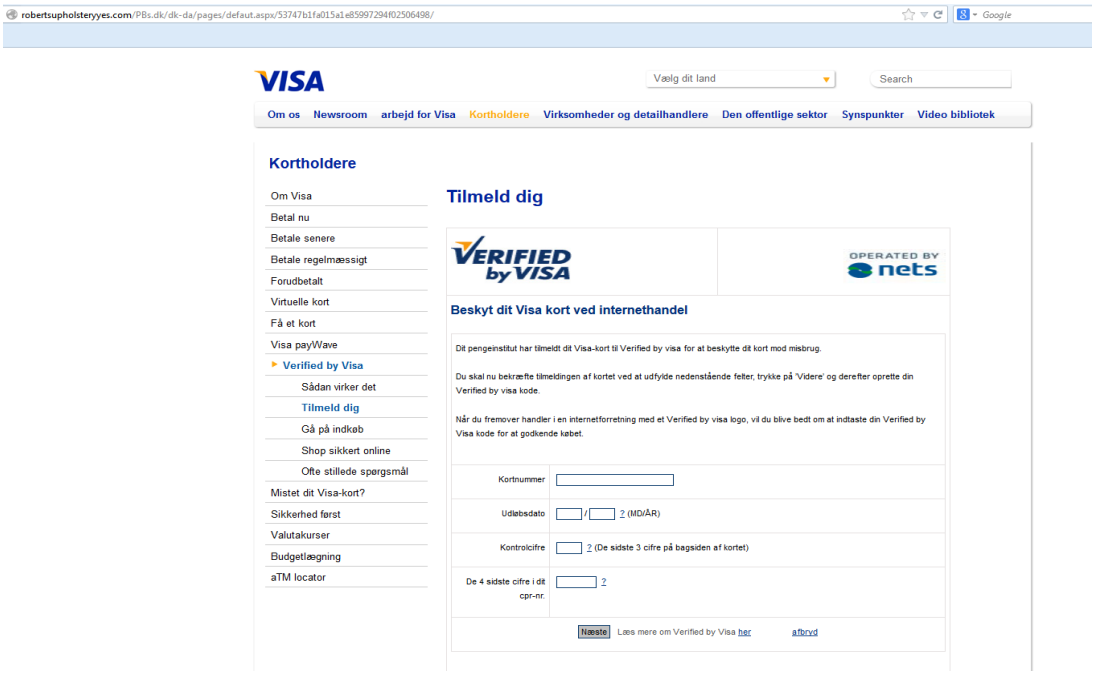


Ripartizione degli attacchi di phishing portati nei confronti dei sistemi di pagamento online nel corso del 2013

PayPal, il diffusissimo sistema che offre ai propri utenti servizi di pagamento online e di trasferimento di denaro attraverso Internet, gode, purtroppo, di uno stabile ed elevato grado di popolarità anche presso i truffatori della rete; il 44,12% degli attacchi di phishing organizzati a danno degli utenti dei sistemi di pagamento online ha in effetti preso di mira proprio la suddetta società.

Esempio di pagina web di phishing preposta ad imitare i contenuti del sito ufficiale del sistema di pagamento PayPal

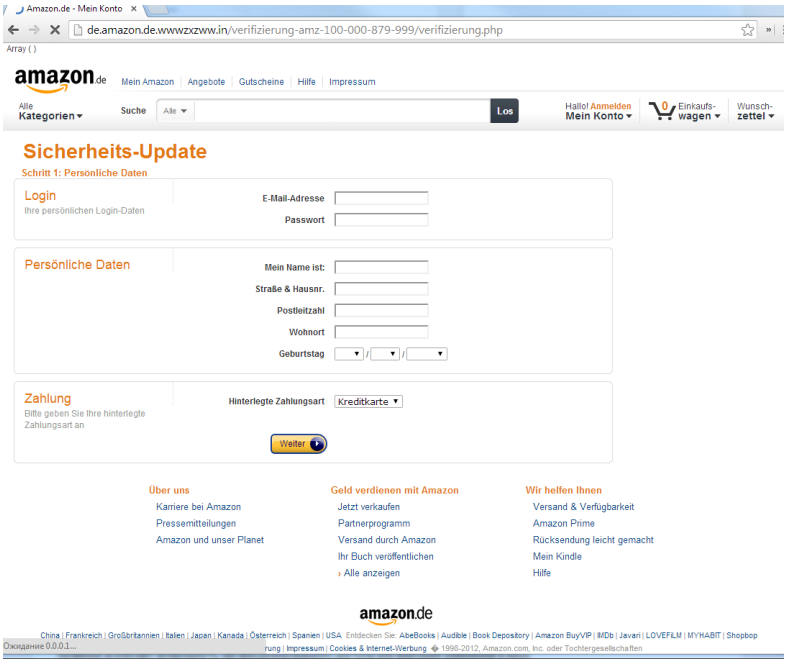
Una quota significativa degli attacchi in questione, pari al 26,26%, ha poi interessato la società American Express. Per contro, le pagine web riconducibili agli altrettanto noti sistemi di pagamento MasterCard International e Visa Inc. sono state falsificate dai malintenzionati in maniera decisamente meno pronunciata; nel 2013, le quote relative agli attacchi di phishing relative a tali sistemi si sono attestate, rispettivamente, su valori pari all' 11,63% e al 6,36% del numero totale degli assalti orditi dai phisher.



Esempio di pagina web di phishing allestita allo scopo di imitare i contenuti del sito ufficiale del sistema di pagamento Visa

Negozi online

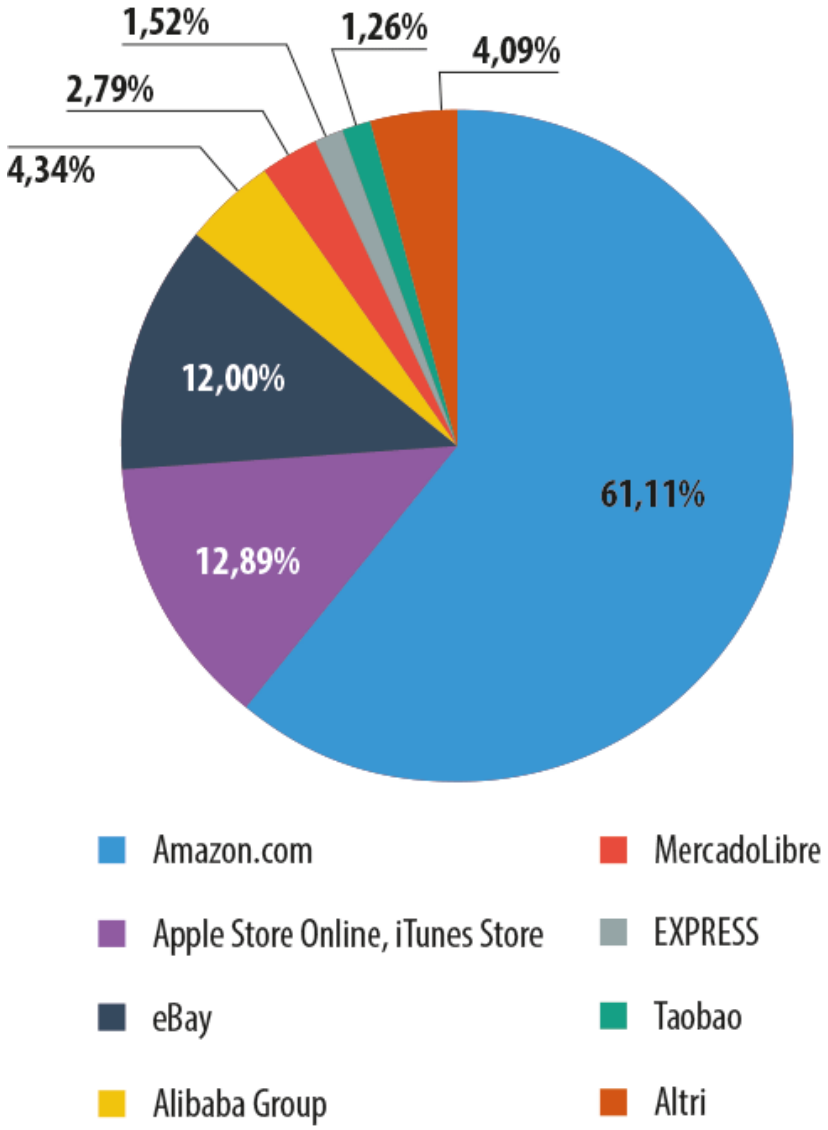
Per quel che riguarda la categoria che raggruppa i negozi online, rileviamo come, ormai da qualche anno a questa parte, la "leadership" per numero di attacchi subiti continui ad essere detenuta, con un ampissimo margine percentuale, dalle pagine web e dai link di phishing che richiamano esplicitamente il nominativo ed il marchio della nota azienda di commercio elettronico Amazon.com (61,11%).



Esempio di pagina web contraffatta volta ad imitare i contenuti del sito ufficiale della piattaforma di e-commerce Amazon, indirizzata agli utenti di lingua tedesca

Essendo il più grande negozio Internet al mondo, in grado di offrire una vastissima gamma di prodotti, Amazon rappresenta indubbiamente un irrinunciabile punto di riferimento per un elevato numero di utenti; ovviamente, è per questo specifico motivo che tale piattaforma di commercio elettronico gode di un costante ed alto livello di popolarità anche presso i malintenzionati specializzati nel creare pagine web fasulle al fine di carpire i dati sensibili degli utenti-vittima.

Come pone in risalto il grafico qui sotto inserito, una significativa quota degli attacchi di phishing condotti nei confronti dei negozi online è relativa al brand Apple (12,89%); nella circostanza, i cybercriminali hanno cercato di imitare le pagine Internet dedicate alla vendita online dei dispositivi Apple, così come le pagine web relative al noto negozio di applicazioni App Store e alla celebre piattaforma di contenuti online iTunes Store.



Ripartizione degli attacchi di phishing portati nei confronti dei negozi online nel corso del 2013

Tra i bersagli prediletti dai phisher, nell'ambito della categoria degli shop online, troviamo poi eBay (12%); la casa di aste più famosa della rete rappresenta, anch'essa, uno degli obiettivi più ambiti di tale specifica tipologia di attacchi di phishing. Si registrano inoltre, sempre più di frequente, attacchi nei confronti di Alibaba (4,34%), l'importante gruppo cinese composto da una serie di compagnie operanti principalmente nella sfera del commercio elettronico (piattaforme di compravendita su scala globale, specifici motori di ricerca dedicati allo shopping, servizi "in-the-cloud"). Nel corso del 2013 è stato rilevato un consistente numero di attacchi di phishing anche a danno dei potenziali utenti di Taobao (1,26%), altra nota piattaforma web cinese dedita all'online shopping. Osserviamo, infine, come quasi il 3% degli attacchi rivolti ai negozi online abbia avuto quale target MercadoLibre.com, l'equivalente latino-americano di eBay. Il diagramma qui sopra riportato pone in risalto, in maniera inequivocabile, l'elevato grado di internazionalizzazione del phishing "finanziario". Risulta quindi del tutto evidente come, al giorno d'oggi, possano divenire vittima degli attacchi organizzati dai phisher non solo gli utenti anglofoni, ma anche persone di madrelingua cinese, spagnola, portoghese, e molte altre ancora.

Peculiarità delle dinamiche degli attacchi di phishing

E' di particolare interesse osservare come le attività di business e di marketing svolte da una determinata società, il cui nominativo viene utilizzato dai malintenzionati per la conduzione di campagne di phishing, influiscano in maniera considerevole sul volume stesso degli attacchi eseguiti.

Tale specifica tendenza può essere dimostrata andando ad esaminare, in qualità di esempio, il grafico relativo agli attacchi in cui i phisher hanno indebitamente sfruttato il nominativo della società Apple e la gamma dei prodotti da quest'ultima lanciati sul mercato globale.

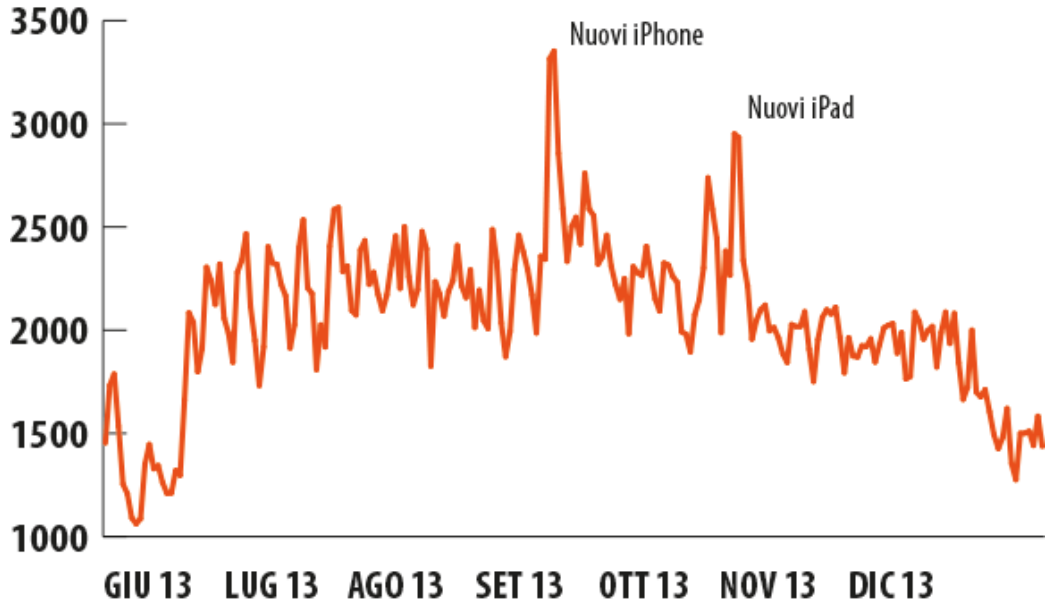


Grafico degli attacchi di phishing in cui è stato sfruttato il brand Apple - Periodo: secondo semestre del 2013

Quasi per tutto l'arco dell'anno oggetto del presente report, le dinamiche inerenti ai rilevamenti eseguiti - grazie alle tecnologie di protezione IT implementate nei prodotti

Kaspersky Lab - nei confronti delle minacce volte a sfruttare il marchio Apple, hanno presentato un'evidente serie di alti e bassi, picchi e repentine cadute, ma sempre entro limiti ben precisi, ovvero dai 1.000 ai 2.500 rilevamenti giornalieri. Tuttavia, come traspare dal grafico qui sopra inserito, nella "storia" di tali attacchi si sono chiaramente registrati due picchi massimi, i quali, come evidenzia la relativa timeline, hanno esattamente coinciso con l'annuncio del rilascio dei nuovi smartphone iPhone 5s e 5c (10 settembre 2013) e dei nuovi tablet iPad Air ed iPad Mini con display Retina (22 ottobre 2013).

In tal caso, la logica che ha "ispirato" l'azione dei truffatori appare bene evidente: le tecnologie Apple rappresentano sempre un tema "caldo" a livello di news e discussioni nell'ambito dei forum Internet, ed in particolar modo proprio alla vigilia degli attesi e consueti annunci riguardo all'immissione sul mercato di nuovi prodotti della Mela. Per i malfattori del phishing, l'utilizzo di parole chiave particolarmente "calde" rappresenta un metodo del tutto abituale nel cercare di attirare un vasto pubblico di utenti verso i siti web fasulli approntati per l'occasione; come emerge in maniera netta dal grafico qui analizzato, tale metodo sembra davvero funzionare alla perfezione.

La società Apple, ad ogni caso, non costituisce di sicuro l'unico bersaglio appetibile per i phisher, tra i potenziali obiettivi nei confronti dei quali il numero degli attacchi portati dai malintenzionati può variare a seconda delle specifiche attività di marketing intraprese dall'azienda oggetto di losche attenzioni. Unitamente alle grandi calamità naturali ed ai principali eventi internazionali, la cui vasta copertura mediatica - assieme alle accese discussioni che di solito vanno ad infiammare i forum su Internet - produce inevitabilmente, di volta in volta, la comparsa del cosiddetto phishing tematico o di appositi mailing di spam, una campagna di marketing di vaste proporzioni - condotta da una banca, un negozio di e-commerce od altra organizzazione operante in ambito commerciale o finanziario - può di sicuro divenire, a sua volta, una buona occasione per lanciare estesi ed insistiti attacchi di phishing.

La conclusione più semplice e logica, suggerita dall'analisi da noi effettuata, è la seguente: per gli istituti bancari, i sistemi di pagamento online e le altre organizzazioni operanti nel settore finanziario, che regolarmente conducono attività di marketing su Internet - in aggiunta alle campagne pubblicitarie abitualmente intraprese per attirare nuovi clienti - sarebbe quantomai necessario avviare specifiche campagne per informare la propria clientela riguardo alle temibili cyber-minacce cui sono potenzialmente sottoposti gli utenti.

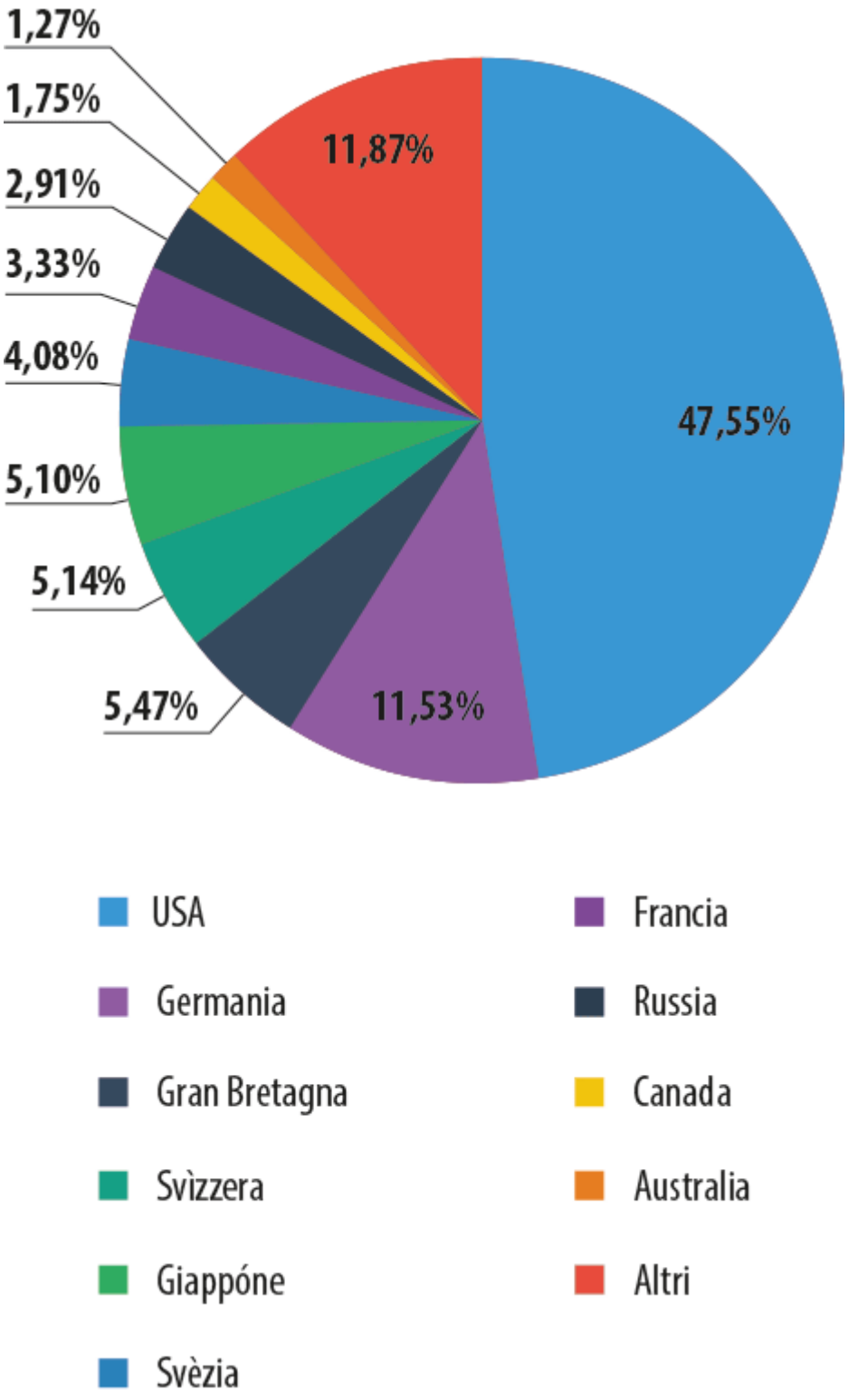
Il phishing nei confronti di OS X: i primi segnali di una crescente minaccia

Il numero degli attacchi informatici portati nei confronti dei proprietari di computer provvisti di sistema operativo OS X è sempre risultato essere di varie volte inferiore rispetto al volume degli assalti IT condotti a danno degli utenti Windows. Tale specifica situazione può essere spiegata in maniera estremamente semplice: sebbene Apple promuova attivamente i propri computer e laptop Mac in ogni angolo del globo, il numero degli utenti che si avvalgono di tali dispositivi non può essere al momento attuale minimamente comparato al numero complessivo dei PC dotati di OS Windows. Pertanto, guidati dal desiderio di massimizzare i profitti, i cybercriminali rivolgono naturalmente maggiori "attenzioni" agli utenti Windows. Tale affermazione risulta ad ogni caso valida soltanto quando si parla specificamente di programmi malware. In effetti, i malintenzionati non debbono davvero far nulla di particolare

o complesso per attaccare gli utenti Mac tramite estese operazioni di phishing. Ovviamente, i sistemi operativi Windows ed OS X presentano differenze fondamentali e sostanziali tra loro, le quali non consentono ai virus writer di poter sviluppare dei malware "universali", in grado di colpire entrambe le piattaforme; tuttavia, sia gli utenti PC che gli utenti Mac, caricano ogni giorno sul proprio browser le medesime pagine web. Per tale motivo, le minacce IT riconducibili alla sfera del phishing, diffuse attraverso i consueti metodi di ingegneria sociale, non risultano di fatto in numero inferiore, per gli utenti della Mela, rispetto alle minacce informatiche potenzialmente rivolte agli utenti dei Personal Computer. I risultati dell'indagine condotta da Kaspersky Lab hanno pienamente confermato tale specifico elemento.

E' ad ogni caso doveroso precisare che, per motivi prettamente tecnici, Kaspersky Lab ha avuto la possibilità di raccogliere i relativi dati statistici, attraverso gli utenti Mac, soltanto a partire dal mese di novembre 2013; pertanto, tutte le informazioni relative agli utenti del sistema operativo Mac OS X, presenti nella ricerca effettuata dai nostri esperti, sono state raccolte nel periodo che comprende i mesi di novembre e dicembre dell'anno 2013. Sebbene il periodo di osservazione risulti indubbiamente limitato, i dati ricevuti in tale intervallo di tempo consentono di potersi comunque fare un'idea piuttosto precisa riguardo al panorama delle minacce IT - legate al phishing - dirette agli utenti della piattaforma OS X, e di rilevare, quindi, significative differenze rispetto al quadro "generale" della situazione.

Annotiamo, in primo luogo, come nel 2013 il 7,8% dei rilevamenti eseguiti grazie alle tecnologie di sicurezza IT da noi sviluppate sia stato realizzato attraverso prodotti Kaspersky Lab appositamente creati per garantire un elevato livello di protezione dei computer Mac. Circa la metà del volume complessivo degli attacchi di phishing ha interessato utenti ubicati sul territorio degli Stati Uniti d'America (47,55%); l' 11,53% di tali attacchi si è poi registrato in Germania, mentre il 5,47% degli stessi ha avuto luogo in Gran Bretagna. Allo stesso modo, sono entrate a far parte dell'elenco dei paesi maggiormente sottoposti agli assalti organizzati dai phisher la Svezia e l'Australia.

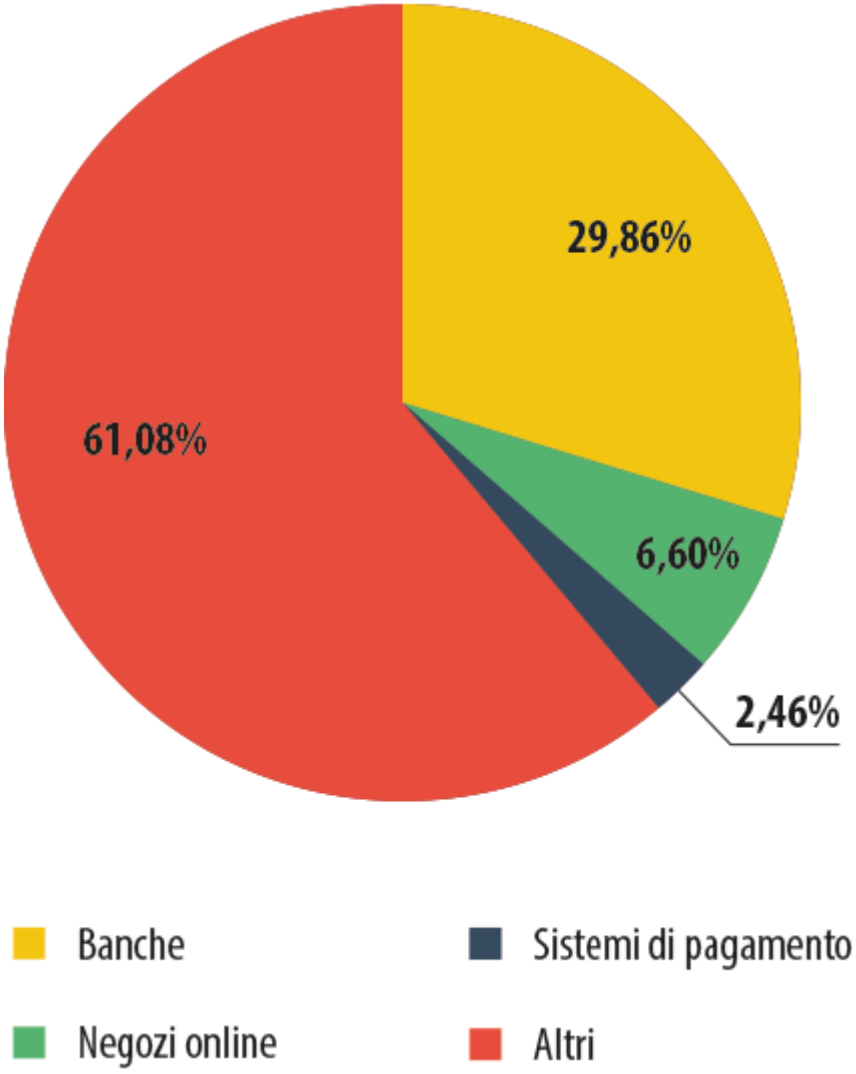


TOP-10 inerente ai paesi attaccati con maggiore frequenza dai phisher - Situazione relativa agli utenti Mac

Le evidenti differenze rilevate riguardo alla ripartizione per paesi di tali attacchi di phishing trovano una logica spiegazione nella maggiore diffusione dei computer Apple proprio all'interno delle nazioni sopra elencate. Non a caso, gli Stati Uniti ed i paesi europei ad alto

tasso di sviluppo tecnologico rappresentano, tradizionalmente, i principali mercati di sbocco per i prodotti rilasciati dalla casa di Cupertino.

Nel periodo analizzato dai nostri esperti, circa il 38,92% del numero totale dei rilevamenti eseguiti sui computer Apple dal modulo Anti-phishing web di Kaspersky Lab ha riguardato pagine web di phishing a chiaro orientamento "finanziario"; tale indice risulta superiore di quasi 7,5 punti percentuali rispetto all'analoga quota "finanziaria" calcolata sul volume complessivo degli attacchi verificatisi. La maggior parte degli incidenti di phishing (29,86%) ha avuto luogo nel momento in cui gli utenti si sono imbattuti in pagine web contraffatte volte ad imitare le pagine Internet presenti nei siti ufficiali di vari istituti bancari; al contempo, il 6,6% dei rilevamenti è risultato riconducibile alla categoria che raggruppa i negozi Internet e le aste online; l'indice relativo ai sistemi di pagamento ha fatto infine registrare un valore pari a 2,46 punti percentuali.



Il phishing finanziario nei confronti degli utenti Mac

Le cifre da noi elaborate sulla base dei dati raccolti evidenziano in maniera inequivocabile come i proprietari dei computer provvisti di sistema operativo Mac debbano fronteggiare gli

attacchi di phishing con la stessa frequenza con cui si imbattono in questi ultimi gli utenti equipaggiati di personal computer dotato di OS Windows. La probabilità di divenire vittima di un attacco di phishing finanziario risulta addirittura superiore proprio per gli utenti che si avvalgono del sistema operativo Mac OS X sviluppato da Apple.

Si conclude qui l'analisi tracciata dagli esperti di Kaspersky Lab riguardo al crescente fenomeno del phishing finanziario, relativamente all'anno 2013. Sebbene il phishing rappresenti indubbiamente, al giorno d'oggi, una minaccia IT alquanto diffusa, quando si parla di atti cybercriminali legati alla sfera finanziaria degli utenti, ci accorgiamo di come tale minaccia appaia ad ogni caso di dimensioni relativamente contenute se confrontata all'estensione globale del vasto panorama delle minacce informatiche connesse all'ambito finanziario. In effetti, all'interno di tale temibile scenario, il ruolo principale viene attualmente svolto da un'ampia gamma di programmi malware a specifico orientamento "finanziario"; si tratta, nella fattispecie, di pericolosi software nocivi in grado di carpire le credenziali di cui si avvalgono gli utenti per accedere ai propri account bancari online; da questi ultimi vengono in tal modo sottratte cospicue somme di denaro, a totale insaputa delle vittime del raggiro. La parte successiva del report da noi stilato riguardo all'evoluzione delle cyber-minacce finanziarie nel corso del 2013 sarà quindi specificamente dedicata all'analisi dei vari aspetti e peculiarità del cosiddetto malware "finanziario".