KASPERSKY lab

Le cyber-minacce «finanziarie» nell'anno 2013. Parte 2: malware

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":

Malware per PC

- Nel 2013, il numero complessivo degli attacchi informatici nel corso dei quali sono stati utilizzati programmi malware preposti al furto di dati sensibili di natura finanziaria ha fatto registrare un incremento pari al 27,6%, raggiungendo in tal modo l'elevata cifra complessiva di 28,4 milioni di assalti IT. Sono risultati sottoposti ad attacco informatico, in totale, 3,8 milioni di utenti; nella circostanza, il tasso di crescita annuale, riguardo a tale parametro, è risultato pari al 18,6%.
- La quota relativa agli utenti divenuti vittima di attacchi di natura finanziaria, condotti tramite il dispiegamento di temibili programmi dannosi da parte dei cybercriminali, si è attestata, nel 2013, su un valore medio pari al 6,2% del numero complessivo di utenti PC sottoposti ad attacco informatico. Rispetto al 2012, tale indice evidenzia un incremento di 1,3 punti percentuali.
- E' stato rilevato, dagli esperti di Kaspersky Lab, come, nell'ambito dei software nocivi ad orientamento tipicamente "finanziario", si siano sviluppati in maniera particolarmente attiva quegli strumenti dannosi legati all'impetuoso sviluppo del Bitcoin, la nota criptovaluta globale. Il ruolo principale, per ciò che riguarda tale specifica tipologia di malware, continua tuttavia ad essere svolto, così come negli anni passati, dai software nocivi appositamente creati per sottrarre cospicue somme di denaro dagli account bancari degli utenti-vittima, quali, ad esempio, il famigerato malware Zeus.

Malware mobile

- Nel secondo semestre del 2013, all'interno della "collezione" di Kaspersky Lab, il numero delle applicazioni nocive destinate ai dispositivi mobili provvisti di OS Android - preposte al furto dei dati sensibili legati alle risorse finanziarie degli utenti - si è quasi quintuplicato, passando dai 265 sample di malware presenti nel mese di giugno, ai 1.321 sample di software nocivo "mobile" complessivamente rilevati entro la fine del mese di dicembre.
- Nel corso del 2013 sono stati individuati dai nostri esperti, per la prima volta, programmi Trojan specificamente rivolti alla piattaforma Android in grado di sottrarre denaro dai conti bancari degli utenti sottoposti ad attacco informatico.

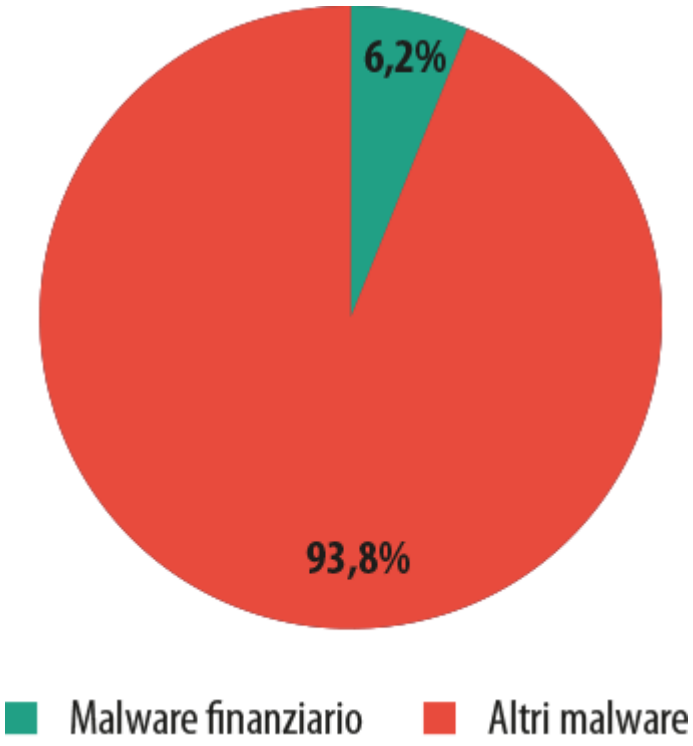
Nei successivi capitoli del report da noi stilato provvederemo ad esaminare in dettaglio le dinamiche degli attacchi "finanziari" che hanno maggiormente contrassegnato l'anno 2013, così come la geografia degli stessi e gli obiettivi da essi presi di mira.

Il malware finanziario

I programmi appositamente sviluppati dai virus writer per eseguire il furto di denaro "elettronico" e per carpire informazioni sensibili di natura finanziaria rappresentano indubbiamente una delle tipologie di malware più sofisticate e complesse. Tale categoria di software nocivi consente ai cybercriminali di convertire rapidamente gli "sforzi" da essi profusi in cospicui profitti; è per tale motivo che i criminali della Rete non risparmiano certamente le proprie forze ed i mezzi finanziari di cui dispongono per creare e poi sfruttare - nella conduzione di attività illecite legate al crimine informatico - temibili programmi malware riconducibili alla specifica tipologia che comprende i trojan ed i backdoor "finanziari". E' stato ad esempio osservato a più riprese, dagli esperti di Kaspersky Lab, come gli autori di software nocivi siano di fatto disposti a sborsare decine di migliaia di dollari per ottenere informazioni riguardo alle nuove vulnerabilità via via individuate in applicazioni e sistemi operativi, con il preciso intento di eludere poi l'azione protettiva svolta dai prodotti anti-malware e surclassare, in tal modo, la sempre nutrita concorrenza cybercriminale, anch'essa impegnata ad escogitare nuove e sempre più temibili minacce IT.

Complessivamente, lungo tutto l'arco del 2013, le soluzioni di sicurezza IT sviluppate da Kaspersky Lab hanno neutralizzato 28,4 milioni di attacchi informatici nel corso dei quali sono stati dispiegati, dai criminali, programmi malware specificamente volti a sottrarre agli utenti le risorse finanziarie online di cui questi ultimi dispongono. Sottolineiamo come, rispetto all'anno precedente, il volume totale degli attacchi respinti sia aumentato del 27,6%. Allo stesso modo, ha fatto registrare un sensibile incremento (+ 18,6%), anche il numero degli utenti della Rete complessivamente attaccati mediante l'utilizzo di malware "finanziari", risultato pari a 3,8 milioni. L'indagine condotta dai nostri esperti si è basata sui dati relativi agli attacchi eseguiti mediante trojan bancari, keylogger, programmi malware adibiti al furto dei wallet virtuali Bitcoin e software preposti all'upload, sul computer-vittima, di programmi in grado di generare tale moneta virtuale.

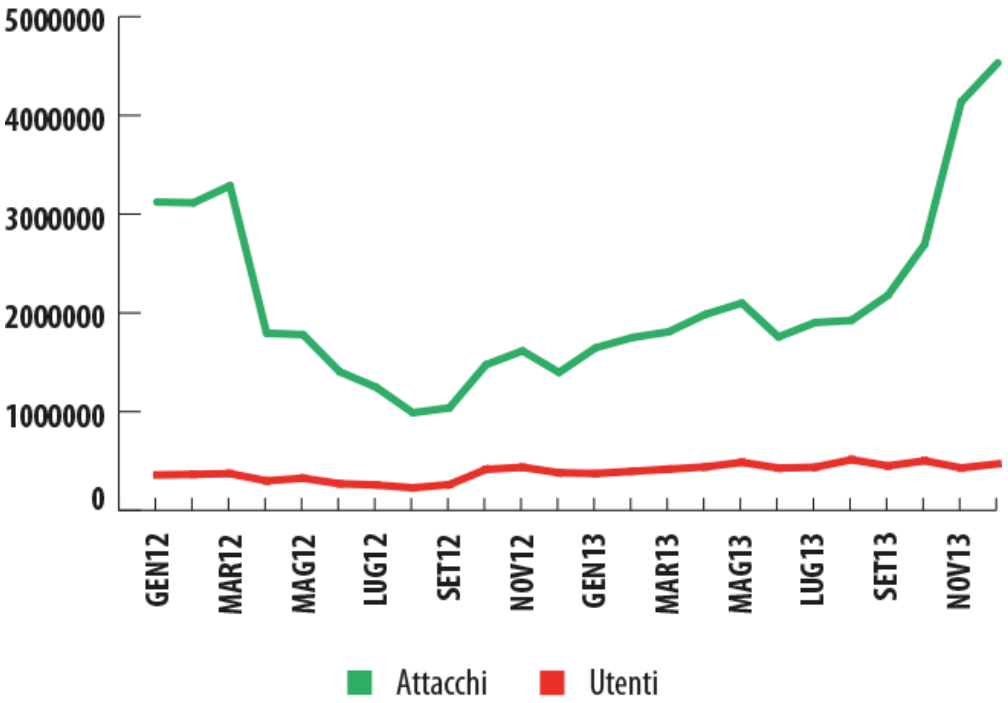
Considerando il numero complessivo degli attacchi nocivi portati dai criminali, rileviamo, in primo luogo, come il "contributo" fornito dai programmi nocivi preposti ad attività cybercriminali inerenti al furto e alla frode, risulti relativamente contenuto; nel 2013, la quota ad esso attribuibile si è attestata su un valore medio pari allo 0,44% del volume totale degli attacchi IT neutralizzati dalle nostre soluzioni anti-malware. Tale indice, ad ogni caso, ha evidenziato un aumento di 0,12 punti percentuali rispetto all'analoga quota riscontrata nell'anno precedente. Se, tuttavia, prendiamo in considerazione il numero degli utenti sottoposti ad attacco, la quota inerente alle minacce informatiche ad orientamento finanziario risulta sensibilmente superiore: secondo i dati da noi raccolti ed elaborati, emerge in effetti come, sul numero complessivo delle persone rimaste vittima, nel corso dell'anno passato, di attacchi da parte di programmi dannosi riconducibili ad ogni possibile tipologia esistente di malware, ben il 6,2% degli utenti coinvolti abbia avuto a che fare con qualche "esemplare" di software nocivo appartenente alla "specie" del malware finanziario. Rispetto al 2012, tale importante indice ha fatto registrare un aumento di 1,3 punti percentuali.



Utenti sottoposti ad attacco nel corso del 2013

Nel 2013, il malware utilizzato per la conduzione di attacchi IT a carattere finanziario ha interessato il 6,2% del numero complessivo di utenti divenuti bersaglio di programmi dannosi

Emerge indubbiamente una correlazione piuttosto flebile tra il numero di attacchi eseguiti ed il numero di utenti interessati dagli stessi. Notiamo, in effetti, come nel periodo 2012-2013 il volume complessivo degli attacchi registratisi mensilmente abbia di frequente subito variazioni quantificabili in decine di punti percentuali. Nella primavera del 2012, ad esempio, tale volume ha evidenziato una forte diminuzione, per poi tornare sui livelli precedenti soltanto nell'autunno del 2013; per contro, il grafico qui sotto riportato pone in risalto come il numero degli utenti sottoposti ad attacco non sia risultato soggetto ad oscillazioni così brusche ed abbia mostrato, mese dopo mese, un andamento "positivo", progressivamente crescente.



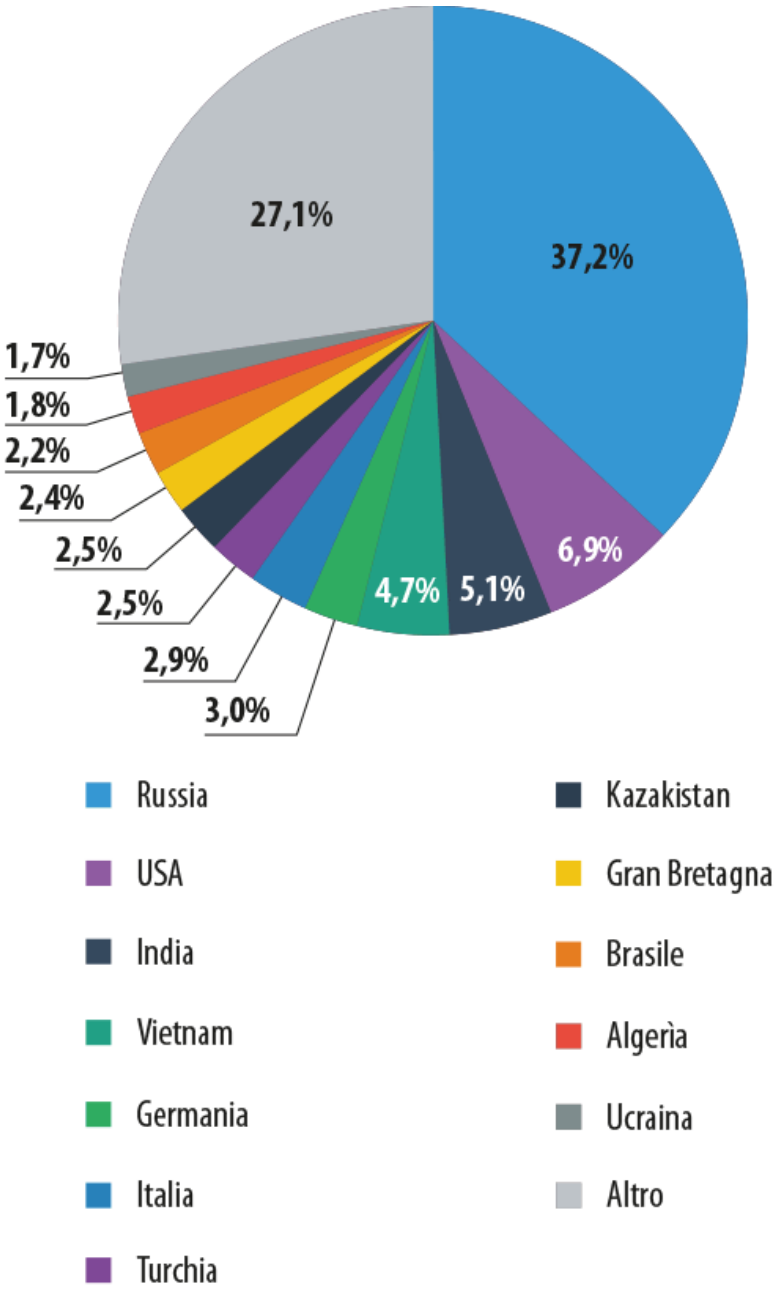
Malware finanziario: numero di attacchi e numero di utenti attaccati a confronto - Periodo: 2012-2013

Nel corso del 2013 abbiamo assistito ad un significativo aumento del numero degli utenti sottoposti ad attacco da parte di programmi malware legati alla sfera finanziaria

La marcata diminuzione del numero degli attacchi verificatisi nella primavera del 2012 può essere probabilmente imputata alla cessazione delle attività illecite in precedenza condotte da alcuni gruppi di cybercriminali. A sua volta, il picco di assalti IT da parte del malware finanziario, registratosi nella seconda metà del 2013, può essere attribuito a vari fattori: i malintenzionati hanno in primo luogo individuato nuove vulnerabilità critiche nella piattaforma Oracle Java; ciò ha evidentemente consentito ai cybercriminali di aumentare sensibilmente l'intensità degli attacchi. Allo stesso modo, a seguito della crescita esponenziale del tasso di cambio del Bitcoin, manifestatasi nella parte finale dell'anno 2013, i criminali hanno "ben" pensato di dispiegare un considerevole numero di programmi nocivi in grado di realizzare il furto degli ambiti wallet elettronici contenenti la celebre criptovaluta.

Le frontiere delle cyber-minacce finanziarie: geografia degli attacchi e degli utenti sottoposti ad attacco

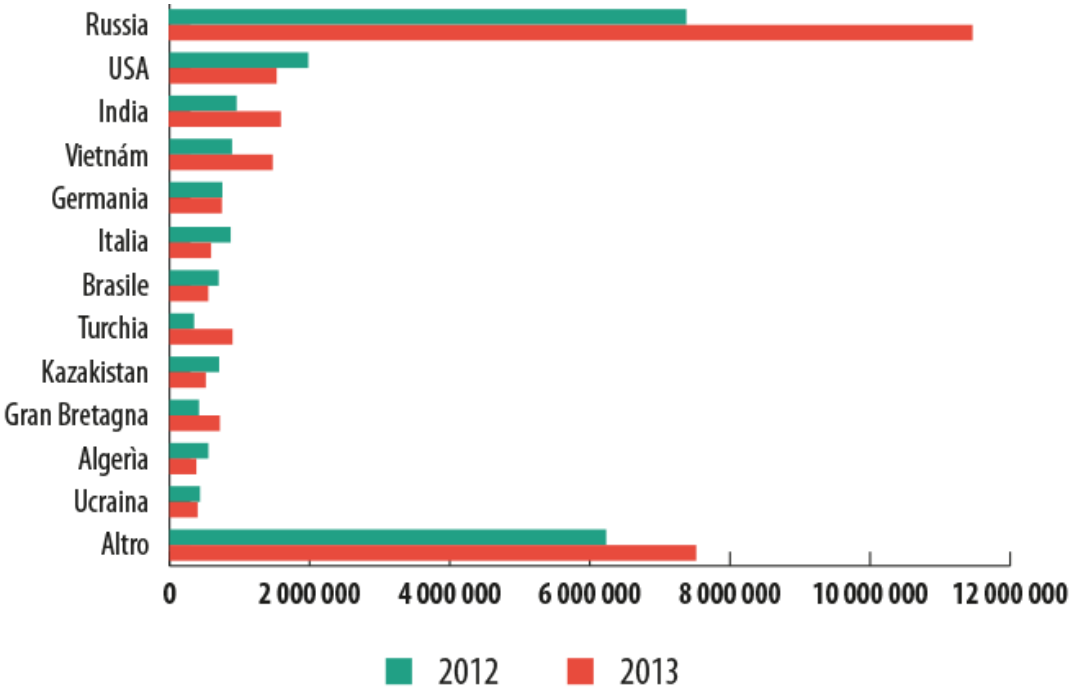
Come evidenzia il grafico qui sotto inserito, la speciale graduatoria relativa ai paesi che, nel corso del biennio 2012-2013, sono risultati più frequentemente sottoposti agli attacchi informatici portati dai truffatori attraverso i temibili programmi malware legati alla sfera finanziaria, è capeggiata dalla Federazione Russa, con un ampio margine percentuale rispetto alle altre nazioni presenti in classifica. La quota ascrivibile agli attacchi effettuati nei confronti degli utenti situati entro i confini del territorio russo si è in effetti attestata su un valore medio decisamente elevato, pari ad oltre il 37%. Basti pensare che, nel periodo preso in considerazione dai nostri analisti, nessuno degli indici attribuibili agli altri paesi presenti nel rating qui analizzato ha superato la soglia dei dieci punti percentuali.



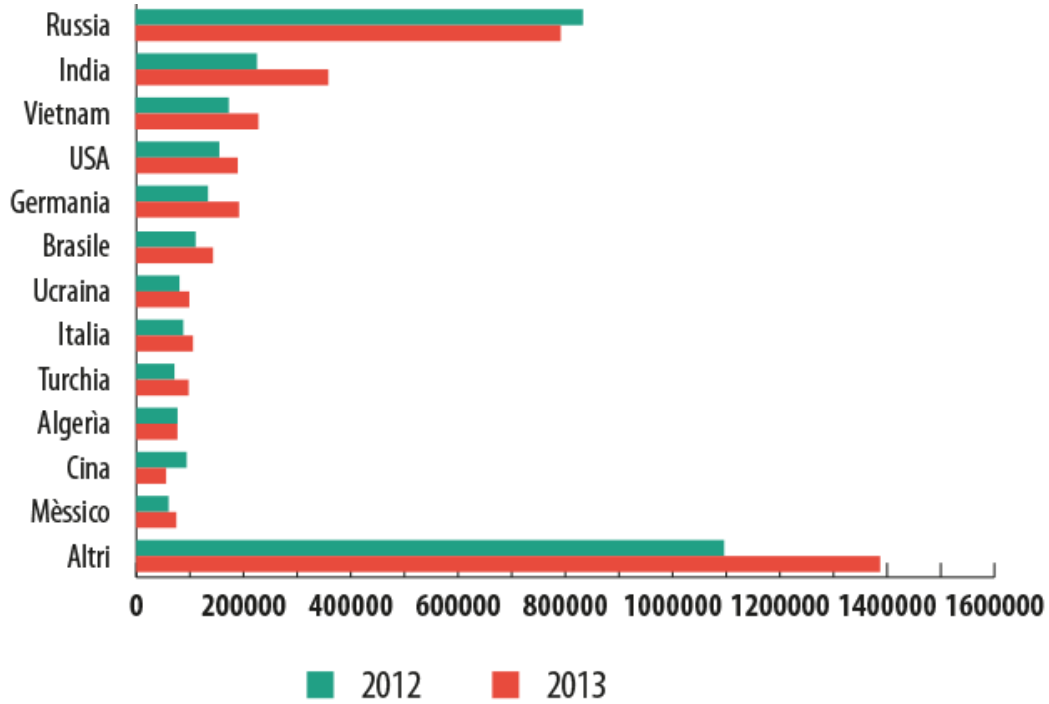
I paesi maggiormente sottoposti agli attacchi nel periodo 2012-2013

Ai primi 10 paesi presenti in graduatoria risulta complessivamente riconducibile circa il 70% del volume totale degli assalti informatici condotti dai cybercriminali, nel corso degli ultimi due anni, mediante l'utilizzo dei famigerati malware finanziari.

La Russia detiene ugualmente la poco invidiabile leadership riguardo al tasso di crescita fatto registrare da tale genere di attacchi informatici nel breve volgere di un anno. E' tuttavia piuttosto singolare rilevare come il numero degli utenti attaccati sul territorio della Federazione Russa nel corso del 2013 sia leggermente diminuito, mentre per la maggior parte degli altri paesi presenti nelle prime dieci posizioni della speciale graduatoria da noi stilata è stato invece riscontrato un significativo aumento del valore di tale indice rispetto al 2012.



Geografia degli attacchi informatici riconducibili al malware finanziario



Geografia degli utenti sottoposti ad attacchi informatici riconducibili al malware finanziario

Nell'arco di un anno, il numero degli utenti sottoposti ad attacchi condotti mediante l'utilizzo di programmi malware di natura finanziaria è risultato in aumento in ben 8 dei 10 paesi che occupano le posizioni di vertice della graduatoria relativa al numero di utenti attaccati in ogni singolo paese

Come evidenzia il grafico qui sopra riportato, sono stati proprio gli utenti ubicati in territorio russo a rischiare più spesso degli altri di essere vittima di attacchi informatici legati alla sfera finanziaria; nel 2013, ogni utente situato entro i confini della Federazione Russa, preso di mira dai malintenzionati dediti al cybercrimine finanziario, è stato in media attaccato da questi ultimi 14,5 volte. Per quel che riguarda gli abitanti degli Stati Uniti, invece, tale indice è mediamente risultato di poco superiore alle 8 volte.

Paese	Numero di attacchi con utilizzo di malware finanziario	Dinamica annuale	Numero di attacchi mediamente subiti da ogni singolo utente
Federazione Russa	11.474.000	55,28%	**14,47**
Turchia	899.000	156,41%	**9,22**
Stati Uniti	1.529.000	-22,76%	**8,08**
Vietnam	1.473.000	65,08%	**6,43**
Kazakhstan	517.000	-26,88%	**6,15**
Italia	593.000	-32,05%	**5,61**
India	1.600.000	65,03%	**4,47**
Ukraina	401.000	-7,54%	**4,07**
Germania	747.000	-0,73%	**3,9**
Brasile	553.000	-21,02%	**3,87**

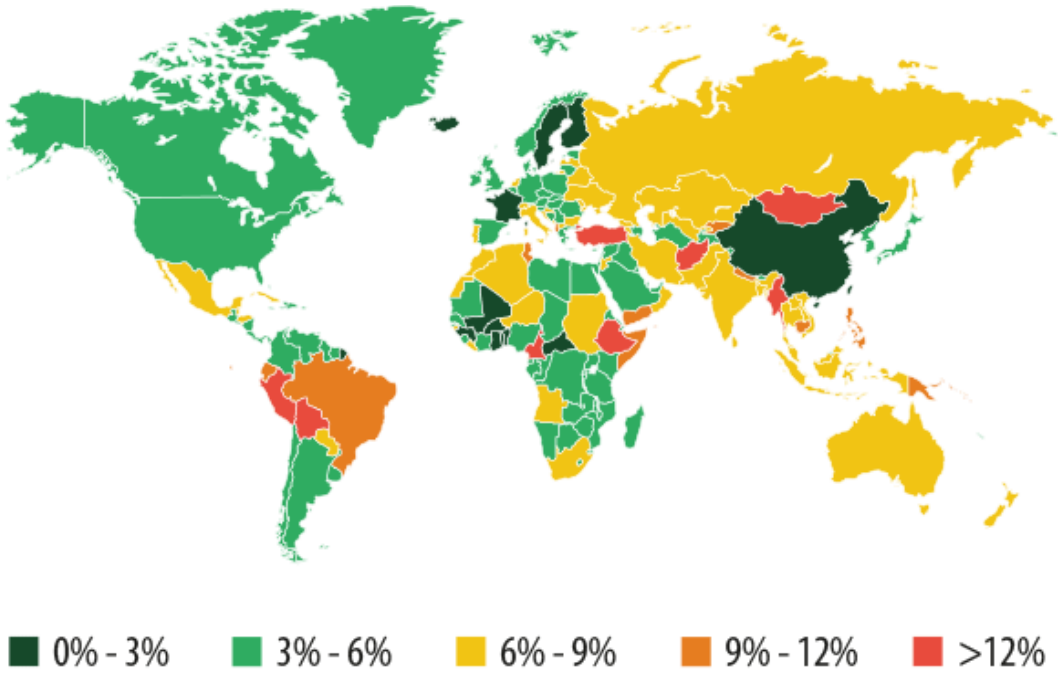
Numero di attacchi mediamente subiti da ogni singolo abitante del paese, divenuto bersaglio, nel corso dell'anno 2013, di attacchi eseguiti mediante l'utilizzo di malware finanziario

Continuando la nostra analisi, rileviamo come la speciale graduatoria relativa al maggior numero di cyberattacchi - verificatisi in un determinato paese - riconducibili alla categoria delle minacce IT legate alla sfera finanziaria degli utenti, risulti capeggiata da Turchia e Brasile. Per questi due paesi, la quota relativa al numero di utenti sottoposti ad attacchi informatici eseguiti mediante il dispiegamento di malware finanziario si è attestata, rispettivamente, su valori pari al 12% e al 10,5% del numero complessivo di utenti che, nel corso del 2013, si sono imbattuti in temibili programmi malware. Per ciò che riguarda la Russia, tale indice è risultato leggermente superiore al 6%, mentre negli Stati Uniti soltanto un utente su trenta, tra quelli complessivamente attaccati dal malware, ha dovuto confrontarsi con cyber-minacce di tipo finanziario.

Paese	Numero di utenti attaccati dal malware finanziario	Dinamica annuale	% sul numero di utenti attaccati da qualsiasi tipo di malware
Turchia	97.000	37,05%	**12,01%**
Brasile	143.000	29,28%	**10,48%**
Kazakhstan	84.000	5,11%	**8,46%**
Italia	105.000	20,49%	**8,39%**
Vietnam	229.000	31,77%	**7,4%**
India	358.000	59,1%	**6,79%**
Federazione Russa	792.000	-4,99%	**6,16%**
Ukraina	98.000	22,73%	**6,08%**
Germania	191.000	43,22%	**5,52%**
Stati Uniti	189.000	22,30%	**3,1%**

Numero di utenti sottoposti ad attacco da parte del malware finanziario nel corso del 2013 e rispettiva quota percentuale sul numero totale degli abitanti del paese che in tale periodo si sono imbattuti in qualsiasi tipo di programma malware

Se andiamo ad esaminare in dettaglio il quadro geografico mondiale notiamo immediatamente come la quota relativa agli attacchi informatici di natura finanziaria sia risultata relativamente contenuta in Cina, Stati Uniti, Canada e numerosi paesi europei. I paesi leader riguardo a tale specifico parametro si trovano sparsi un po' in tutto il globo: segnaliamo in particolar modo, tra di essi, Mongolia, Camerun, Turchia e Perù.

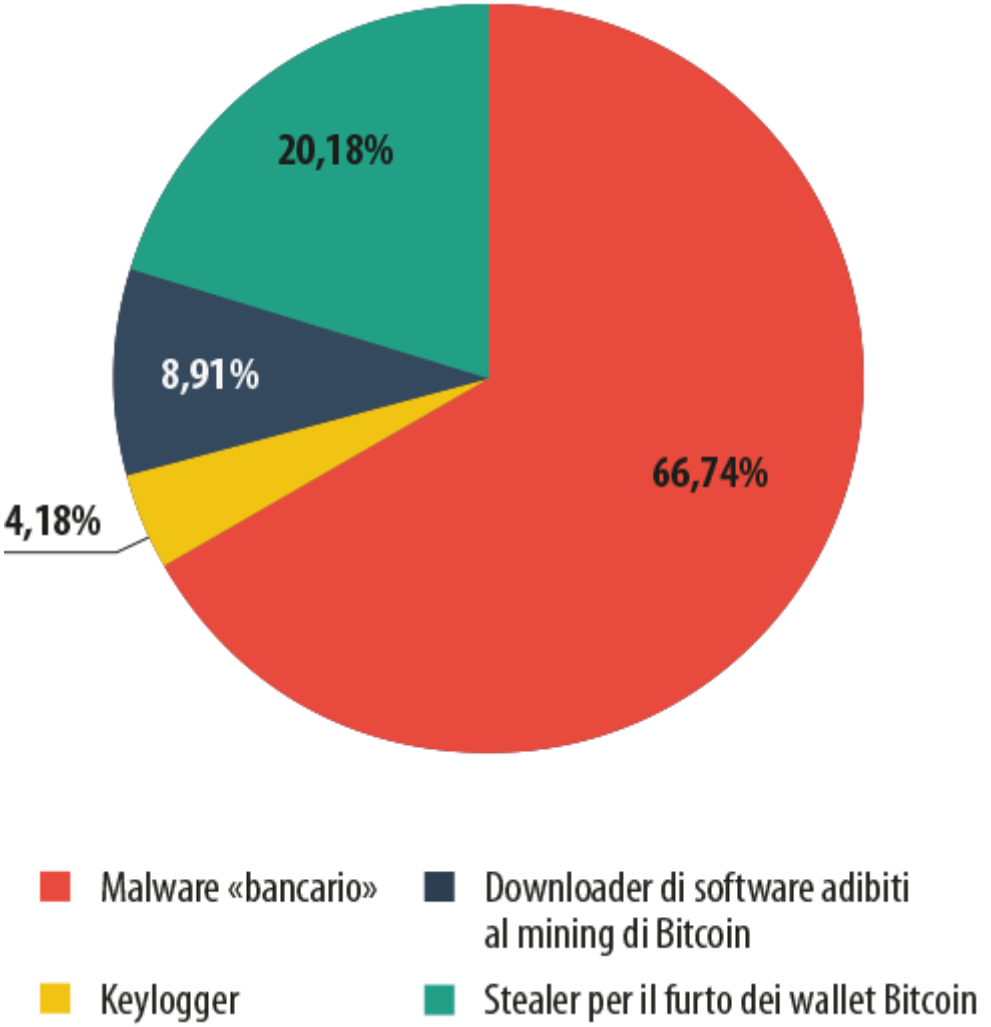


Percentuale di utenti sottoposti ad attacco da parte di programmi malware di tipo finanziario, sul numero totale degli utenti attaccati dal malware - Situazione relativa al 2013

Conosci il tuo nemico: le varie «specie» di malware finanziario

Per comprendere meglio quali tipologie di programma malware, tra quelle appositamente sviluppate dai virus writer per carpire le risorse finanziarie degli utenti, hanno maggiormente contrassegnato, nel corso del 2013, il torbido panorama delle minacce informatiche - gli esperti di Kaspersky Lab hanno innanzitutto suddiviso in varie categorie gli strumenti nocivi utilizzati dai cybercriminali per svolgere tale genere di attività illecite. Per condurre le necessarie analisi, sono stati selezionati oltre trenta sample di software nocivo, tra i malware più frequentemente utilizzati dai truffatori per sferrare gli attacchi riconducibili alla sfera finanziaria. La campionatura eseguita è stata poi suddivisa in quattro gruppi ben distinti tra loro, a seconda delle specifiche funzionalità possedute dai vari programmi nocivi selezionati e degli effettivi scopi che questi ultimi si prefiggono. Gli analisti di Kaspersky Lab hanno così definito le seguenti categorie di malware finanziario: trojan bancari, keylogger, strumenti per realizzare il furto dei wallet virtuali Bitcoin e programmi adibiti al download di software in grado di generare gli stessi Bitcoin.

Il gruppo di gran lunga più numeroso, come evidenzia ampiamente il grafico qui sotto inserito, è rappresentato proprio dai cosiddetti trojan-banker. Tale nutrita "specie" di malware finanziario comprende i programmi trojan e i programmi backdoor preposti a sottrarre cospicue somme di denaro dagli account bancari degli utenti, così come software dannosi di tal genere specificamente progettati per carpire le informazioni sensibili necessarie per la successiva realizzazione del furto a danno degli utenti dei sistemi di banking online. Tra i numerosi malware appartenenti a tale temibile categoria segnaliamo, in primo luogo, i famigerati Zbot, Carberp e SpyEye.



Attacchi informatici con utilizzo di malware finanziario - Situazione relativa al 2013

I rappresentanti della seconda categoria delineata dai nostri esperti, ovvero i keylogger, sono, in sostanza, programmi nocivi preposti al furto dei dati confidenziali custoditi nei computer degli utenti, incluso, ovviamente, le informazioni sensibili direttamente collegate alle finanze online di questi ultimi. Sottolineiamo, a tal proposito, come siano spesso provvisti di funzionalità analoghe gli stessi trojan bancari; per tale motivo, il grado di popolarità dei keylogger, quali strumenti dannosi utilizzati in maniera autonoma, risulta attualmente in fase di declino presso le folte schiere dei truffatori dediti al cybercrimine. Ad ogni caso, i programmi di tal genere maggiormente diffusi sono, al momento attuale, i malware denominati KeyLogger e Ardamax.

Le due rimanenti categorie di malware sono direttamente collegate al mondo del Bitcoin, la celeberrima criptovaluta che, nel corso di questi ultimi due anni, è divenuta suo malgrado un'ambita preda per i criminali specializzati nel cybercrimine finanziario. Tale tipologia di malware comprende, come già accennato in precedenza, sia strumenti dannosi appositamente creati per compiere il furto dei portafogli (wallet) Bitcoin, sia programmi adibiti

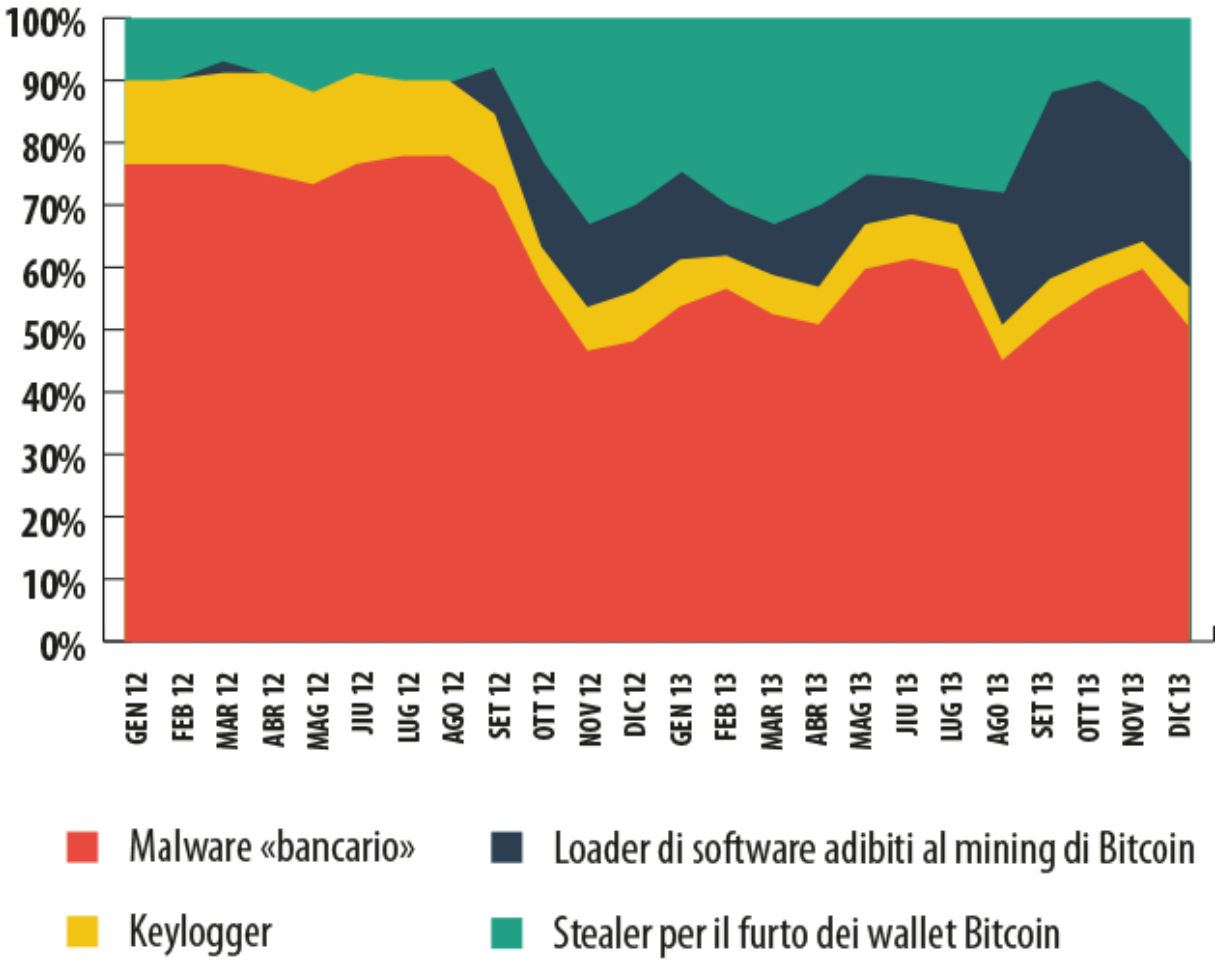
all'installazione sul computer-vittima - a totale insaputa dell'utente preso di mira - di applicazioni in grado di generare tale moneta virtuale (processo comunemente noto con il nome di "mining").

Alla prima "specie" di malware finanziario "dedicato" alla nota criptovaluta appartengono quei software nocivi in grado di realizzare il furto del file wallet, il prezioso contenitore nel quale vengono custodite tutte le informazioni (chiavi) relative ai Bitcoin posseduti dall'utente. La classificazione della seconda specie di malware risulta invece un po' più complessa: in effetti, per realizzare l'installazione di apposite applicazioni adibite alle attività di generazione dei Bitcoin ("mining") può essere in pratica utilizzato qualsiasi malware in grado di effettuare il download, sul computer infetto, di ulteriori programmi, senza che l'utente-vittima possa in qualche modo accorgersi dell'operazione dannosa svolta a suo danno. Per tale motivo, per condurre la nostra analisi, sono stati selezionati esclusivamente quei sample di malware "specializzati" in tale genere di attività, in altre parole i software nocivi visti a più riprese, dagli esperti di Kaspersky Lab, eseguire il download "segreto" e la successiva installazione di strumenti specificamente dedicati al mining.

Riteniamo doveroso puntualizzare, ad ogni caso, che tale suddivisione non implica criteri di precisione assoluta. Il medesimo keylogger, in effetti, può essere impiegato dai malintenzionati sia per carpire dati sensibili di natura finanziaria, sia per eseguire il furto di login e password relativi ad account utilizzati per il gioco online. Di solito, però, i programmi malware presentano comunque qualche particolare "specializzazione", la quale definisce la tipologia predominante di attività illecita svolta - nella specifica circostanza - dai criminali informatici. Ciò consente, quindi, di ricondurre tali software nocivi ad un determinato tipo di attività cybercriminale; nel nostro caso, tale attività criminosa va a colpire direttamente la sfera finanziaria degli utenti.

Gli attacchi condotti con l'utilizzo del malware «bancario»

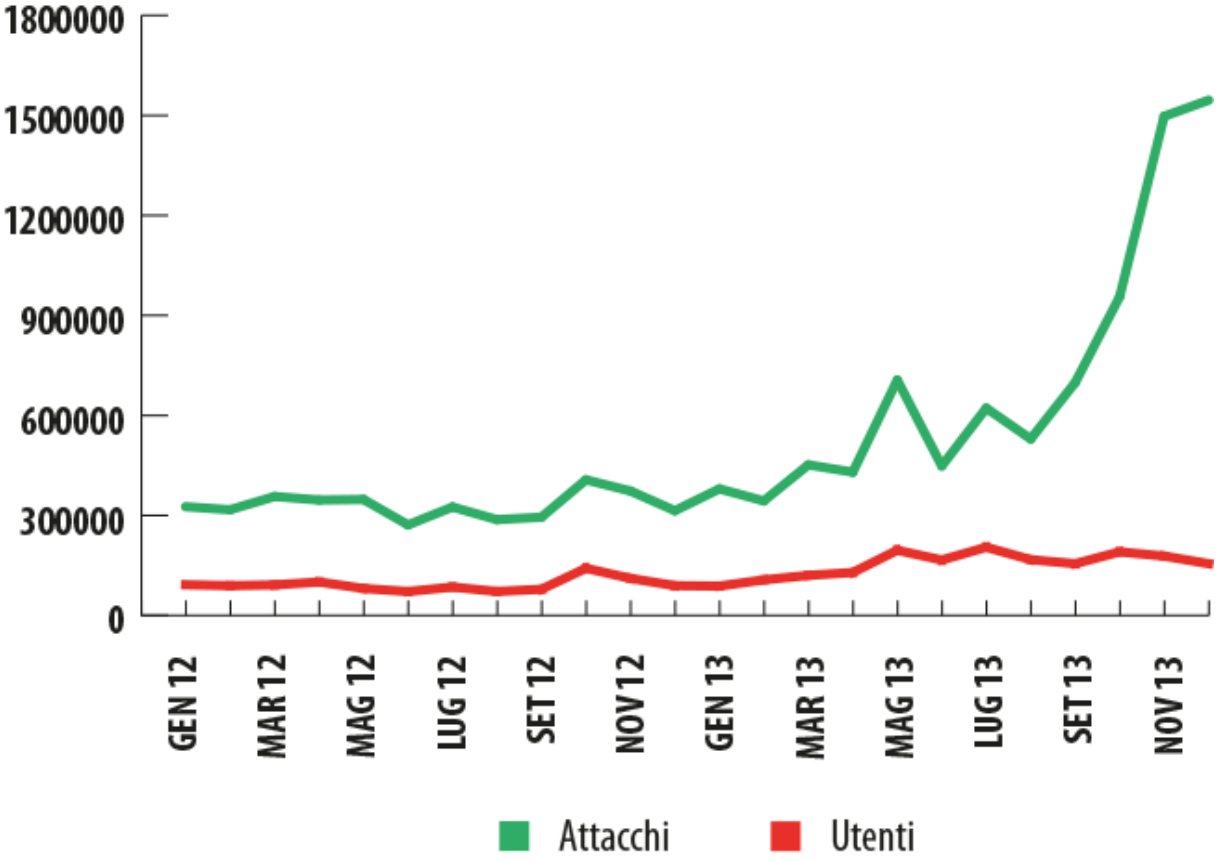
Nel corso del 2013, nel panorama delle cyber-minacce finanziarie globali un ruolo preponderante è stato indubbiamente svolto dai cosiddetti "banker"; si tratta, nella fattispecie, di temibili programmi malware appositamente sviluppati dai virus writer per sottrarre denaro dai conti bancari degli utenti. Nell'arco di un solo anno, sono in effetti risultati riconducibili a tali software dannosi quasi 19 milioni di cyber-attacchi, ovvero i due terzi del volume complessivo degli assalti finanziari condotti mediante l'utilizzo di appositi malware.



Alla fine del 2013 la quota complessiva relativa agli utenti sottoposti mensilmente ad attacchi informatici da parte di programmi malware specializzati nel furto dei Bitcoin e downloader di applicazioni in grado di eseguire attività di mining (generazione di Bitcoin) si è sensibilmente avvicinata alla quota percentuale attribuibile ai banker

Nella sfera del banking malware, il software nocivo in assoluto più attivo si è rivelato essere - sia per numero di attacchi complessivi che per numero totale di utenti sottoposti ad attacco - il programma trojan classificato dagli esperti di sicurezza IT con la denominazione di Zbot (Zeus). Nel volgere di un anno, il numero degli attacchi informatici ascrivibili alle numerose varianti di tale trojan è più che raddoppiato, mentre il numero totale degli utenti attaccati dalle varianti di Zbot ha superato l'indice complessivamente attribuibile agli altri banker presenti

nella speciale TOP-10 da noi stilata.

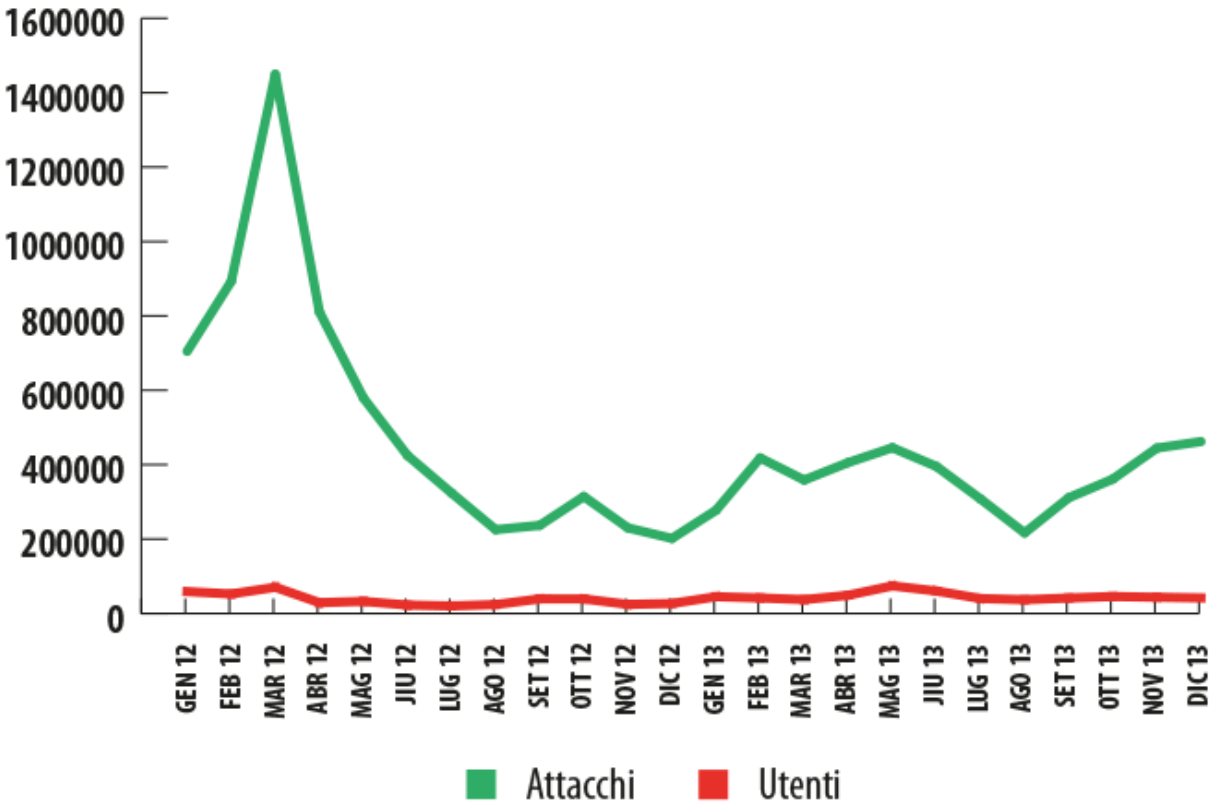


Zbot, 2012-2013

Nel 2011 il codice sorgente del trojan Zbot è stato reso pubblicamente accessibile; sulla base di tale codice sono state successivamente create, e continuano ad essere tuttora create, nuove varianti di tale malware; ciò influisce considerevolmente sui dati statistici complessivi riguardo agli attacchi eseguiti dai cybercriminali mediante il dispiegamento del software nocivo in questione. E' ugualmente noto come, proprio sulla base di Zbot, sia stata inoltre sviluppata la piattaforma Citadel, uno dei più evidenti tentativi di trasferire i principi generalmente applicati al software commerciale a quella sfera che, nello specifico, riguarda la creazione di insidiosi programmi malware. In effetti, agli utenti del sistema Citadel non era riservata soltanto la possibilità di procedere all'acquisto del suddetto trojan; essi avevano ugualmente l'opportunità di beneficiare del supporto tecnico previsto e di ricevere aggiornamenti operativi, appositamente rilasciati per cercare di impedire il rilevamento del programma da parte delle soluzioni antivirus. Allo stesso modo, nell'ambito delle risorse web dedicate alla piattaforma Citadel era stata organizzata una vera e propria community di hacker, i quali potevano in tal modo richiedere o fornire elementi specifici relativi alll'introduzione di nuove funzionalità. All'inizio del mese di giugno 2013, tuttavia, la società Microsoft, in collaborazione con l' FBI, annunciava la chiusura di un elevato numero di estese botnet create sulla base del malware Citadel (con oltre cinque milioni di utenti interessati); ciò ha rappresentato, indiscutibilmente, una significativa ed importante vittoria nel quadro

della dura lotta quotidianamente condotta contro la criminalità informatica. Ad ogni caso, come testimoniano i dati statistici raccolti ed elaborati dagli esperti di Kaspersky Lab, tale eclatante avvenimento non ha influito in maniera così determinante a livello di diffusione del malware specificamente sviluppato per carpire i dati sensibili di natura finanziaria.

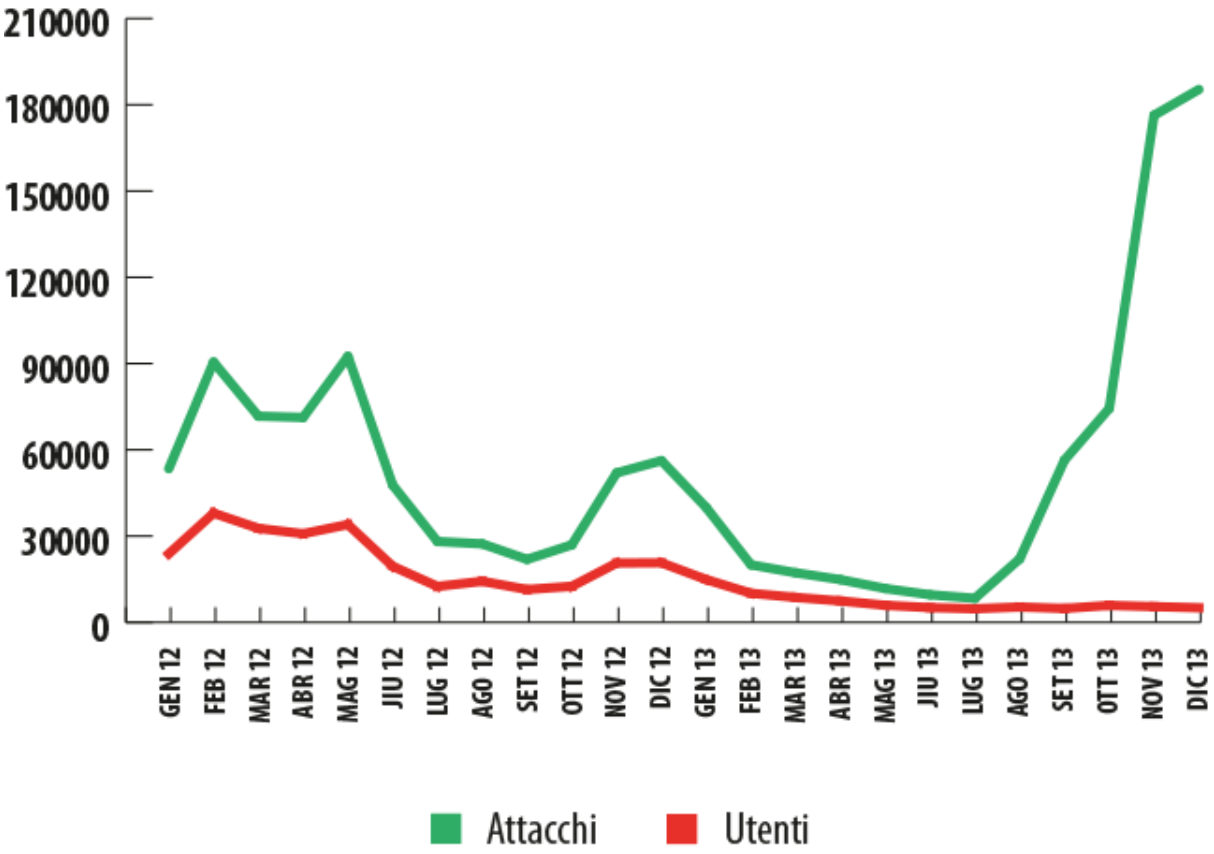
La forte e repentina diminuzione del numero di attacchi informatici imputabili al trojan Qhost può essere a sua volta collegata all'arresto degli autori di tale malware, i quali, nel corso del 2011, si sono resi responsabili del furto di circa 400 mila dollari, sottratti ai clienti di un istituto bancario russo di primaria importanza. I creatori del programma malware in questione sono stati assicurati alla giustizia e quindi condannati già nell'anno 2012; ciò non ha impedito, tuttavia, l'ulteriore diffusione di tale minaccia IT. Di fatto, per ciò che riguarda il suddetto software nocivo, la relativa semplicità a livello di configurazione, unita ad un'evidente facilità di utilizzo, finisce inevitabilmente e costantemente per attirare le attenzioni di nuove schiere di cybercriminali.



Qhost, 2012-2013

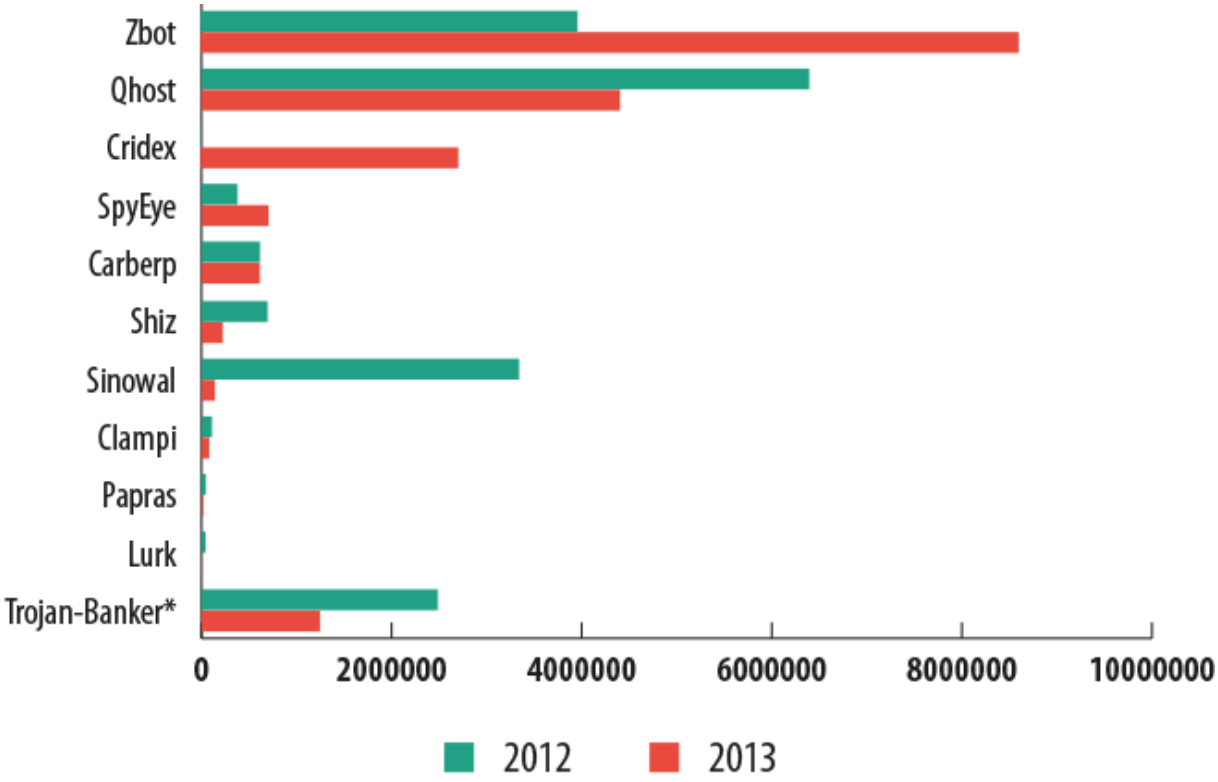
Come evidenzia il grafico qui di seguito inserito, il numero degli attacchi finanziari che hanno visto quale protagonista il trojan Carberp è sensibilmente calato nella prima metà del 2013, dopo l'arresto, avvenuto nella primavera dello scorso anno, di vari utilizzatori del trojan in questione; di tale gruppo di criminali informatici, presumibilmente, facevano parte anche gli stessi autori del malware qui analizzato. A partire dai mesi estivi, tuttavia, si è verificata una significativa crescita del numero degli attacchi condotti attraverso tale programma trojan;

così, la quantità di attacchi complessivamente registratisi nell'anno oggetto del presente report può essere di fatto comparata agli analoghi valori rilevati riguardo all'attività di Carberp nell'anno 2012. L'evidente "performance" fatta segnare nella seconda metà del 2013 è stata di sicuro determinata, tra l'altro, dalla pubblicazione del codice sorgente di tale malware finanziario; il fatto che il codice di Carberp sia stato reso di pubblico dominio ha ovviamente fornito un impulso decisivo per la creazione di nuove versioni del trojan. Ad ogni caso, è di particolare interesse osservare come, nonostante ciò, nell'arco di un solo anno, il numero degli utenti attaccati dalle varianti di tale programma presenti sulla scena del malware globale sia complessivamente diminuito di varie volte.



Carberp, 2012-2013

Nel concludere la nostra breve analisi sull'evoluzione del banking malware nel corso di questi ultimi due anni, sottolineiamo come emerga in maniera chiara ed evidente la tendenza generale che caratterizza l'impiego di tale tipologia di programmi nocivi da parte dei cybercriminali: dopo un periodo di relativa "quiete", manifestatosi nella seconda metà del 2012, nel 2013 i truffatori specializzati nella conduzione di attacchi informatici che prevedono l'utilizzo di malware finanziario hanno notevolmente intensificato le loro attività criminose; lo testimonia, in maniera inequivocabile, il sensibile aumento del numero totale degli attacchi e del numero degli utenti complessivamente sottoposti a tale genere di attacco informatico.



Numero di attacchi con utilizzo di malware bancari: 2012 e 2013 a confronto

** Trojan-Banker è una firma universale utilizzata nei database di Kaspersky Lab; essa si avvale di metodi euristici per effettuare il rilevamento del malware finanziario*

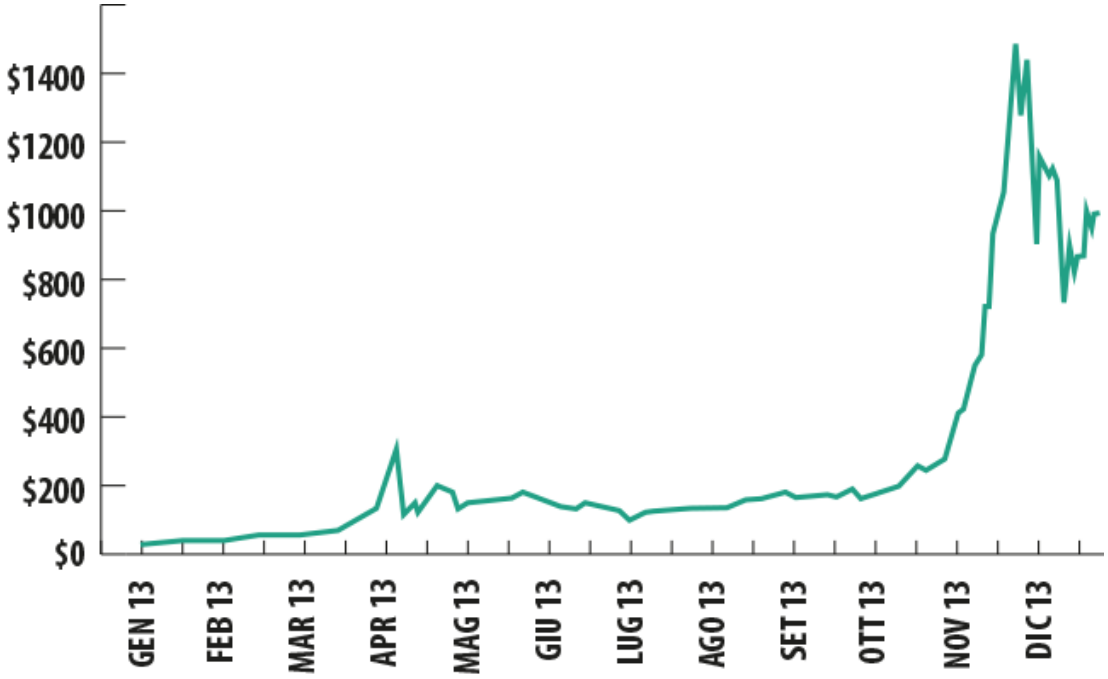
Bitcoin, moneta virtuale a rischio

Il nome Bitcoin identifica una criptovaluta elettronica attualmente molto diffusa, in grado di "funzionare" senza alcun tipo di regolamentazione statale; si tratta, in sostanza, di una moneta virtuale appositamente creata per poter operare esclusivamente attraverso la rete capillare composta dalle persone che ne fanno abitualmente uso. La valuta digitale Bitcoin, come è noto, è stata lanciata nell'anno 2009 da un programmatore e matematico giapponese, conosciuto con lo pseudonimo di Satoshi Nakamoto. Inizialmente, la celebre moneta elettronica veniva utilizzata soltanto da una ristretta cerchia di persone operanti nel settore dell'Information Technology; progressivamente, tuttavia, il Bitcoin ha acquisito un'indiscussa popolarità ed un pubblico di utenti sempre più vasto, in ogni angolo del globo. E' doveroso ad ogni caso sottolineare come, nei primi tempi, abbia contribuito alla crescente diffusione del Bitcoin il fatto che, attraverso tale criptovaluta, risultava possibile effettuare operazioni di pagamento nell'ambito di alcuni siti web molto frequentati, principalmente adibiti alla vendita di prodotti e servizi illegali. Tale specifico orientamento iniziale a livello di utilizzo della valuta elettronica in questione non appare per nulla casuale, in quanto il sistema Bitcoin prevede, di per se stesso, il possesso ed il trasferimento anonimo delle monete virtuali così denominate.

Esempio di portafoglio Bitcoin stampato su carta (variante della versione virtuale del wallet)

In teoria, può ottenere dei Bitcoin chiunque lo desideri, semplicemente sfruttando la potenza di calcolo del proprio computer; l'attività di generazione della nota criptovaluta viene tradizionalmente definita con il nome di "mining", termine che richiama il processo di estrazione dell'oro in miniera. L'essenza del mining è costituita dallo svolgimento di una serie di task di natura crittografica, su cui si basa il funzionamento stesso della rete Bitcoin.

Molti degli utenti che, al momento attuale, risultano particolarmente "ricchi" in Bitcoin hanno costruito la propria "fortuna" già nell'immediata fase successiva alla creazione di tale valuta elettronica, quando il Bitcoin non era ancora ufficialmente riconosciuto come strumento di liquidità monetaria. Ad ogni caso, con la crescente popolarità acquisita dalla criptovaluta in questione, è di fatto divenuto sempre più complesso poter ricavare i preziosi Bitcoin con la sola potenza di calcolo del computer di cui si dispone; ciò è dovuto, essenzialmente, ad una delle principali peculiarità su cui si fonda tale sistema, in quanto è previsto, a tutti gli effetti, un limite massimo al numero totale di Bitcoin che possono essere in circolazione. Al momento attuale, la complessità che presentano i calcoli necessari per realizzare il processo di mining è divenuta così elevata al punto che l'attività di generazione di Bitcoin su computer ordinari risulta ormai tutt'altro che redditizia; il potenziale profitto che si può ottenere attraverso il mining è in effetti in grado di coprire a stento le spese che si devono comunque affrontare per il costo dell'energia elettrica.



All'inizio del 2013 il corso del Bitcoin si situava a quota 13,6 dollari; a dicembre dello stesso anno la criptomoneta ha raggiunto il proprio massimo storico, superando i 1.200 dollari

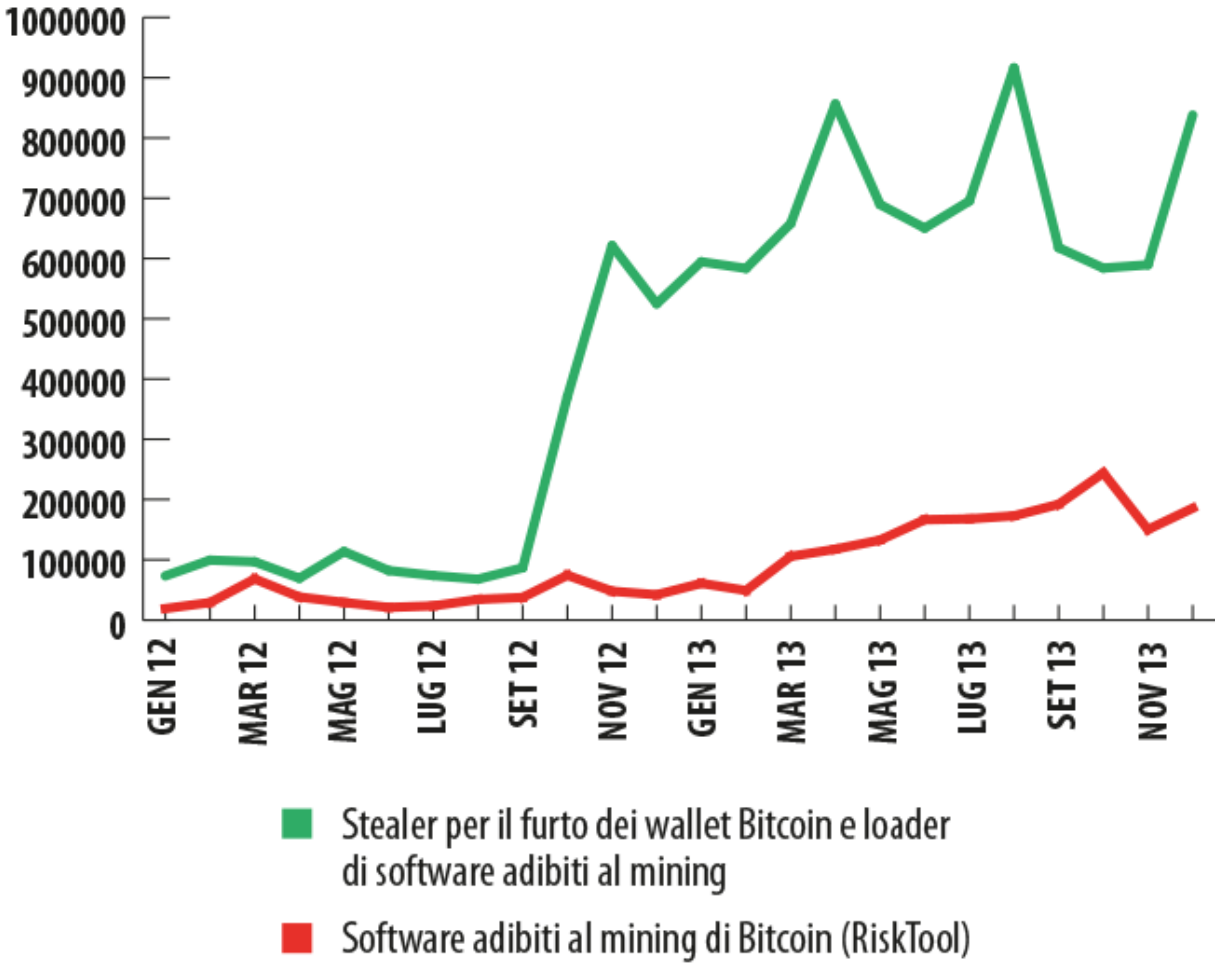
Nel corso dell'anno oggetto del presente report il corso del Bitcoin è cresciuto in maniera esponenziale, superando addirittura, alla fine di dicembre, il valore di 1.200 dollari USA. Dopo tale inatteso exploit, il corso della celebre criptovaluta ha vissuto una fase di declino, anche a causa di una certa diffidenza manifestata nei confronti di quest'ultima da parte delle banche centrali di tutta una serie di paesi. Ad esempio, il rifiuto espressamente pronunciato dalla Banca Popolare Cinese (la banca centrale della Repubblica Popolare Cinese) riguardo all'esecuzione di operazioni finanziarie con le varie borse Bitcoin esistenti ha fatto sì che il valore della valuta digitale venisse rapidamente abbattuto di circa di un terzo. Altre nazioni, tuttavia, hanno adottato un atteggiamento particolarmente "benevolo" nei confronti del Bitcoin: il Ministero delle Finanze tedesco, ad esempio, ha ufficialmente riconosciuto la nota criptovaluta come strumento di pagamento a tutti gli effetti; in Canada e negli Stati Uniti, poi, sono stati addirittura installati appositi apparecchi bancomat per consentire di incassare i Bitcoin, trasformando gli stessi in contanti.

Riassumendo, nel breve volgere di qualche anno, da fenomeno Internet quasi esclusivamente "da camera", ad appannaggio di una ristretta cerchia di appassionati, il Bitcoin si è trasformato, se non proprio in una effettiva unità monetaria, perlomeno in un'entità virtuale provvista di valore reale, e quindi soggetta ad una domanda particolarmente elevata. Naturalmente, una simile "ghiotta" situazione non poteva certo non attirare le losche attenzioni di numerosi malintenzionati. Di fatto, dal momento in cui si è iniziato ad operare con il Bitcoin come moneta "reale" nell'ambito di alcune note piattaforme di trading online, ed un numero sempre maggiore di venditori ha cominciato ad accettare la nota valuta digitale come effettiva forma di pagamento per merci e servizi - i cybercriminali hanno manifestato, da parte loro, un interesse sempre crescente e particolarmente attivo nei confronti del Bitcoin.

I Bitcoin vengono in genere custoditi sui computer degli utenti, tramite un apposito file wallet (provvisto di estensione wallet.dat od altro, a seconda dell'applicazione utilizzata per le attività di mining). Se tale file non risulta codificato ed un cybercriminale riesce a sottrarlo al legittimo proprietario, il malintenzionato di turno potrà liberamente ed agevolmente trasferire sul proprio portafoglio virtuale le risorse finanziarie rubate dall'indirizzo bitcoin violato. La rete Bitcoin consente a tutti coloro che vi partecipano di poter accedere alla cronologia delle transazioni finanziarie effettuate da qualsiasi utente; in teoria, risulta possibile venire a sapere su quale altro portafoglio virtuale possano essere stati trasferiti i "soldi" rubati. Il fatto, però, è che il sistema di cryptocurrency al momento più diffuso al mondo non viene in pratica regolato da nessun ente o autorità, governativi o meno, per cui denunciare un eventuale furto subito alle forze dell'ordine risulterebbe semplicemente inutile, per non dire assurdo.

In aggiunta al furto degli ambiti portafogli digitali, i cybercriminali possono compiere un'ulteriore azione illecita riguardo al Bitcoin, ovvero utilizzare i computer delle proprie "vittime" per le attività di mining, più o meno come sono soliti fare certi truffatori per le operazioni di invio di montagne di spam o per compiere altri atti criminosi di analoga portata. Oltre a ciò, sono ugualmente comparsi sulla scena del malware correlato alla celebre moneta elettronica alcuni programmi "estorsori", i quali richiedono il pagamento di un certo importo in Bitcoin per decodificare i dati dell'utente precedentemente criptati.

Il grafico qui sotto inserito pone in evidenza le dinamiche che hanno caratterizzato sia gli attacchi informatici in cui sono stati utilizzati strumenti nocivi per realizzare il furto dei wallet Bitcoin, sia le attività cybercriminali che hanno fatto ricorso a programmi malware "multifunzionali", specializzati nell'installazione, sul computer sottoposto ad attacco, di applicazioni in grado di generare la criptovaluta in questione tramite il processo di mining. In aggiunta a tali casistiche, sono stati ugualmente presi in considerazione quegli eventi in cui è stato comunque effettuato il rilevamento, sul computer dell'utente, di applicazioni adibite al mining dei Bitcoin; si tratta, nella circostanza, sia di quei programmi che possono essere stati installati dagli stessi utenti, sia di quelle applicazioni caricate sul computer-vittima a totale insaputa di questi ultimi. I prodotti Kaspersky Lab associano le applicazioni impiegate per lo svolgimento di attività di mining alla specifica categoria denominata RiskTool. Ciò significa che l'applicazione in tal modo classificata è provvista di funzionalità potenzialmente dannose, per cui l'utente viene debitamente messo in guardia relativamente alla situazione in atto.

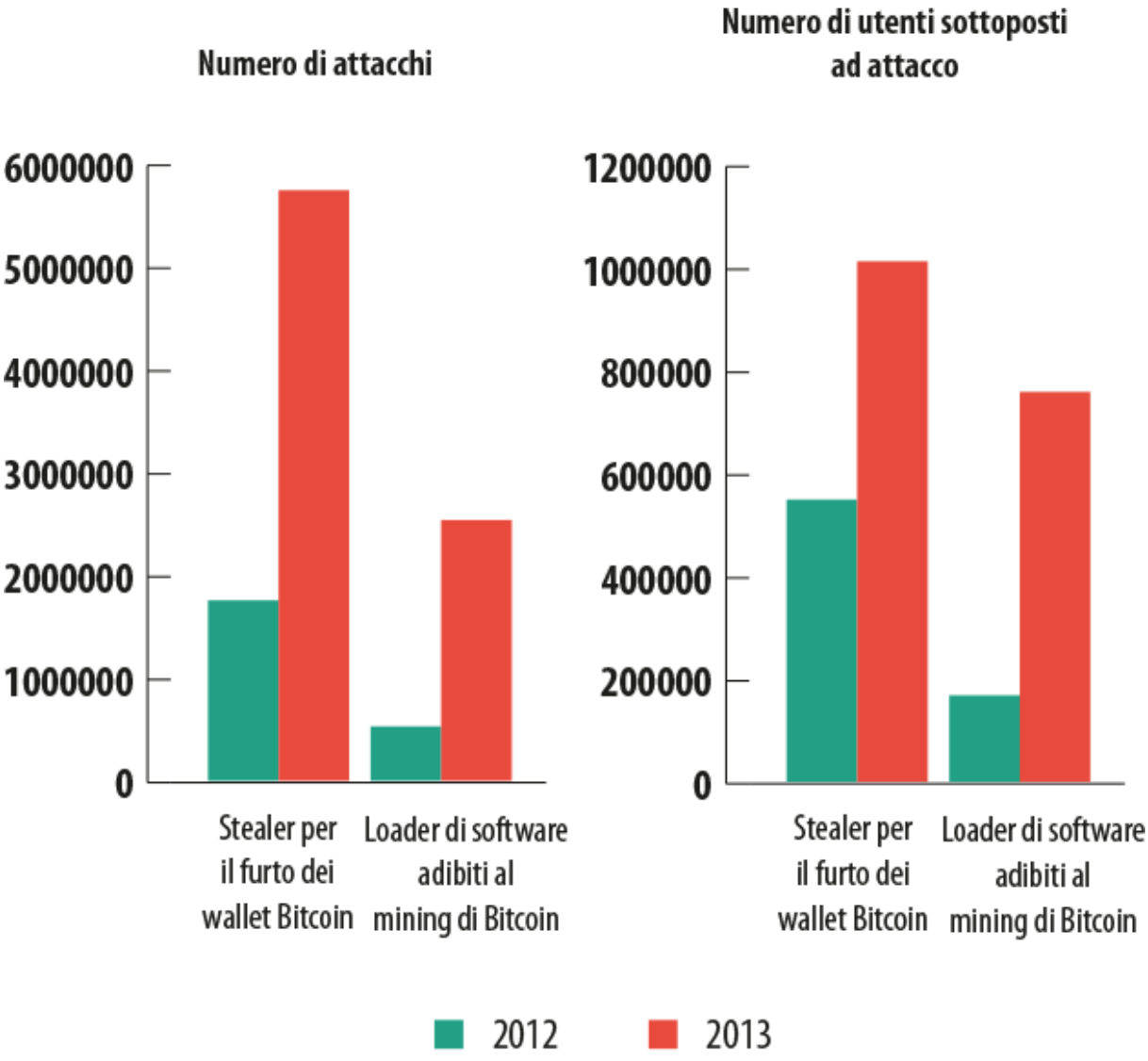


Come evidenzia il grafico, il numero dei rilevamenti eseguiti dai prodotti Kaspersky Lab adibiti alla protezione IT nei confronti dei programmi malware preposti al furto dei wallet e nei confronti dei programmi specializzati nel caricamento di software per le operazioni di mining dei Bitcoin - ha iniziato a crescere sensibilmente nella seconda metà del 2012. Le dinamiche che hanno caratterizzato tale genere di attacchi informatici sono divenute ancor più interessanti nel corso del 2013. Uno dei due picchi principali, registratisi riguardo ai rilevamenti effettuati dalle soluzioni di sicurezza di Kaspersky Lab in merito al malware appositamente sviluppato per colpire il sistema Bitcoin, si è verificato nel mese di aprile. Proprio in questo mese, nell'anno passato, il corso del Bitcoin è improvvisamente schizzato a quota 230 dollari; è evidente come la repentina crescita del valore della nota valuta digitale abbia indotto i cybercriminali a diffondere in maniera ancor più attiva programmi malware "ad hoc", preposti al furto o al mining dei Bitcoin.

Sempre nel mese di aprile dello scorso anno, tuttavia, la quotazione della criptovaluta qui esaminata è poi improvvisamente scesa ad 83 dollari. Alla repentina caduta ha fatto quindi seguito, alla fine di aprile 2013, una ripresa sino a quota 149 dollari; nel successivo mese di maggio, il corso si è finalmente stabilizzato. Nel periodo intercorrente da maggio ad agosto il valore del Bitcoin si è mantenuto entro un range di 90-100 dollari, per poi crescere lievemente nel corso dei mesi successivi. Come si può osservare confrontando i due grafici in questione, tale dinamica si è dimostrata molto flebilmente correlata alla situazione che si è specularmente manifestata sull'opposto "fronte", quello relativo al malware specificamente

"dedicato" alla criptomoneta; non è tuttavia escluso che proprio il processo di stabilizzazione del corso del Bitcoin abbia provocato una nuova impennata degli attacchi nel mese di agosto. Un altro repentino picco riguardo al numero di attacchi rilevati si è poi verificato nel successivo mese di dicembre. In questo stesso mese, il corso del Bitcoin è dapprima sceso drasticamente, passando da 1.000 a 584 dollari, per poi salire di nuovo vertiginosamente alla fine di dicembre e raggiungere in tal modo quota 804 dollari.

Sempre a partire dal mese di aprile 2013 è sensibilmente aumentato il numero dei rilevamenti effettuati dai prodotti Kaspersky Lab riguardo ai software impiegati per le attività di generazione dei Bitcoin. Tale crescita si è protratta sino ad ottobre, mentre in novembre il numero dei rilevamenti eseguiti ha iniziato a diminuire.



Complessivamente, nel corso del 2013, sia il numero dei rilevamenti realizzati tramite i prodotti Kaspersky Lab, sia il numero degli utenti che si sono via via imbattuti in programmi malware o programmi potenzialmente nocivi correlati al sistema Bitcoin, è cresciuto di varie volte rispetto al 2012. E' di particolare interesse osservare come, ad iniziare all'incirca dal

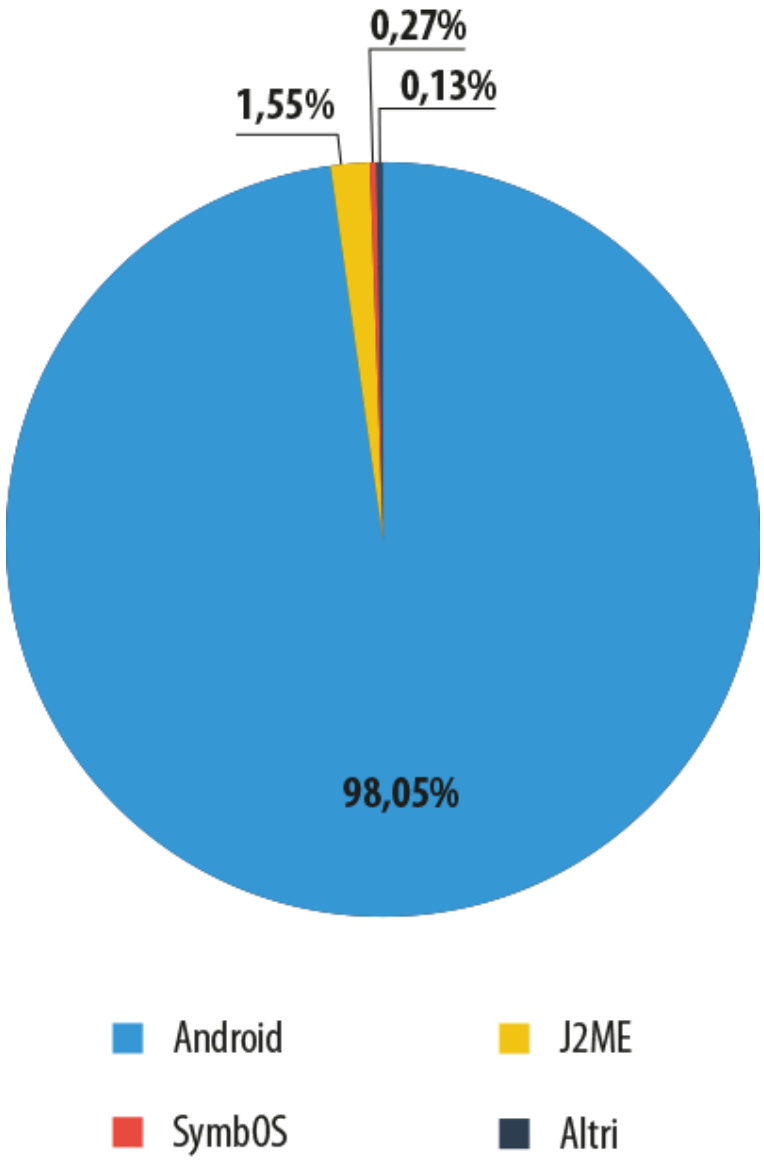
mese di ottobre 2013, il numero dei rilevamenti eseguiti nei confronti dei programmi maligni specializzati nell'installare software per le operazioni di mining dei Bitcoin abbia iniziato a diminuire, mentre il numero dei rilevamenti riguardanti i malware preposti al furto dei wallet virtuali sia invece aumentato. Ciò potrebbe essere la naturale conseguenza della specifica peculiarità che contraddistingue la nota valuta elettronica: maggiore è la quantità di "monete" che si genera all'interno del sistema, tanto più complesso diviene il produrne di nuove. Tale circostanza potrebbe aver di fatto costretto i malintenzionati a concentrare le loro attività illecite sulla ricerca e sul furto dei portafogli virtuali Bitcoin, contenenti criptovaluta già generata in precedenza.

I programmi appositamente sviluppati dai virus writer per carpire le informazioni sensibili legate alla sfera finanziaria degli utenti rappresentano indubbiamente una delle tipologie di malware più temibili in assoluto. L'entità ed il livello di pericolosità di tale temibile minaccia IT risultano in costante aumento, anche a causa dell'enorme numero di potenziali vittime degli attacchi informatici in cui viene dispiegato tale genere di malware. In sostanza, ogni titolare di carta di credito, che navighi in Internet servendosi di un computer scarsamente protetto, è soggetto a cadere nelle trappole (più o meno) abilmente tese dai truffatori. Computer e laptop, poi, non sono affatto gli unici dispositivi attraverso i quali gli utenti eseguono transazioni finanziarie in Rete. Al giorno d'oggi, in pratica, quasi ogni utente dispone di uno smartphone o di un tablet. Per i cybercriminali, tali dispositivi mobili rappresentano, in sostanza, una sorta di potenziale ed ulteriore "buco" nelle tasche degli utenti dei servizi online legati al settore finanziario.

Le cyber-minacce rivolte al mobile banking

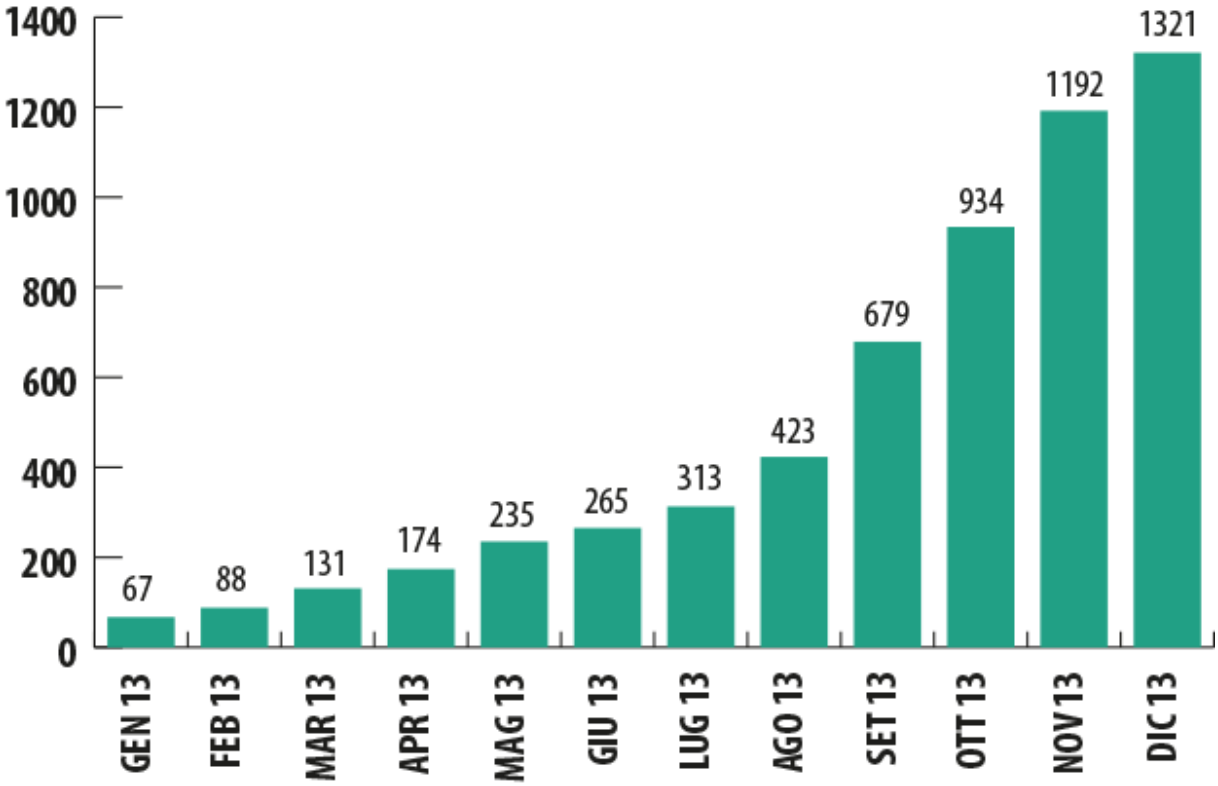
Per lungo tempo i dispositivi mobili sono rimasti, per i cybercriminali, una sorta di "Terra Incognita". In gran parte, tale situazione è stata determinata sia dalle funzionalità alquanto limitate di cui erano provvisti i dispositivi mobili di prima generazione, sia dall'effettiva difficoltà nello sviluppare software adeguati per tale genere di apparecchi. Tuttavia, con l'avvento di smartphone e tablet - dispositivi multifunzionali collegati in Rete - e con l'ampia disponibilità di strumenti per la creazione delle relative applicazioni, tutto è rapidamente cambiato. Gli esperti di Kaspersky Lab stanno rilevando, già da alcuni anni, una costante crescita del numero di programmi malware appositamente progettati e sviluppati dai virus writer per attaccare le piattaforme mobili, ed in particolar modo il sistema operativo Android.

Nel 2013, l'OS Android ha rappresentato il principale obiettivo degli attacchi informatici lanciati dai cybercriminali nei confronti dei dispositivi mobili. In effetti, addirittura il 98,1% del numero complessivo di malware mobili individuati dagli esperti di sicurezza IT nel corso dell'anno 2013 è risultato essere destinato al sistema operativo di Mountain View, tradizionalmente simboleggiato dal piccolo robot verde. Ciò testimonia in maniera inequivocabile sia la vastissima popolarità ormai raggiunta a livello planetario dall'OS Android, sia la vulnerabilità intrinseca dell'architettura che contraddistingue tale piattaforma mobile.



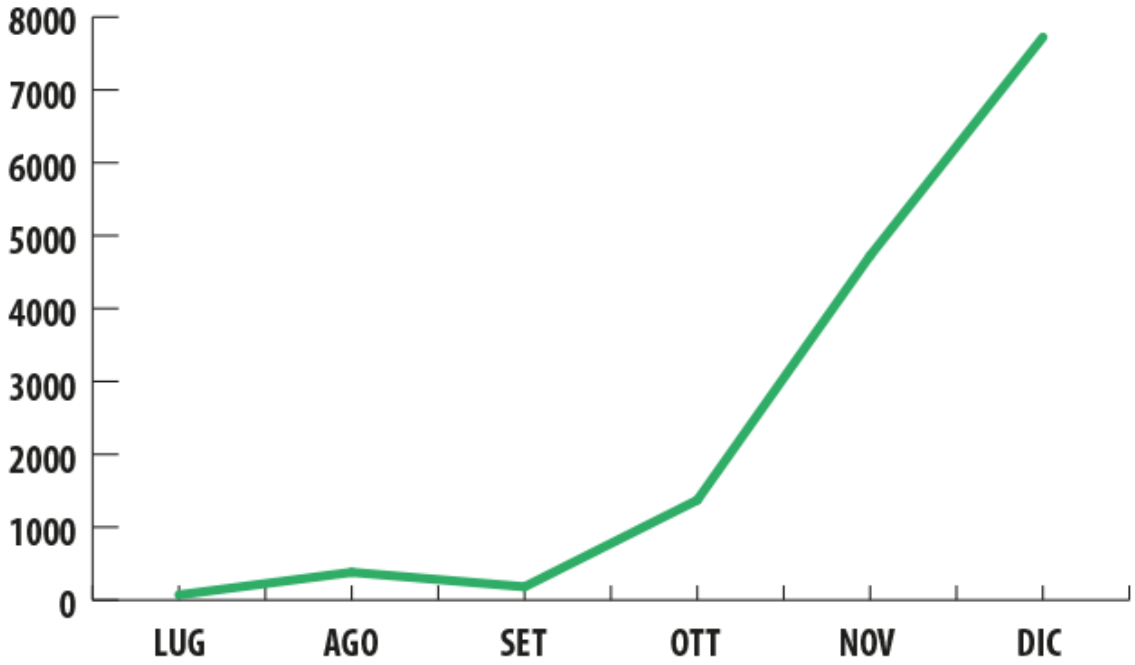
Il malware mobile nel 2013

La maggior parte dei malware mobili attualmente in circolazione è stata appositamente progettata dai virus writer allo scopo di sottrarre illecitamente significative somme di denaro agli utenti-vittima. Risultano specializzati nella conduzione di attività nocive riconducibili a tale specifica tipologia cybercriminale i famigerati Trojan-SMS, numerosi programmi Backdoor ed una parte dei programmi dannosi appartenenti alla categoria dei Trojan. Una delle più pericolose tendenze rilevate nel corso del 2013 nella sfera del malware destinato ai dispositivi mobili è indubbiamente rappresentata dal sensibile aumento del numero di programmi nocivi preposti al furto dei dati sensibili utilizzati per l'accesso ai sistemi di banking online e alla conseguente sottrazione delle somme di denaro custodite nei conti bancari degli utenti.



Numero di sample di programmi malware destinati al banking mobile presenti all'interno della "collezione" di Kaspersky Lab - Situazione relativa al 2013

Il numero dei software maligni riconducibili a tale specifica tipologia ha iniziato a crescere in maniera decisamente pronunciata a partire dal mese di luglio, raggiungendo in tal modo, nel successivo mese di dicembre, la considerevole quantità di oltre 1.300 esemplari unici di malware. A partire dallo stesso periodo è ugualmente aumentato in maniera considerevole il numero dei relativi attacchi informatici bloccati e neutralizzati dai prodotti Kaspersky Lab.



Gli attacchi informatici eseguiti mediante l'utilizzo di malware destinato al mobile banking - Situazione relativa alla seconda metà del 2013

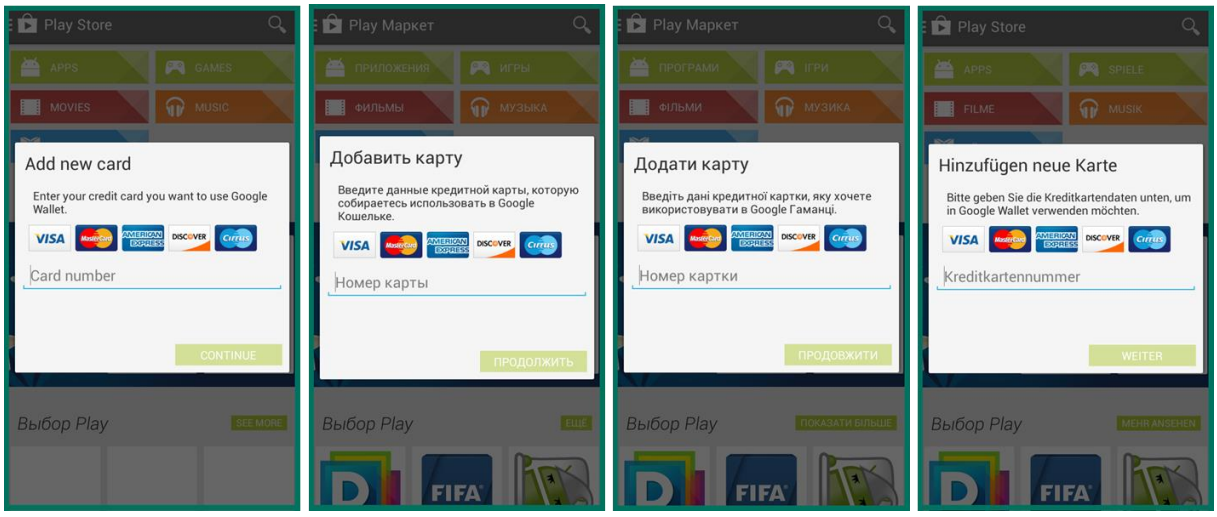
I malware mobili utilizzati dai criminali nei confronti dei clienti dei sistemi di banking online avevano tuttavia già fatto la loro comparsa sulla scena del cybercrimine negli anni precedenti. ZitMo (il "fratello" mobile del famigerato trojan Zeus creato dai virus writer per colpire la piattaforma Win32), ad esempio, è ben noto agli esperti di sicurezza IT sin dall'anno 2010, pur non essendo stato mai individuato nell'ambito di attacchi informatici di massa, proprio in ragione delle specifiche funzionalità da esso possedute. Il malware ZitMo, in effetti, è in grado di operare soltanto se abbinato al trojan Zeus, destinato ai computer desktop. Quest'ultimo intercetta login e password necessari per accedere all'account online dell'utente-vittima, mentre la principale funzione espletata da ZitMo consiste nel carpire le password monouso (si tratta, nella fattispecie, dei cosiddetti codici segreti mTAN - mobile Transaction Authentication Number) utilizzate per confermare l'esecuzione della transazione finanziaria all'interno del sistema di banking online; tali password vengono in seguito trasmesse ai malintenzionati in agguato, i quali si avvalgono dei dati sensibili illecitamente sottratti per realizzare il furto del denaro presente sull'account dell'utente.

Lo schema fraudolento sopra descritto è stato ampiamente utilizzato dai cybercriminali anche nel corso del 2013; nel frattempo, tra l'altro, si sono dotati di temibili "fratelli minori" - appositamente destinati a colpire i dispositivi mobili - anche i principali concorrenti del trojan Zeus: SpyEye (SpitMo) e Carberp (CitMo). Anche a questi ultimi, tuttavia, non è risultata imputabile un'elevata quantità di attacchi informatici. Il motivo di tale particolare situazione può risiedere nel fatto che sul mercato nero delle cyber-minacce sono ugualmente comparsi

programmi trojan indiscutibilmente dotati di un livello di "autonomia" ben superiore, essendo gli stessi in grado di poter "lavorare" senza il supporto di alcun partner "da desktop".

Un tipico esempio di malware del genere è indubbiamente rappresentato dal programma trojan denominato Svpeng, individuato dagli esperti di Kaspersky Lab nel mese di luglio 2013. Il trojan in questione sfrutta una specifica peculiarità che contraddistingue alcuni sistemi di mobile banking allestiti da banche russe; attraverso tale particolarità esso è in grado di sottrarre denaro dal conto bancario dell'utente-vittima.

In Russia, in effetti, alcuni istituti di credito di primaria importanza mettono a disposizione dei propri clienti un particolare servizio grazie al quale risulta possibile ricaricare l'account del telefono mobile tramite il trasferimento di una determinata somma di denaro direttamente dalla carta di credito di cui è titolare l'utente. Per beneficiare di tale comoda opportunità, il cliente della banca dovrà semplicemente inviare dal proprio smartphone, verso uno speciale numero telefonico predisposto dall'istituto bancario, un SMS dal contenuto prestabilito. Da parte sua, il trojan Svpeng provvede ad inviare appositi messaggi SMS verso i numeri relativi ai servizi SMS forniti da due di tali banche russe. In questo modo, i cybercriminali che si celano dietro Svpeng possono agevolmente determinare se le credit card rilasciate da tali banche risultano collegate o meno al numero di telefono dello smartphone infettato dal malware; una volta rilevata l'esistenza del conto bancario, i malintenzionati potranno poi venire a conoscenza del saldo in esso presente. Compiute tali operazioni, i criminali avranno l'opportunità di impartire al trojan Svpeng un apposito comando per effettuare il trasferimento di una determinata somma di denaro dal conto bancario all'account telefonico mobile dell'utente-vittima.



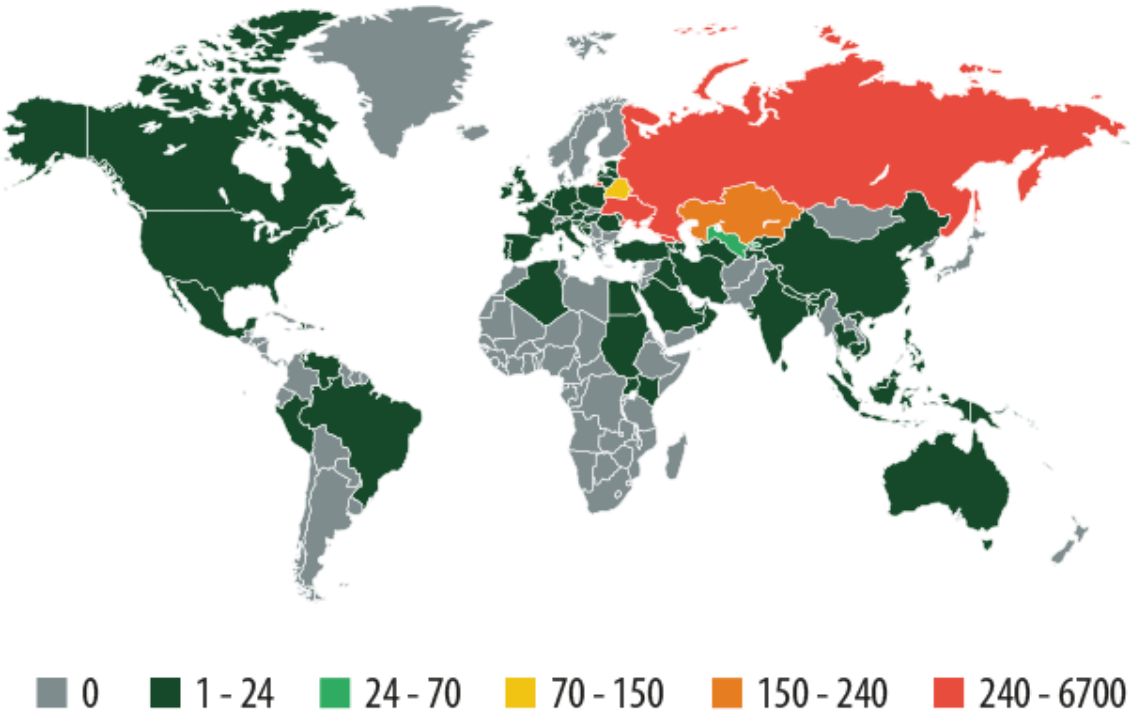
L'interfaccia fasulla creata dal trojan Svpeng allo scopo di carpire i dati sensibili dell'utente

In seguito, il denaro furtivamente trasferito sull'account di telefonia potrà essere prelevato attraverso varie modalità, ad esempio mediante il trasferimento della somma illecitamente carpita su un apposito portafoglio elettronico, magari tramite un account personale aperto presso l'operatore di telefonia mobile, oppure mediante il semplice invio di messaggi SMS verso numeri premium a pagamento. In aggiunta alle funzionalità dannose sopra descritte il

malware Svpeng è ugualmente in grado di eseguire il furto di login e password utilizzati per accedere ai sistemi di online banking.

Altri due significativi esempi di pericolosi trojan bancari individuati dagli analisti di Kaspersky Lab sono rappresentati dai malware rispettivamente identificati con la denominazione di Perkele e Wroba. Il primo dei due si presenta, in sostanza, come l'esatto analogo di ZitMo: la principale funzionalità di cui è provvisto Perkele consiste difatti nell'intercettare le password monouso utilizzate dai clienti degli istituti bancari per confermare le transazioni finanziarie in corso. Wroba, invece, provvede innanzitutto a ricercare, all'interno del dispositivo mobile infetto, le applicazioni relative al banking online; una volta individuate, se presenti, ne effettua la rimozione, per poi caricare sullo smartphone compromesso copie fasulle di tali applicazioni, attraverso le quali raccoglierà tutti i dati necessari per eseguire le procedure di autenticazione; i dati sensibili così carpiti vengono infine trasmessi ai malintenzionati di turno.

La maggior parte degli attacchi IT realizzati nel corso del 2013 tramite il dispiegamento di trojan bancari mobili si è registrata, secondo i dati raccolti ed elaborati da Kaspersky Lab, sul territorio della Federazione Russa e dei paesi limitrofi. Il malware Perkele, tuttavia, è stato impiegato per portare attacchi non solo nei confronti degli utenti di istituti bancari russi, ma anche dei clienti di alcune note banche europee. Wroba, da parte sua, è risultato invece essere principalmente indirizzato agli utenti mobili ubicati nella Corea del Sud.



Ripartizione geografica degli attacchi condotti nel corso del 2013 mediante l'utilizzo di applicazioni Android dannose destinate al mobile banking

Per il momento, in cifre assolute, l'entità complessiva degli attacchi IT di tal genere - eseguiti tramite l'utilizzo di malware finanziario specificamente rivolto a colpire gli utenti dei dispositivi mobili e rilevati dai prodotti Kaspersky Lab - risulta relativamente contenuta. Da più di un semestre, tuttavia, si registra ormai una netta tendenza verso un significativo e costante incremento del volume di tali attacchi. Si tratta, indiscutibilmente, di un preciso segnale d'allarme: tutti gli utenti dei dispositivi mobili - ed in particolar modo quelli che si avvalgono della piattaforma Android - debbono necessariamente adottare un atteggiamento di estrema prudenza e cautela riguardo all'effettiva sicurezza dei dati sensibili legati alla propria sfera finanziaria.

Al tempo stesso, anche gli utenti dei dispositivi mobili provvisti di sistema operativo iOS non dovrebbero "rilassarsi" troppo. Sebbene al momento attuale non si registrino vere e proprie "ondate" di programmi malware volti a carpire i dati confidenziali dei proprietari di iPhone ed iPad, occorre pur sempre tener conto del fatto che all'interno del suddetto sistema operativo vengono regolarmente rilevati dei bug, i quali possono essere potenzialmente sfruttati per la creazione di software nocivi riconducibili a tale specifica tipologia. In tal senso, uno degli esempi più recenti ed eclatanti è rappresentato dalla vulnerabilità rilevata dagli analisti alla fine del mese di febbraio 2014; tale falla di sicurezza consente, in effetti, di poter determinare i caratteri immessi dall'utente attraverso la tastiera virtuale presente sul dispositivo. Sfruttando la vulnerabilità sopra menzionata, un malintenzionato potrebbe, tra l'altro, impadronirsi di login e password utilizzati per accedere ai sistemi di banking online.

Conclusioni: tenete bene d'occhio il vostro portafoglio digitale

L'indagine condotta dagli esperti di Kaspersky Lab ha chiaramente dimostrato come il denaro "elettronico" degli utenti della Rete si trovi in una situazione di costante rischio e pericolo. Di fatto, i malintenzionati possono essere in agguato ovunque, pronti a tendere le più insidiose "trappole", sia nel momento in cui l'utente opera sul proprio conto bancario tramite il sistema di banking online prescelto, sia quando egli effettua il pagamento della merce acquistata presso il negozio Internet preferito.

Nel corso del 2013, tutte le varie tipologie di cyber-minaccia finanziaria che attualmente popolano il torbido e complesso panorama della criminalità informatica, hanno evidenziato un preoccupante ed esteso fenomeno di crescita. Ad esempio, la quota inerente agli attacchi di phishing condotti nei confronti degli utenti di istituti bancari di primaria importanza, spesso di caratura internazionale, è in sostanza raddoppiata, mentre risulta aumentato di circa un terzo, rispetto all'anno precedente, il numero degli attacchi informatici portati alla sfera finanziaria degli utenti mediante l'utilizzo di temibili programmi malware.

Per ciò che riguarda il segmento del malware finanziario, ad ogni caso, non è stato segnalato l'ingresso sulla scena di significative "new entry", in grado di oscurare, in qualche modo, la

"fama" già raggiunta da malware quali Zbot e Qhost. Così, tali software nocivi, assieme ad altri trojan ormai ben noti, si sono resi responsabili della maggior parte degli attacchi verificatisi lungo tutto l'arco dello scorso anno. I criminali hanno tuttavia dimostrato ancora una volta la loro indiscussa prontezza nel reagire immediatamente ad ogni importante cambiamento che si produce nel settore oggetto delle loro losche attenzioni; prova ne è il fatto che, già alla fine del 2012, si registrava una repentina ed esponenziale crescita del numero degli attacchi informatici appositamente allestiti per realizzare il furto degli ambiti Bitcoin; tale tendenza è poi proseguita, manifestandosi peraltro in maniera ancor più pronunciata, nel corso del 2013.

Per rafforzare la protezione nei confronti delle cosiddette cyber-minacce finanziarie, gli esperti di Kaspersky Lab raccomandano di adottare le misure qui di seguito descritte.

Per le società

- Sulle imprese, di fatto, poggia gran parte della responsabilità riguardo al livello di sicurezza IT degli utenti. Le società che operano nel settore finanziario, ad esempio, dovrebbero informare gli utenti relativamente alle temibili minacce derivanti dalle attività illecite condotte in Rete dai cybertruffatori, e fornire quindi tutti i consigli necessari al fine di evitare possibili perdite e danni prodotti da malintenzionati.
- Gli istituti bancari ed i sistemi di pagamento dovrebbero necessariamente proporre alla propria clientela un sistema di protezione integrale nei confronti della cybercriminalità. Un chiaro esempio di una simile soluzione di sicurezza IT è rappresentato dalla piattaforma Kaspersky Fraud Prevention, in grado di garantire un'efficace protezione multilivello nei confronti dei truffatori della Rete.

Per gli utenti privati e per gli utenti dei sistemi di banking online

- Gli autori di programmi malware basano spesso la loro attività sullo sfruttamento delle vulnerabilità via via individuate in programmi che risultano particolarmente diffusi presso il pubblico degli utenti. Si rivela pertanto indispensabile avvalersi esclusivamente delle versioni più recenti delle applicazioni utilizzate sul proprio computer, così come provvedere ad installare tempestivamente tutti gli aggiornamenti che riguardano il sistema operativo in uso.
- Vi sono poi, indubbiamente, determinate regole "universali" da adottare e seguire scrupolosamente per poter operare in tutta sicurezza nel mondo di Internet, le quali contribuiscono di sicuro a ridurre i potenziali rischi connessi alle attività condotte in Rete dai cybercriminali, incluso gli attacchi mirati alla sfera finanziaria degli utenti. Questi ultimi dovrebbero pertanto scegliere password particolarmente "solide" e complesse, che si rivelino uniche ed esclusive per ogni servizio online frequentato; occorre inoltre utilizzare con la dovuta cautela le reti Wi-Fi pubbliche, così come evitare di custodire informazioni di natura confidenziale sul proprio browser, e via dicendo.
- Risulta poi indispensabile l'utilizzo di prodotti sicuri ed affidabili per ciò che riguarda la protezione nei confronti del malware, prodotti la cui reale efficacia sia stata già ampiamente confermata da test indipendenti condotti su di essi. Inoltre, alcuni prodotti, quali ad esempio la soluzione di sicurezza Kaspersky Internet Security, sono già provvisti di strumenti incorporati, in grado di assicurare un elevato livello di

protezione nel momento stesso in cui l'utente si accinge ad operare con i servizi online legati alla propria sfera finanziaria.

- Se utilizzate uno smartphone o un tablet per accedere ad un sistema di banking online, così come alle pagine web di un sistema di pagamento, oppure per effettuare acquisti in negozi Internet, non trascurate affatto la protezione IT del vostro dispositivo mobile, mediante l'impiego di una soluzione di sicurezza solida ed affidabile, quale Kaspersky Internet Security for Android, adeguatamente provvista di strumenti avanzati per offrire un'efficace protezione nei confronti del malware e del phishing, così come in caso di smarrimento o furto del dispositivo.

Per i possessori di criptovaluta

A causa della relativa "giovinezza" del Bitcoin e di altri sistemi di moneta digitale analoghi, quali Litecoin, Dogecoin, e molti altri ancora, un elevato numero di utenti non possiede ancora la necessaria dimestichezza riguardo all'utilizzo di tali piattaforme; per questo motivo, gli esperti di Kaspersky Lab consigliano di adottare le seguenti misure per poter operare in sicurezza con le criptovalute:

- Evitate di utilizzare servizi online per custodire i vostri "risparmi" in moneta elettronica; si dovrebbe invece far uso di speciali applicazioni-portafoglio.
- Suddividete in vari portafogli virtuali l'importo in criptovaluta di cui disponete; ciò consentirà di limitare le eventuali perdite in caso di furto di uno di essi.
- Conservate in appositi supporti codificati i wallet utilizzati per la custodia a lungo termine della vostra moneta elettronica. In alternativa, si può ugualmente provvedere a stampare su carta il proprio portafoglio digitale.