McAfee
An Intel Company

REPORT McAFEE LABS SULLE MINACCE

Giugno 2014

Report

McAFEE LABS

McAfee Labs è il più autorevole laboratorio di idee a livello mondiale per la ricerca e l'informazione sulle minacce e per la sicurezza informatica. Grazie ai dati raccolti da milioni di sensori su tutti i principali vettori di minacce — file, Web, messaggi e rete — McAfee Labs offre informazioni sulle minacce in tempo reale, analisi critica e valutazioni di esperti per migliorare la protezione e ridurre i rischi.

www.mcafee.com/it/mcafee-labs.aspx

INTRODUZIONE

I report McAfee testimoniano il nostro impegno nell'indagare e nello spiegare gli eventi di spionaggio informatico.

Come scriveva il poeta scozzese Robert Burns, "I migliori piani dei topi e degli uomini van spesso di traverso" *(A un topo, cui avevo distrutto il nido con l'aratro, 1785).* Sono passati più di 200 anni, e la sua osservazione resta valida.

Il nostro obiettivo è pubblicare il *Report McAfee Labs sulle minacce* nel più breve tempo possibile dopo la fine di ciascun trimestre. Questo trimestre, però, le cose sono andate diversamente. Come sa praticamente chiunque si occupi di sicurezza, la vulnerabilità Heartbleed è stata resa nota in aprile, proprio mentre stavamo iniziando a redigere questo report. Gran parte dell'attenzione dei nostri esperti di minacce si è concentrata subito su Heartbleed, sia per capire come funzionava, sia per garantire che le tecnologie McAfee fossero in grado di proteggere adeguatamente i nostri clienti. Risultato? Questo report è stato pubblicato in ritardo, e i nostri migliori piani sono andati di traverso.

In questo report non parleremo di Heartbleed, perché è ancora troppo presto per capire esattamente quale impatto potrà avere, ma non perdetevi la nostra analisi nel prossimo *Report sulle minacce.* Ci dedicheremo invece a vari argomenti di interesse per molti dei nostri clienti. I due servizi sul malware mobile esaminano aspetti diversi di questo problema in continua evoluzione. Analizziamo inoltre un curioso fenomeno che riguarda il mining o generazione di moneta virtuale, in cui chi ci guadagna sono solo i venditori degli strumenti per eseguire l'operazione. Parliamo infine della diminuzione del numero dei nuovi rootkit e dei motivi per cui riteniamo che a breve ci sarà un'inversione di tendenza.

Richiamiamo inoltre la vostra attenzione su altri importanti report McAfee, tutti dedicati allo spionaggio informatico. In aprile, Verizon ha pubblicato il *Verizon 2014 Data Breach Investigations Report* (Rapporto investigativo sulle violazioni di dati 2014). McAfee ha collaborato con Verizon fornendo i dati contenuti nel report sullo spionaggio informatico *Dissecting Operation Troy (Analisi di Operazione Troy)*. All'inizio di giugno, poi, abbiamo pubblicato un report commissionato al Center for Strategic and International Studies dal titolo *Net Losses—Estimating the Global Cost of Cybercrime (Perdite nette — Una stima del costo globale del crimine informatico).* Tutti questi report testimoniano il significativo investimento effettuato da McAfee per diventare la fonte di informazioni e di analisi più attendibile del settore in materia di spionaggio informatico.

Vincent Weafer, Vice Presidente Senior, McAfee Labs

Segui McAfee Labs

SOMMARIO

REPORT McAFEE LABS SULLE MINACCE
Giugno 2014

Questo report è stato preparato e redatto da:

Benjamin Cruz
Deepak Gupta
Aditya Kapoor
Haifei Li
Charles McFarland
Francisca Moreno
François Paget
Craig Schmugar
Rick Simon
Dan Sommer
Bing Sun
James Walter
Adam Wosotowsky
Chong Xu

SINTESI

I criminali informatici hanno creato centinaia di cloni di Flappy Bird che contengono malware. Il nostro campione di 300 cloni ha individuato 238 cloni di Flappy Bird contenenti malware.

Secondo McAfee Labs, chi vende botnet sostenendo che il mining di moneta virtuale è redditizio è un venditore di fumo.

Dopo il calo nel numero dei nuovi rootkit registrato a partire dal 2011, McAfee Labs ritiene probabile un'inversione di tendenza a breve.

Attraverso una serie di esempi, McAfee Labs spiega come non sia sufficiente proteggere le piattaforme mobili. Gli sviluppatori di app mobili devono fare maggiori sforzi per proteggere le loro app e gli utenti devono prestare maggiore attenzione nel concedere autorizzazioni alle app.

Segui McAfee Labs

L'attacco dei cloni di Flappy Bird

L'argomento può sembrare frivolo, ma il fenomeno ha alcune gravi conseguenze. Tra la fine dell'anno scorso e l'inizio di quest'anno, Flappy Bird, un gioco per smartphone, ha avuto una diffusione massiccia fra gli utenti. Ciononostante, il suo creatore lo ha ritirato dal mercato lo scorso febbraio. Vista l'enorme popolarità del gioco, alcuni intraprendenti criminali informatici hanno sviluppato centinaia di cloni di Flappy Bird contenenti malware. McAfee Labs ha testato 300 di questi cloni e ha scoperto che in quasi l'80% dei casi contenevano malware. Tra i comportamenti che abbiamo rilevato, telefonate effettuate senza l'autorizzazione dell'utente, invio, registrazione e ricezione di SMS, estrazione di dati dalla rubrica e monitoraggio della posizione geografica. Nei casi peggiori, il malware otteneva l'accesso root, che consente un controllo illimitato su tutti i dati del dispositivo mobile, comprese le informazioni aziendali riservate.

Non è una questione di mining

McAfee Labs ha redatto diversi report sulla moneta virtuale, fra cui *Riciclaggio digitale, Jackpot! Riciclaggio di denaro attraverso il gioco d'azzardo online* e il *Report McAfee Labs sulle minacce: terzo trimestre 2013*. Questo trimestre ci addentriamo in un fenomeno che riguarda la moneta virtuale e che ci lascia quanto meno perplessi. Infatti, abbiamo notato che esistono botnet infettate da malware dotate di funzionalità di mining di moneta virtuale. Tuttavia, facendo qualche calcolo, sembra alquanto improbabile che la generazione di moneta virtuale attraverso le botnet garantisca a chi le gestisce maggiori guadagni. A nostro parere, gli unici a ricavare qualcosa da questa funzionalità sono gli sviluppatori di strumenti per botnet.

Rootkit di nuovo in aumento

Buone notizie — o almeno, così credevamo. Dalla metà del 2011, McAfee Labs ha osservato una diminuzione nel numero dei nuovi rootkit. Nell'ultimo trimestre abbiamo addirittura rilevato il numero più basso di nuovi rootkit dal 2008. È probabile che questo calo sia dovuto alla protezione aggiuntiva presente nei microprocessori a 64 bit e nei corrispondenti sistemi operativi a 64 bit. Tuttavia, i criminali informatici hanno mille risorse e questo trimestre abbiamo osservato un'inversione della tendenza al calo, benché dovuta a una singola famiglia di malware a 32 bit. Gli aggressori hanno imparato a intercettare i certificati digitali a livello di root, a sfruttare le vulnerabilità del kernel esistenti e ad aggirare le misure di sicurezza dei sistemi a 64 bit. Siamo convinti che le nuove tecniche sviluppate per aggirare le protezioni dei sistemi a 64 bit porteranno in breve a un aumento degli attacchi rootkit.

Il malware mobile sfrutta le vulnerabilità delle piattaforme, le app e i servizi

Per questo argomento abbiamo raccolto una serie di casi che evidenziano i metodi con cui il malware sfrutta le piattaforme dei dispositivi mobili. Il primo esempio illustra come un'app proposta sull'app store Google Play scarica, installa e lancia automaticamente altre app senza l'autorizzazione dell'utente. In questo esempio, l'app responsabile dell'abuso non scarica malware ma sfrutta un sistema di download a pagamento. Tuttavia, da qui al download automatico di app infettate da malware il passo è breve. In un secondo esempio, un trojan sfrutta una falla di sicurezza in un servizio di portafoglio digitale legale per rubare denaro. Infine, un terzo esempio mostra come è stata utilizzata una debolezza nel metodo di crittografia di WhatsApp, l'app di messaggistica più diffusa, per il furto di conversazioni e di foto. Anche se questa vulnerabilità è stata risolta, il caso in questione dimostra che gli attacchi continueranno a cercare i punti deboli delle piattaforme mobili.

Nel 1° trimestre 2014 il numero totale di campioni di malware presenti nello "zoo" di McAfee Labs ha superato la barriera dei 200 milioni.

ARGOMENTI PRINCIPALI DEL TRIMESTRE

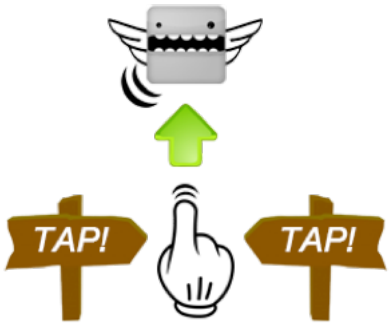
L'attacco dei cloni di Flappy Bird

Ancora una volta notiamo come l'accoppiata social engineering-gioco più in voga del momento sia un potente generatore di malware. L'attuale epidemia è dovuta a uno stuolo di cloni malevoli di "Flappy Bird".

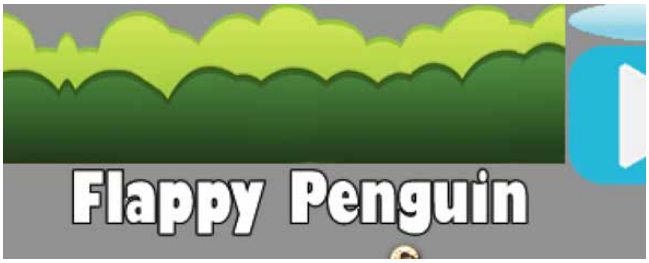
Il gioco "Flappy Bird" in versione originale è stato reso disponibile su Apple iOS a metà del 2013 e su Android all'inizio di quest'anno. Ha avuto un successo folgorante, con oltre 50 milioni di download, e ha fatto del suo sviluppatore Dong Nguyen una celebrità, prima che questi ritirasse l'app dal mercato in febbraio.

Negli ultimi *Report McAfee Labs sulle minacce* avevamo segnalato un brusco aumento della diffusione del malware mobile. La Flappy Bird-mania e la conseguente invasione di malware sono un ottimo esempio di come gli autori di malware approfittino dell'eccessivo entusiasmo degli utenti per un'app o per un gioco legittimo. Esistevano già dei cloni pericolosi di Flappy Bird prima che fosse ritirato dai negozi online, ma la richiesta di giochi simili a Flappy Bird è aumentata solo dopo il ritiro dell'app. Nel primo trimestre del 2014 abbiamo visto emergere centinaia di cloni di Flappy Bird, per la maggior parte malevoli.

Il gioco Flappy Bird originale.



Un clone malevolo di Flappy Bird.



Un altro clone malevolo di Flappy Bird.

Segui McAfee Labs

Alla fine del primo trimestre, McAfee Labs ha isolato un campione di 300 cloni di Flappy Bird dal suo "zoo" di malware mobile. Di questi 300, 238 sono stati giudicati pericolosi. Considerando la rapidità con cui sono spuntate queste app malevole, e il numero di volte in cui sono state scaricate, la situazione è allarmante.

Ma che cosa fanno queste app malevole? A parte il fatto di sfruttare il richiamo di Flappy Bird a fini di social engineering, hanno molte più funzionalità rispetto al gioco originale. In realtà, possono mettere in atto molti comportamenti discutibili, dannosi e invasivi.

Quando si analizza la pericolosità di un'applicazione o di un pacchetto mobile, alcuni comportamenti causano più allarmi di altri. L'esempio che segue lo illustra benissimo: com.touch18.flappybird.app (3113ad96fa1b37acb50922ac34f04352) è uno dei numerosi cloni malevoli di Flappy Bird.

Il clone malevolo di Flappy Bird com.touch18.flappybird.app.

Fra i vari comportamenti dannosi, questo clone:

- Effettua telefonate senza l'autorizzazione dell'utente
- Installa applicazioni aggiuntive senza l'autorizzazione dell'utente
- Consente a un'app di monitorare gli SMS in entrata, di registrarli o elaborarli (autorizzazione non dichiarata)
- Invia SMS senza l'autorizzazione dell'utente
- Estrae SMS
- Invia dati a un numero di cellulare via SMS
- Consente a un'app di leggere il contenuto della rubrica dell'utente (autorizzazione non dichiarata)
- Estrae le coordinate GPS (latitudine e longitudine)
- Legge il codice IMEI e l'indirizzo MAC e li trasmette a terzi (JSON) senza l'autorizzazione dell'utente
- Invia dati sull'attività dell'utente a siti esterni
- Consente a un'app di chiamare killBackgroundProcesses(String) (autorizzazione non dichiarata)

Rooting

LEVEL	API CALLS	ISOLATION	DESCRIPTION
	java/lang/Runtime/exec(Ljava/lang/String;)Ljava/lang/Process;	Yes	Tries to get root access on your device

Un clone malevolo di Flappy Bird cerca di ottenere l'accesso root.

Come spieghiamo altrove in questo report, il malware mobile continua la sua rapida ascesa, sia in termini numerici che di efficacia. I dispositivi mobili sono facili obiettivi per gli aggressori. Per impedire l'installazione del codice dannoso, dobbiamo essere diligenti e consapevoli in ogni momento dei nostri comportamenti. La mitigazione tramite controlli software (antimalware, contenitori sicuri e simili) è solo una delle fasi di questo processo: occorre essere responsabili e avere il controllo delle fonti da cui si cercano, si acquisiscono o si installano app e giochi. Molto si ottiene con il buon senso e con una "igiene" sicura ed efficace dei dispositivi mobili.

Segui McAfee Labs

Non è una questione di mining

Dal punto di vista della ricerca sulla sicurezza e sul malware, il business della moneta virtuale ha avuto un'altra evoluzione interessante. Attualmente, infatti, osserviamo botnet dotate di vari livelli di funzionalità di mining di moneta virtuale. Ma anche ammettendo che hardware e alimentazione siano a costo zero (i costi delle botnet e della loro alimentazione sono sostenuti dalle vittime), il livello di difficoltà dei comuni algoritmi di mining e la natura non specializzata del'hardware che viene infettato dal malware vanificano lo sforzo. In sostanza, chi vende botnet sostenendo che il mining di moneta virtuale è redditizio è un venditore di fumo. Inoltre, chi gestisce le botnet rischia di essere scoperto perché è più probabile che le vittime si accorgano dell'attività di calcolo in corso sui loro dispositivi, dal momento che questa consuma notevoli risorse.

Da molti anni il vantaggio economico è il principale stimolo che alimenta l'industria delle botnet infettate da malware. Sviluppare malware, kit ed exploit e acquistarli per creare una botnet in proprio sono attività redditizie.

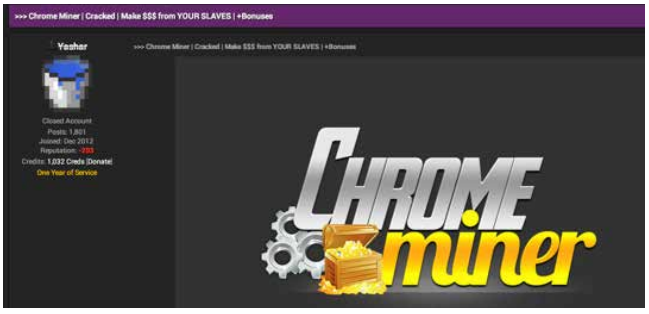
Di recente, nel quadro è intervenuto un altro fattore: la generazione di moneta virtuale è diventata una merce ed è ormai una delle principali funzioni delle botnet. Questa funzionalità viene adottata in tutte le piattaforme più diffuse, comprese quelle mobili. Questo fenomeno assomiglia molto a passate innovazioni nelle botnet e nel malware quali l'avvento degli attacchi DDoS (distributed denial of service), la persistenza delle installazioni, i meccanismi di aggiornamento privati e l'elusione del rilevamento attivo.

Basta andare a curiosare in qualsiasi forum o sito di vendita clandestino dedicato alla sicurezza per trovare una miriade di miner botnet, di builder e di versioni piratate di builder e di kit commerciali SHA-256 e SCRYPT, insieme al consueto assortimento di bot DDoS, criptatori e altri servizi e strumenti nefasti. Tra gli esempi più recenti possiamo citare EnvyMiner, DeadCow, SovietMiner, JHTTP, Black Puppet e Aura. E questi sono solo una minima parte rispetto al totale esistente.

Alcuni esempi di builder o di servizi e relativi prezzi:

- Aura (miner SHA-256, SCRYPT, SCRYPT-Jane). 50 $ per una licenza di durata illimitata
- Black Puppet (Bitcoin). 10 $ al mese o 20 $ licenza illimitata
- HTTP (SHA-256, SCRYPT). 50 $ al mese o 200 $ licenza illimitata
- SovietMiner (SHA-256, SCRYPT). 15 $ al mese
- DeadCow (SHA-256, SCRYPT). 15 $ al mese o 45 $ licenza illimitata

Molti dei più comuni miner bot e toolkit sono stati diffusi in rete illegalmente o piratati, consentendo ad altri di utilizzarli senza limitazioni legate alla licenza.



L'app Chrome Miner, trapelata in rete.

Algoritmi di hash delle criptomonete

SHA-256: la funzione crittografica di hash per il mining è lo standard NIST SHA-256. Questo è il metodo più complesso. Per avere successo, il mining o generazione di moneta virtuale richiede hardware o risorse di elaborazione separate o specializzate (ASIC). Esempi: Bitcoin, Namecoin

SCRYPT: funzione di derivazione di chiave semplificata utilizzata per il mining. Questo metodo è più adatto per l'elaborazione mediante processori grafici molto potenti. Esempi: Litecoin, Dogecoin, Vertcoin

Segui McAfee Labs

L'app Aura Miner, trapelata in rete.

Come nella maggior parte dei kit e dei builder, la funzionalità di mining di moneta virtuale è in gran parte personalizzabile e configurabile. È possibile addirittura controllare la temperatura massima consentita per la CPU durante il mining. Il mining con GPU/CPU fa un uso intensivo delle risorse, e quindi per non essere rilevata la funzionalità deve essere regolata:

una limitazione che compromette il ritorno sull'investimento complessivo di questi bot, oltre ad aumentarne notevolmente la presenza o impatto sui dispositivi infetti e a renderli più evidenti.

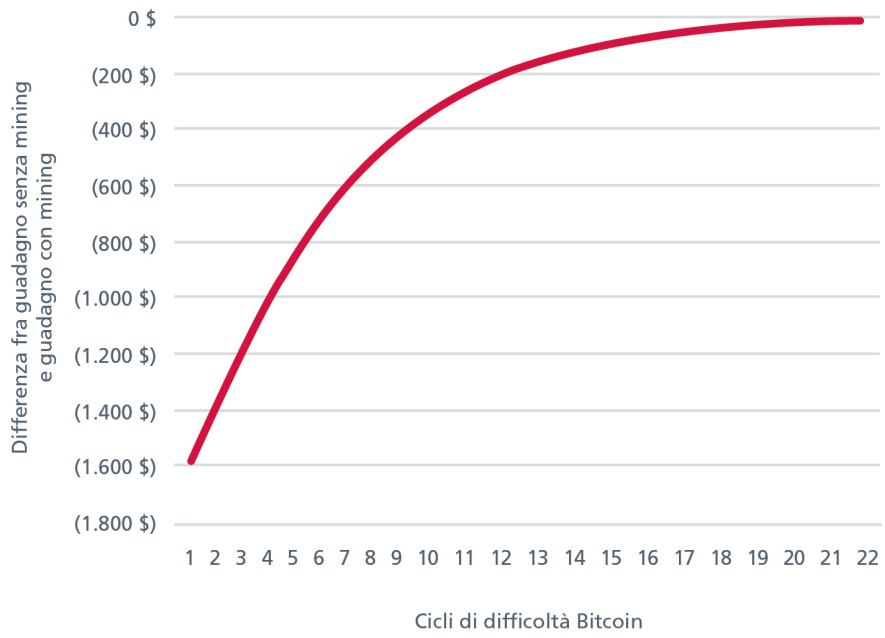
Si tratta di uno sviluppo interessante, per il fatto che il mining di moneta virtuale non aumenta il guadagno di chi gestisce una botnet. Infatti, quanti più miner si aggiungono all'ecosistema, tanto più il mining di moneta virtuale diventa difficile e affamato di risorse. Ai livelli attuali di difficoltà, è poco probabile che un gestore di botnet incrementi il suo guadagno aggiungendo una funzione di mining di moneta virtuale agli attacchi già in corso.

La redditività del mining di moneta virtuale dipende da numerose variabili, fra cui il tasso di difficoltà crescente[1], l'hash rate[2], il valore di mercato della moneta virtuale e l'attrito fra i miner. Nell'ecosistema della botnet, l'attrito si verifica quando il malware viene rilevato o eliminato a causa della sua presenza manifesta sul dispositivo.

Il guadagno di un gestore di botnet si può calcolare tenendo conto, fra le altre variabili, dell'hash rate medio (distribuito fra GPU e CPU di livello consumer e business), dell'attrito, dell'aumento stimato della difficoltà e del numero di infezioni.

Ad esempio, per una botnet che fa mining di moneta virtuale con 10.000 bot persistenti a un hash rate medio aggregato di 100 megahash al secondo, calcolando il 5% di bot in meno durante ogni ciclo di difficoltà a causa del rilevamento o della mitigazione e ipotizzando che il valore di Bitcoin sia 500 $, si otterrebbe il grafico seguente:

DIFFERENZA DI GUADAGNO RISPETTO AL PUNTEGGIO DI DIFFICOLTÀ COMPRENDENDO IL MALWARE CON MINING



Fonte: McAfee Labs, 2014.

Segui McAfee Labs

Il grafico precedente mostra la differenza potenziale di redditività fra una botnet con funzionalità aggiuntiva di mining per Bitcoin e una botnet senza questa funzionalità. Viene mostrata la differenza di guadagno rispetto ai diversi cicli di difficoltà di Bitcoin, che in media sono circa uno ogni due settimane.

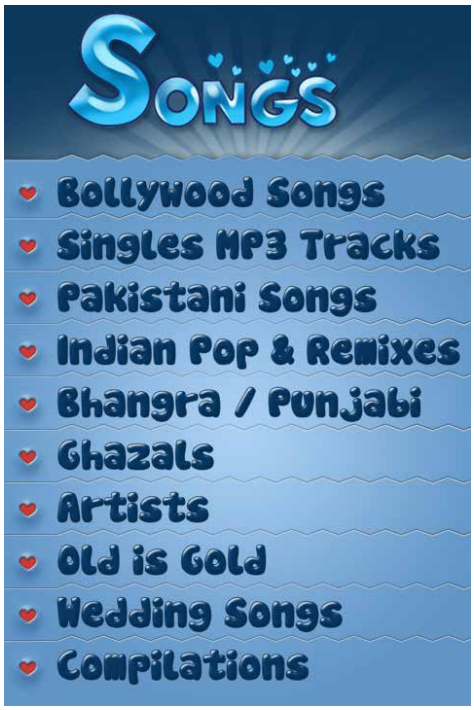
In questo esempio, l'aggiunta del mining di moneta virtuale riduce il potenziale guadagno a causa del maggiore attrito fra i bot e del tempo perso a non eseguire altre operazioni più redditizie quali il furto di password o di numeri di carte di credito. Inoltre, il grafico ipotizza una perdita di solo il 5% dei bot, una percentuale troppo bassa e irrealistica. Problemi analoghi affliggono il mining di moneta virtuale basato su SCRYPT, come Litecoin e Dogecoin.

La perplessità suscitata dall'impossibilità di realizzare guadagni aumenta ulteriormente nel caso di bot che effettuano mining di moneta virtuale su piattaforme mobili. Gli esempi più recenti di mining su Android sono Zorenium, BadLepricon e Songs.

Le piattaforme mobili ne fanno le spese in due modi. In primo luogo, i loro processori sono più lenti rispetto ai processori desktop o laptop di fascia consumer. In secondo luogo, è probabile che la percentuale di attrito delle piattaforme mobili, in proporzione, sia eccessivamente alta. Questo è dovuto alla durata limitata delle batterie delle piattaforme mobili e al rischio aggiuntivo di guasto hardware per via della natura intensiva delle operazioni di mining. Con l'uso di una normale piattaforma mobile è impossibile realizzare guadagni significativi, a meno che la botnet non abbia delle percentuali di attrito eccessivamente basse e irrealistiche.

Nell'esempio ipotetico di una botnet formata da 10.000 dispositivi, il profitto ottenuto senza mining è di 11.000,00 $ e quello ottenuto con il mining è di 11.007,61 $, con un guadagno di soli 7,61 $. Questa cifra presuppone una percentuale di attrito irrealistica dello 0,25%. Con una percentuale di attrito realistica pari al 30%, il potenziale profitto diminuirebbe di 3.265 $.

Il mining di moneta virtuale tramite botnet è ormai diventato un'attività convenzionale. È una funzione proposta in molti toolkit e builder, su più piattaforme diverse. Tuttavia, sussistono molti dubbi sul fatto che questa pratica sia redditizia, viste le risorse necessarie per l'elaborazione degli algoritmi di mining. Ciononostante, i venditori di malware sembrano avere ottimi motivi per ricavare il massimo profitto dalle loro attività.



Songs, l'app di mining per Android.

Ciclo di difficoltà di Bitcoin

La difficoltà è la misura della quantità di lavoro (elaborazione) necessaria per generare catene di blocchi. Il protocollo Bitcoin prevede che la difficoltà sia ricalcolata ogni 2.016 blocchi (circa ogni due settimane).

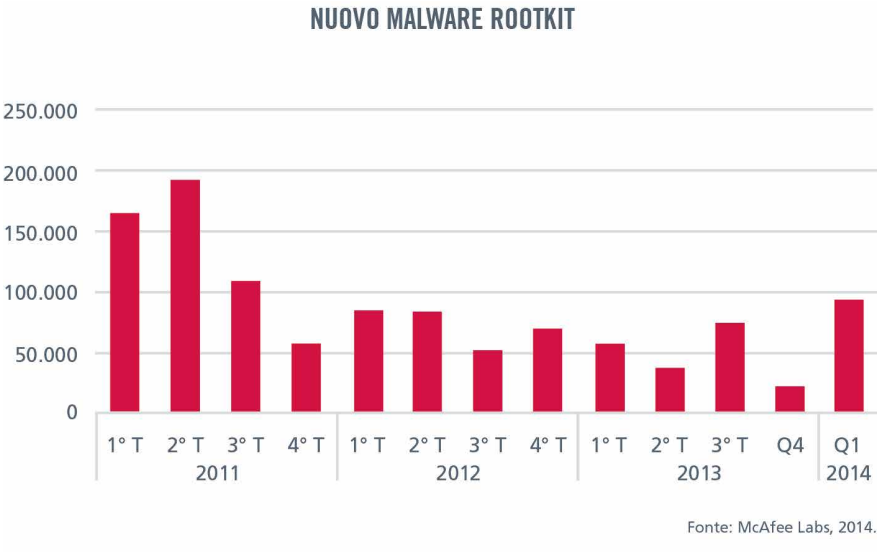
Segui McAfee Labs

Rootkit di nuovo in aumento

All'inizio del 2011, i rootkit avevano raggiunto una diffusione da record. Da allora, McAfee Labs ha rilevato un calo a livelli più modesti, e i dati registrati nell'ultimo trimestre sono i più bassi dal 2008. Attribuiamo il calo all'adozione dei microprocessori a 64 bit, che rendono più difficili gli attacchi al kernel del sistema operativo. Tuttavia, gli aggressori cominciano a trovare dei modi per aggirare le protezioni dei sistemi a 64 bit. Questo trimestre le nuove infezioni da rootkit hanno registrato un nuovo aumento, benché la principale responsabile sia una singola famiglia a 32 bit, il che può rappresentare un'anomalia. Intercettazione di certificati digitali, sfruttamento delle vulnerabilità del kernel, creazione di società fittizie per la firma digitale dei rootkit e attacco alle difese integrate dei sistemi operativi: tutte tattiche per aggirare le protezioni dei sistemi a 64 bit. Riteniamo che queste e altre tecniche porteranno a un aumento degli attacchi rootkit.

Sicurezza delle piattaforme: un ostacolo tangibile per i rootkit

Il brusco calo nel numero di nuovi campioni di rootkit (vedere il grafico) che attaccano Windows rispetto a un paio di anni fa viene attribuito generalmente alla diffusione della piattaforma a 64 bit. Il design dei microprocessori e dei sistemi operativi a 64 bit aumenta la sicurezza del sistema grazie all'applicazione di misure quali il controllo della firma digitale e il componente Kernel Patch Protection per i software che richiedono di essere eseguiti al livello di privilegio più elevato nel kernel.

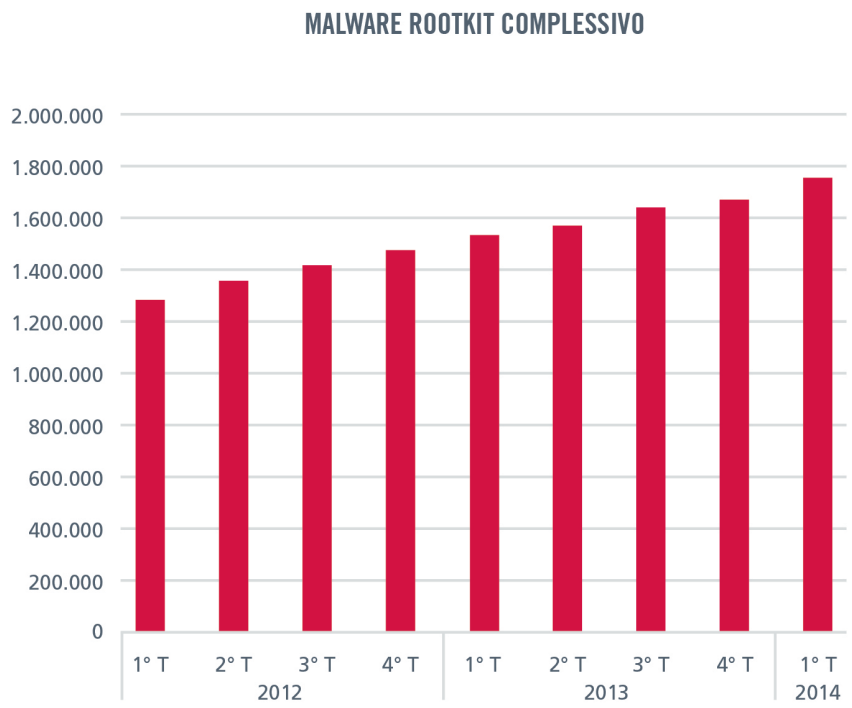


Fonte: McAfee Labs, 2014.

Il numero dei nuovi campioni di rootkit raccolti da McAfee Labs è calato dal 2011 al 2012, e da allora è rimasto relativamente stabile. Siamo convinti che il numero dei nuovi campioni di rootkit riprenderà ad aumentare quando gli aggressori impareranno a eludere le misure di sicurezza dei sistemi a 64 bit.

I microprocessori Intel a 64 bit hanno iniziato a diffondersi in modo massiccio verso la metà degli anni 2000 e sono ormai presenti nella maggior parte dei sistemi. I microprocessori Intel Core i3, i5 e i7 implementano il set di istruzioni a 64 bit.

Segui McAfee Labs



Fonte: McAfee Labs, 2014.

Oltre al rallentamento nel numero di campioni segnalati, abbiamo notato un calo significativo delle tecniche impiegate dai rootkit per ottenere privilegi nel kernel. Gli aggressori non sono più in grado di accedere al kernel con la stessa libertà di cui godevano in passato, e nemmeno di installare driver di dispositivi pericolosi. Queste protezioni hanno sicuramente aumentato i costi di creazione e implementazione dei rootkit sulle piattaforme a 64 bit.

Perché sono così pericolosi i rootkit? Grazie al modo furtivo con cui infettano un sistema, possono restare nascosti e sottrarre informazioni per lunghi periodi di tempo. Più a lungo dura l'infezione, maggiori sono le probabilità che gli aggressori sottraggano o distruggano dati aziendali o personali.

Ostacoli aggirati

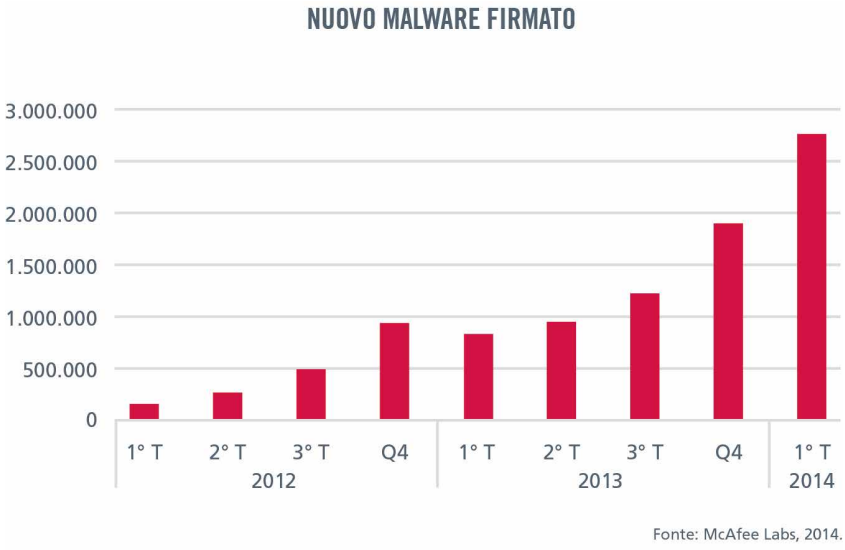
Ormai, gli ostacoli frapposti dai sistemi a 64 bit sembrano poco più che dossi artificiali agli aggressori ben organizzati, che hanno già trovato dei modi per accedere al sistema a livello di kernel.

L'ultimo esempio di elusione pericolosa viene dal rootkit Uroburos[3], che è passato inosservato per tre anni. Uroburos ha sfruttato un vecchio driver del kernel di VirtualBox che aveva una firma digitale valida e una vulnerabilità nota (VirtualBox è una macchina virtuale sviluppata da Oracle). Uroburos ha sfruttato la vulnerabilità del driver del kernel per disabilitare il controllo dei certificati digitali da parte del sistema operativo e caricare il suo malware privo di firma. Una volta caricato nel kernel, il malware disabilitava il componente Kernel Patch Protection — noto anche come PatchGuard — introdotto nei sistemi Windows a 64 bit. PatchGuard impedisce la modifica del kernel tramite patch, una tecnica molto usata dagli aggressori.

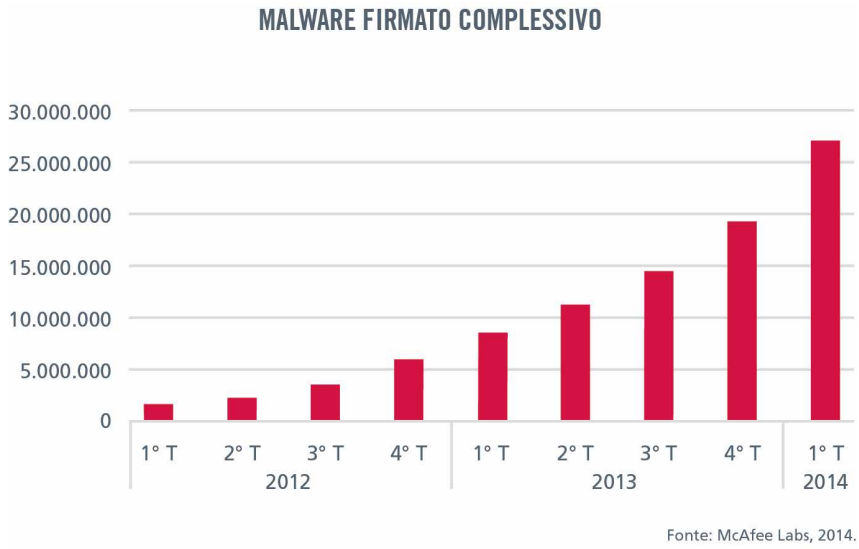
Fiducia mal riposta

Oltre a sfruttare le vulnerabilità dei driver di terzi per ottenere l'accesso al kernel, gli aggressori fanno breccia nei sistemi a 64 bit e li infettano con codice dannoso tramite il furto vero e proprio di chiavi private. Anche una firma digitale valida può essere utile per aggirare le protezioni. Abbiamo osservato una forte tendenza all'aumento in tutti i tipi di file binari malevoli che utilizzano firme digitali (vedere i grafici).

I nuovi file binari firmati pericolosi restano un tipo di attacco molto diffuso, che in questo trimestre è aumentato del 46%.



Fonte: McAfee Labs, 2014.



Fonte: McAfee Labs, 2014.

Segui McAfee Labs

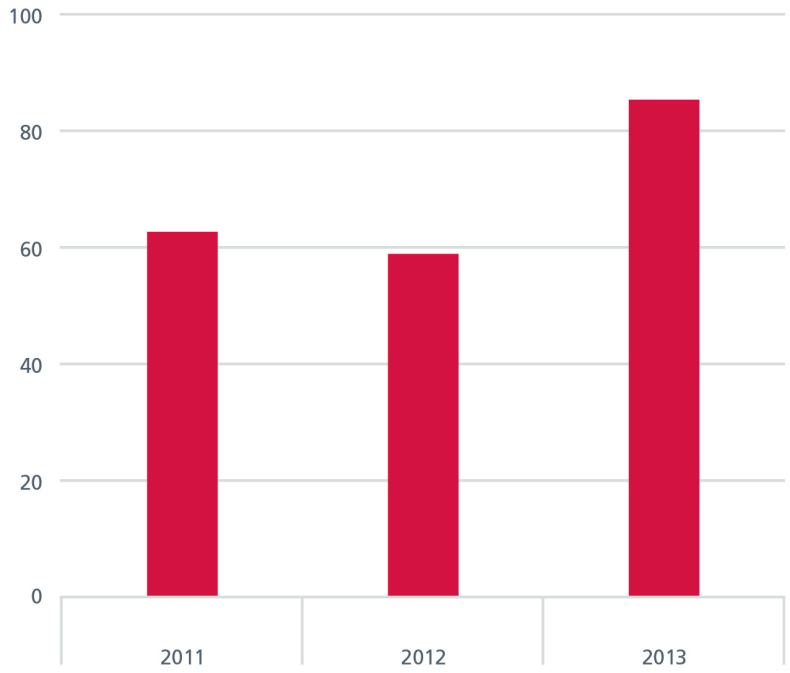
Abbiamo analizzato i dati degli ultimi due anni per vedere quanti rootkit a 64 bit hanno utilizzato certificati digitali rubati. Questi i risultati:

- Dal gennaio 2012, almeno 21 campioni unici di rootkit a 64 bit hanno utilizzato certificati rubati.
- Dal 2012, il malware W64/Winnti ha rubato almeno cinque chiavi private di fornitori legittimi per installare il suo rootkit su sistemi a 64 bit. Di queste cinque, almeno due non sono state revocate e potrebbero essere tuttora in uso, sia per scopi legittimi, sia per scopi illegittimi.
- Almeno un rootkit, W64/Korablin, è stato utilizzato nell'exploit zero-day CVE-2013-0633, forse da aggressori finanziati da governi.

Aumento dei privilegi: kernel zero-day

Negli ultimi anni, il numero di bug legati all'aumento dei privilegi ha subito un incremento, persino nel kernel a 64 bit, più sicuro (vedere il grafico). Parallelamente, anche le metodologie adottate dai ricercatori per individuare le vulnerabilità zero-day nel codice kernel si sono fatte più sofisticate. I ricercatori stanno sviluppando strumenti mirati come le race condition "double fetch" per individuare i difetti nel codice kernel. La storia ci insegna che, quando nella comunità di ricerca inizia un lavoro di questo genere, in breve il suo impatto si manifesta anche nel panorama delle minacce.

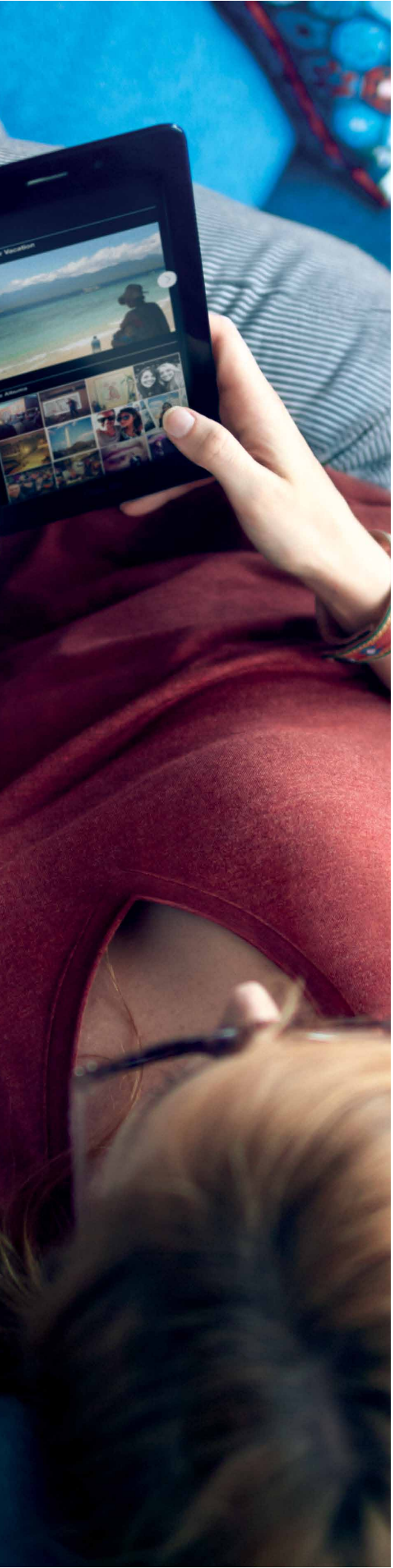
NUOVE VULNERABILITÀ DEL KERNEL DI WINDOWS



Fonte: National Vulnerability Database, 2014.

Nel 2013, il numero di nuove vulnerabilità del kernel in tutte le versioni di Windows è aumentato di oltre il 33%, secondo il National Vulnerability Database.

Segui McAfee Labs



I dati del grafico precedente riguardano solo il kernel Microsoft e i componenti correlati. Ma le vulnerabilità sono numerose anche nei componenti kernel di terzi con firme digitali valide. A nostro avviso, la nuova ondata di attacchi rootkit sfrutterà il numero crescente di vulnerabilità per infiltrarsi nel kernel e assumere il controllo.

Benché i microprocessori e i sistemi operativi Windows a 64 bit abbiano introdotto molte nuove misure di sicurezza, nessun sistema è invulnerabile; con denaro e motivazioni sufficienti, può essere violato. Riteniamo che nei sistemi a 64 bit stia per verificarsi un aumento degli attacchi da parte di malware con firma digitale valida, perché questo sembra il modo più semplice per sfruttare i certificati digitali rubati.

Non possiamo contare esclusivamente sugli ostacoli frapposti da un microprocessore o da un sistema operativo, perché alla lunga saranno aggirati. Il modo migliore per arrestare gli attacchi al kernel consiste nell'adottare protezioni olistiche che abbinino hardware e software, oltre a difese multiple a livello di rete e di endpoint.

Il malware mobile sfrutta le vulnerabilità delle piattaforme, le app e i servizi

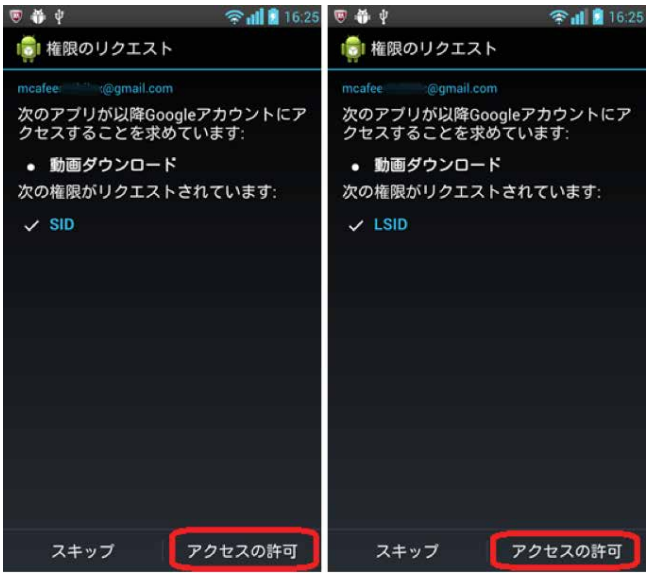
La maggior parte del malware mobile tenta di sottrarre dati sensibili o di inviare SMS a tariffa maggiorata sfruttando le API delle piattaforme standard. In effetti, il malware approfitta delle funzioni ufficiali offerte dalla piattaforma. Di recente, gli sviluppatori di malware hanno iniziato a sfruttare funzioni o vulnerabilità non solo della piattaforma, ma anche di app e servizi legittimi.

Un'app sfrutta le autorizzazioni e l'autenticazione dell'account Google

Sull'app store Google Play, McAfee ha scoperto Android/BadInst.A, un'app per Android sospetta che scarica, installa e lancia automaticamente altre app senza l'autorizzazione dell'utente, che in genere è necessaria per l'installazione manuale di app da Google Play[4]. Poiché questa procedura di conferma in sede di installazione ha un ruolo fondamentale nel garantire la sicurezza di una piattaforma mobile, consentire alle app di saltare questo passaggio comporta rischi non indifferenti per gli utenti dei dispositivi, fra cui quello di installazione invisibile di malware ancora più nocivo.

Android/BadInst.A recupera il nome account di Google dell'utente di un dispositivo e quindi chiede all'utente di essere autorizzata ad accedere a vari servizi Google. Questo avviene mediante AccountManager, un'API standard del framework Android, cui vengono accordate le relative autorizzazioni. In seguito l'app comunica con il server di Google Play utilizzando in modo non ufficiale i token di autorizzazione ottenuti. Infine, l'app scarica, installa e lancia altre app pubblicate su Google Play, senza che vi sia alcun intervento da parte dell'utente.

Il protocollo di comunicazione utilizzato fra il server di Google Play e l'app di servizio omologa sui dispositivi mobili per scaricare e installare automaticamente altre app non è documentato; si tratta di un metodo non ufficiale, non destinato all'uso da parte di app esterne. Sospettiamo che lo sviluppatore di Android/BadInst.A abbia decompilato il protocollo e abbia implementato le medesime procedure nell'app sospetta. Sappiamo inoltre che i token di autorizzazione ottenuti si possono utilizzare per servizi Google diversi da Google Play, per cui è probabile che un malware che sfrutti questo meccanismo di autorizzazione per l'account Google provochi fughe di dati dell'utente ed esegua azioni su vari servizi Google simulandone l'identità.



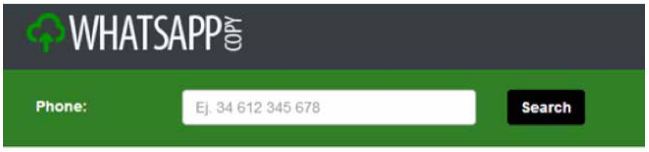
Il malware in giapponese Android/BadInst.A chiede agli utenti l'autorizzazione ad accedere a vari servizi Google.

Un malware sfrutta un servizio di portafoglio digitale e una nota app di messaggistica

Il trojan Android/Waller.A approfitta di una falla di sicurezza in un servizio di portafoglio digitale legittimo per rubare denaro[5]. Il malware sfrutta il protocollo di trasferimento del denaro utilizzato da Visa QIWI Wallet. Questo malware viene installato camuffato da aggiornamento di Adobe Flash Player o di un'altra utilità legittima, e dopo l'installazione viene nascosto dalla schermata iniziale. In background, il malware controlla se l'utente del dispositivo ha un account di portafoglio digitale e se nel portafoglio è presente del denaro, intercetta la risposta di conferma e infine trasferisce il denaro al server dell'aggressore. In questo caso, il malware sfrutta il protocollo che consente di eseguire queste operazioni mediante SMS senza un grado di autenticazione sufficiente, simulando a tutti gli effetti l'app ufficiale.

Il malware Android/Waller.A camuffato da Adobe Flash Player.

McAfee Labs ha scoperto anche il trojan Android/Balloonpopper.A, che sfrutta una debolezza del metodo di crittografia di WhatsApp[6], la popolare app di messaggistica. Fingendo di essere un gioco di nome BalloonPop, questo malware sottrae le conversazioni e le foto di WhatsApp memorizzate sul dispositivo, inviandole segretamente al server remoto dell'aggressore. In seguito, questi le decrittograferà e le pubblicherà sul suo sito Web[7]. Anche se ormai questa vulnerabilità è stata risolta, è facile immaginare che i criminali informatici siano continuamente alla ricerca di altre falle in quest'app diffusissima.



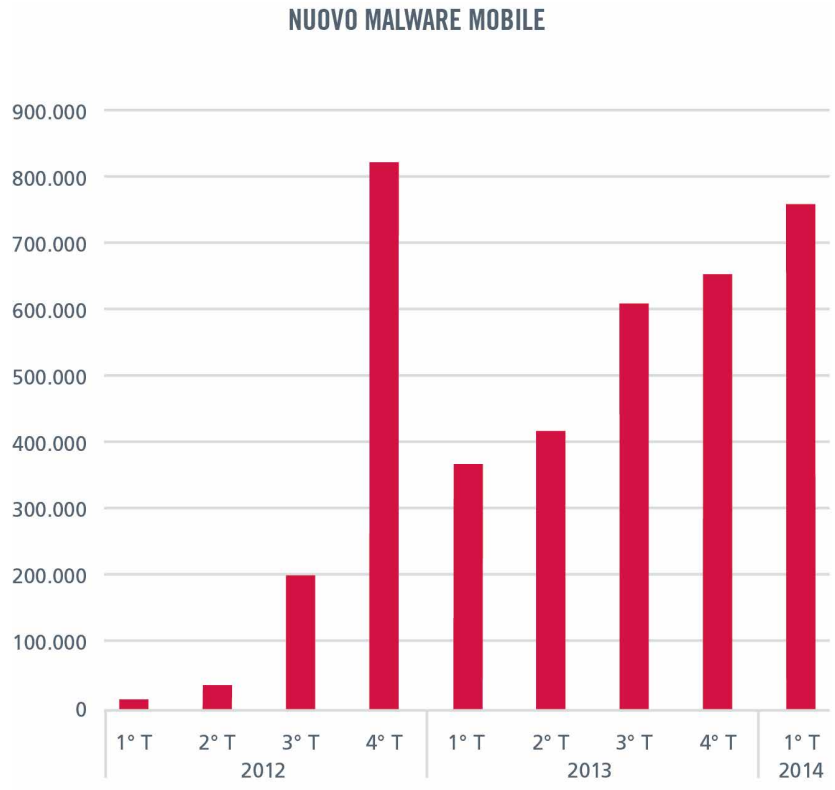
Il sito Web dell'aggressore può divulgare le conversazioni sottratte da WhatsApp.

Piattaforme e app hanno bisogno di protezione

Come si vede da questi esempi, per eludere i sistemi di sorveglianza tradizionali degli app store e dei prodotti di sicurezza il malware mobile ultimamente ha iniziato a utilizzare app e servizi legittimi, oltre alle funzioni standard delle piattaforme. Di conseguenza, non è più sufficiente proteggere la piattaforma sottostante. Riteniamo che gli sviluppatori debbano proteggere app e servizi da usi illegittimi e non autorizzati. Inoltre, gli app store devono garantire che l'accesso ai dati avvenga esclusivamente da parte di app client autenticate e autorizzate. Queste operazioni sono essenziali quando un'app dispone di privilegi più ampi del normale o si occupa di transazioni bancarie, pagamenti e altri dati estremamente sensibili. In sede di installazione e di esecuzione, gli utenti non devono accettare richieste di autorizzazione strane o eccessive. Inoltre, dovrebbero aggiornare le app per risolvere i problemi di sicurezza quando vengono scoperte delle vulnerabilità, e ovviamente evitare tutte le app considerate non sicure.

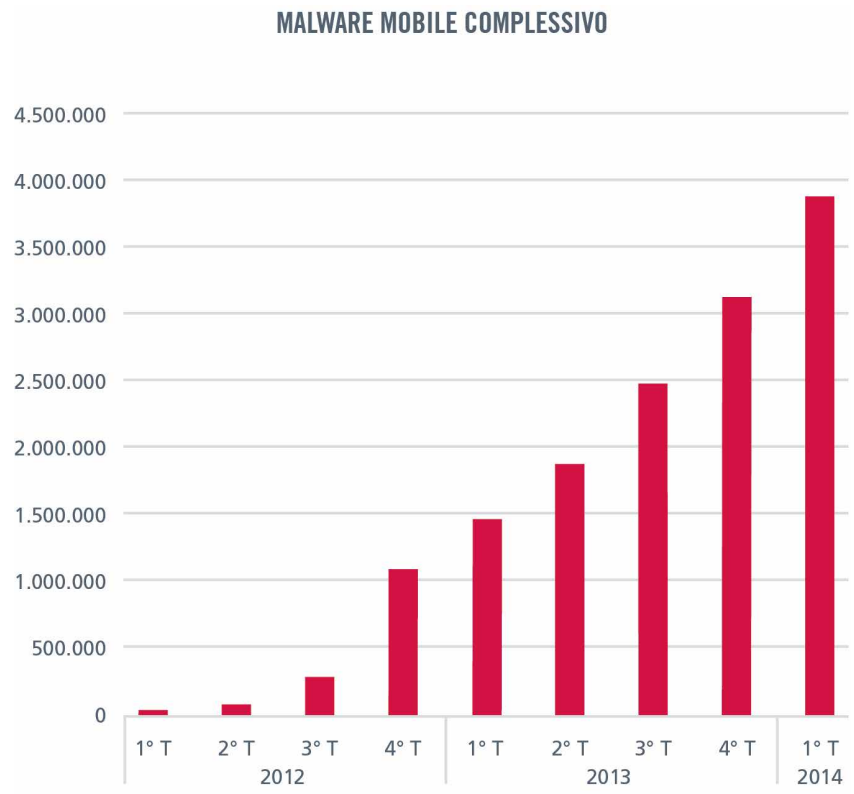
STATISTICHE SULLE MINACCE

Malware mobile



Fonte: McAfee Labs, 2014.

In un solo anno, il numero totale dei campioni di malware mobile è aumentato del 167%.



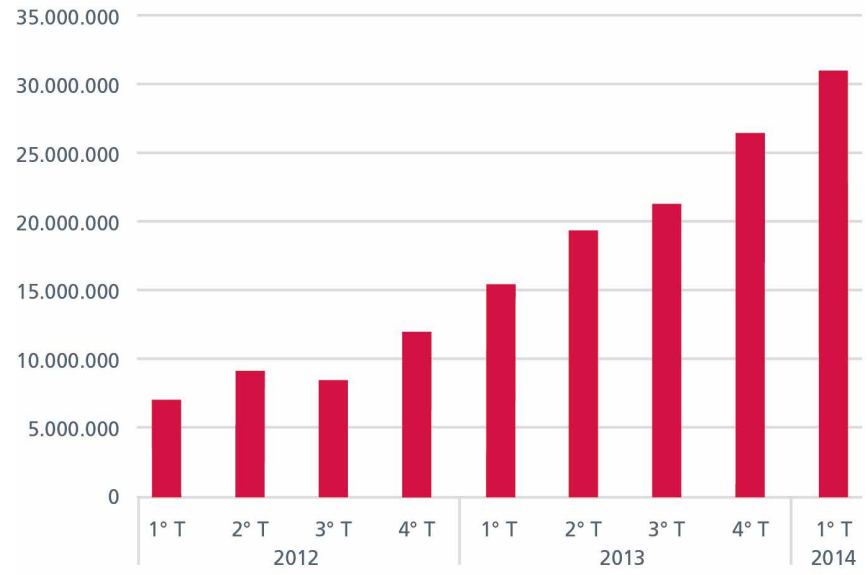
Fonte: McAfee Labs, 2014.

A partire dal *Report McAfee Labs sulle minacce: terzo trimestre 2013,* abbiamo modificato il nostro modo di presentare il malware mobile, sostituendo il conteggio delle famiglie di malware con quello dei campioni unici (conteggio degli hash). Lo abbiamo fatto per due motivi: in primo luogo, volevamo che il metodo utilizzato per il malware mobile fosse coerente con il modo in cui presentiamo tutto il malware; in secondo luogo, presentando il totale delle varianti anziché il totale delle famiglie di malware mobile, forniamo un quadro complessivo più preciso delle modalità con cui il malware mobile colpisce gli utenti.

Segui McAfee Labs

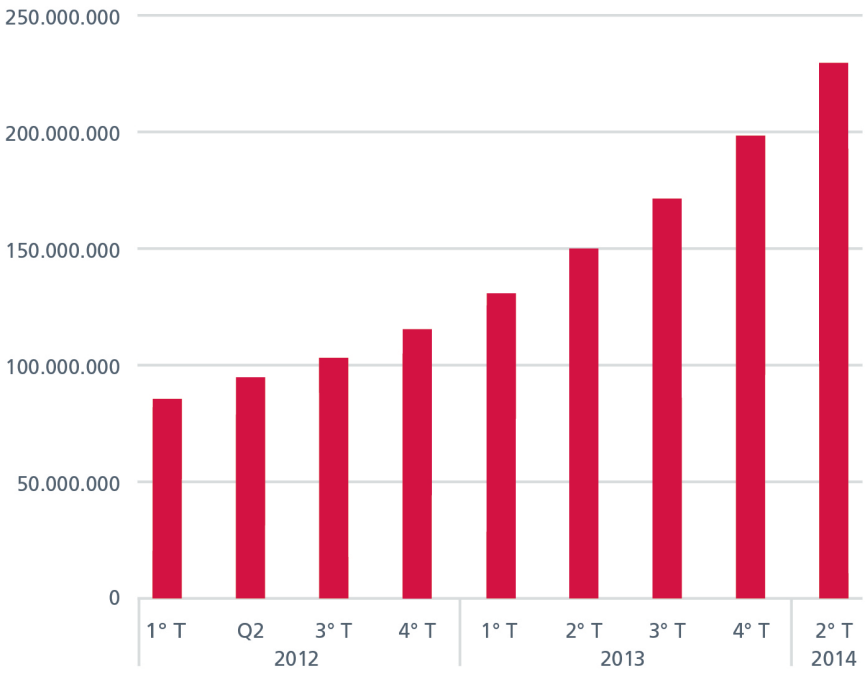
Malware

NUOVO MALWARE



Fonte: McAfee Labs, 2014.

MALWARE COMPLESSIVO



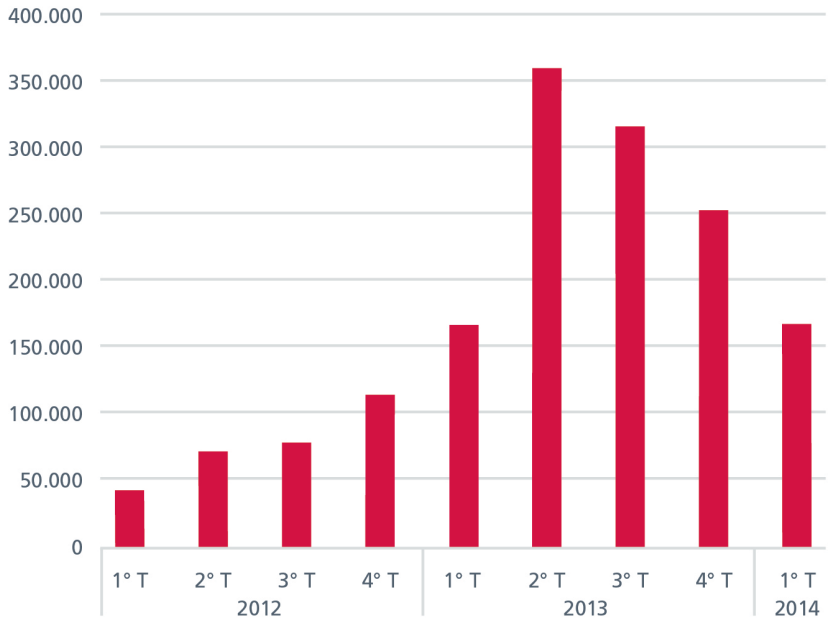
Fonte: McAfee Labs, 2014.

La marcia continua.
Nel 1° trimestre 2014 il numero totale dei campioni di malware presenti nello "zoo" di McAfee Labs ha superato la barriera dei 200 milioni.

Segui McAfee Labs

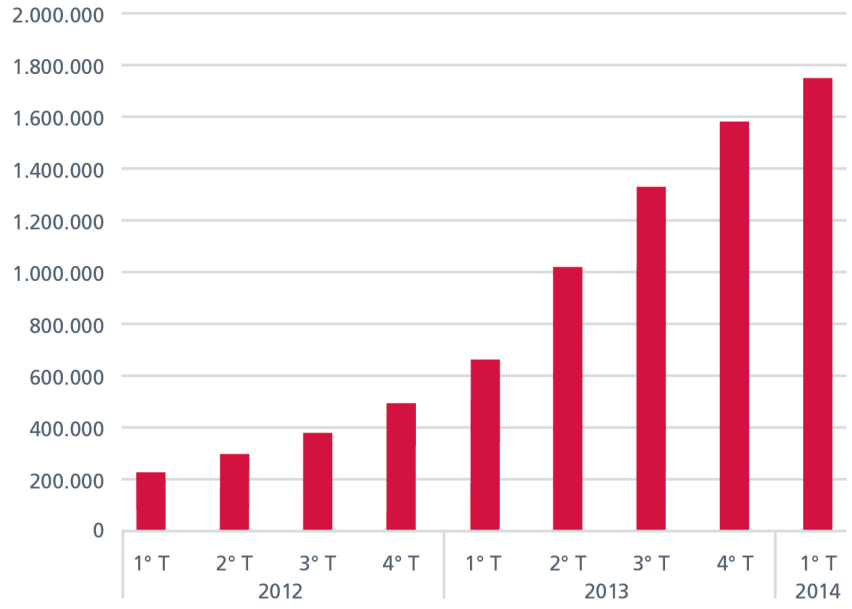
Il numero di nuovi campioni di ransomware è in calo da tre trimestri consecutivi. McAfee Labs ha confermato che la tendenza non è dovuta a un'anomalia. Abbiamo diverse teorie per spiegare i motivi di quanto sta accadendo, ma non abbiamo individuato una causa specifica. È anche possibile che quello attuale sia il punto più basso prima di un nuovo aumento: è già successo con molti altri tipi di malware.

NUOVO RANSOMWARE



Fonte: McAfee Labs, 2014.

RANSOMWARE COMPLESSIVO

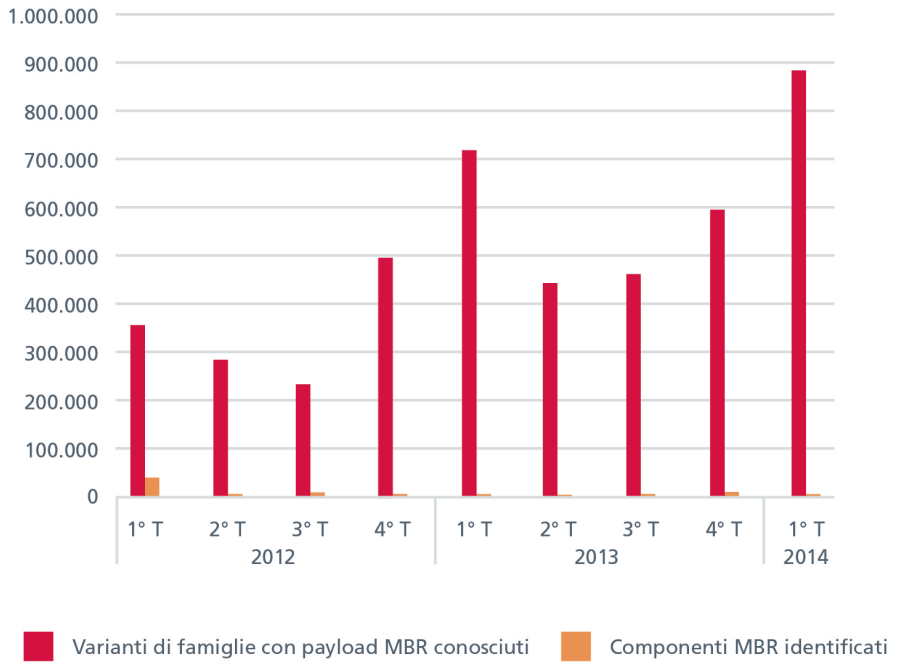


Fonte: McAfee Labs, 2014.

Segui McAfee Labs

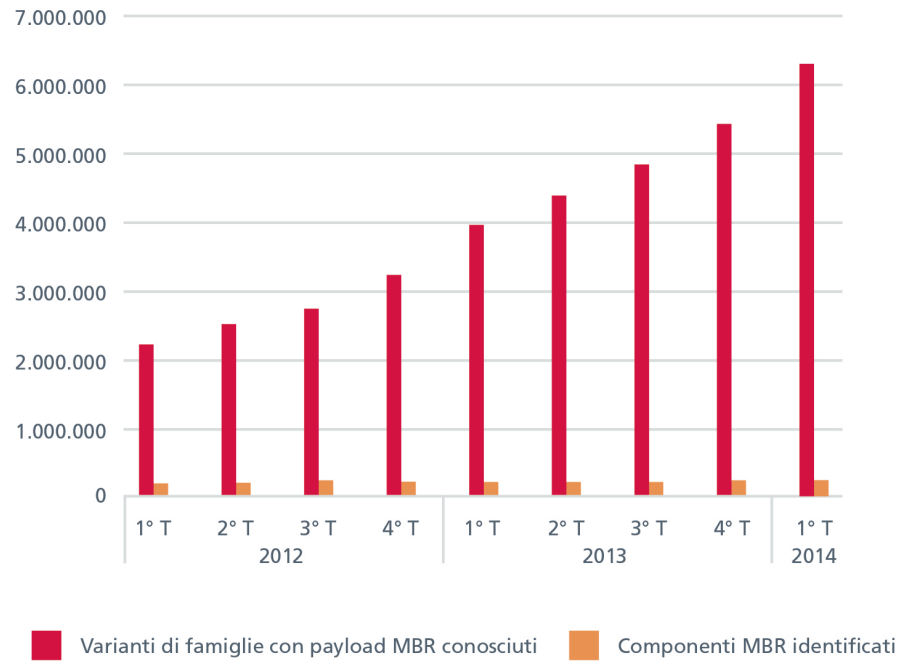
In questo periodo, le nuove minacce che attaccano il record di avvio principale sono aumentate del 49%, toccando un massimo finora mai raggiunto per un singolo trimestre.

NUOVO MALWARE LEGATO AL RECORD DI AVVIO PRINCIPALE



Fonte: McAfee Labs, 2014.

MALWARE LEGATO AL RECORD DI AVVIO PRINCIPALE COMPLESSIVO



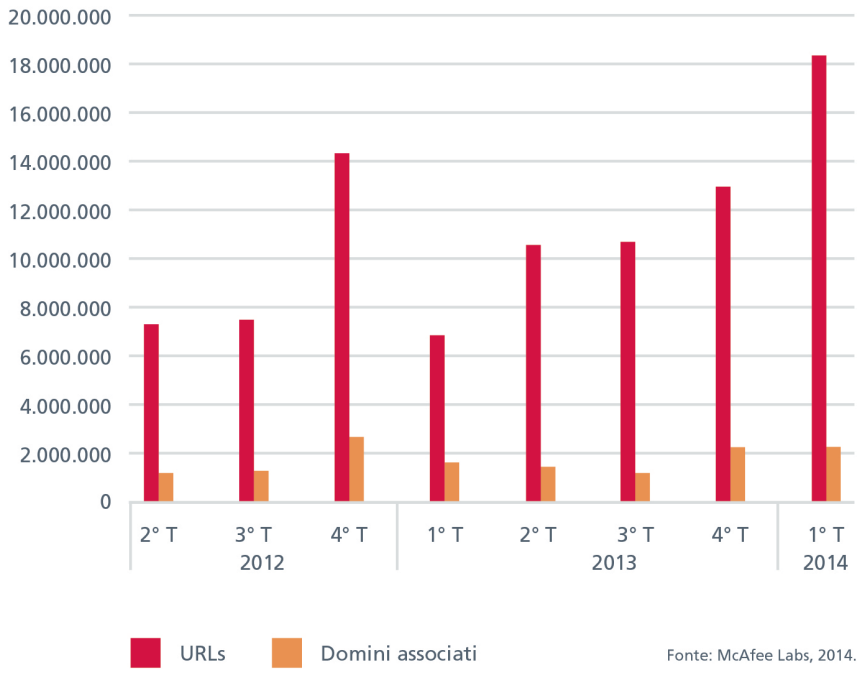
Fonte: McAfee Labs, 2014.

Segui McAfee Labs

Minacce Web

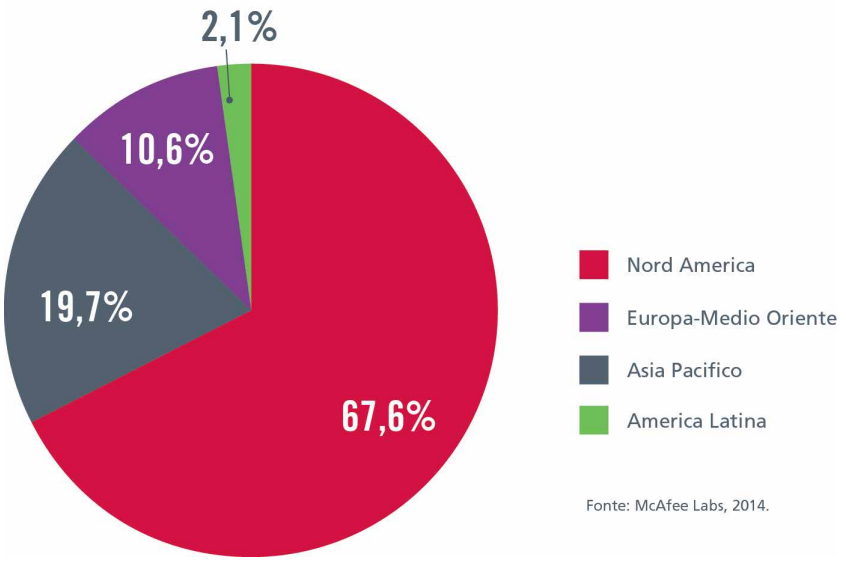
Il conteggio dei nuovi URL sospetti da parte di McAfee Labs ha registrato un record trimestrale con oltre 18 milioni di URL: un aumento del 19% rispetto al 4° trimestre e il quarto aumento trimestrale consecutivo.

NUOVI URL SOSPETTI



Fonte: McAfee Labs, 2014.

POSIZIONE DEI SERVER CON CONTENUTI SOSPETTI



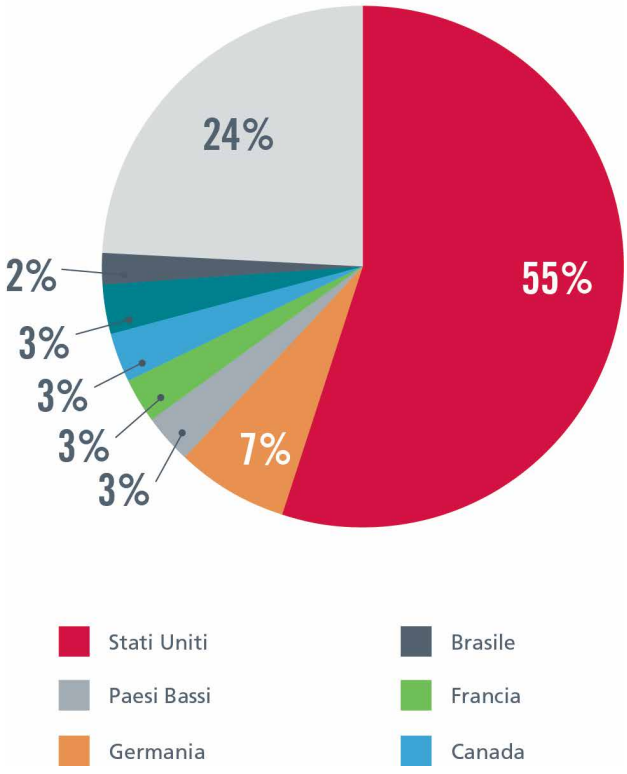
Fonte: McAfee Labs, 2014.

Segui McAfee Labs

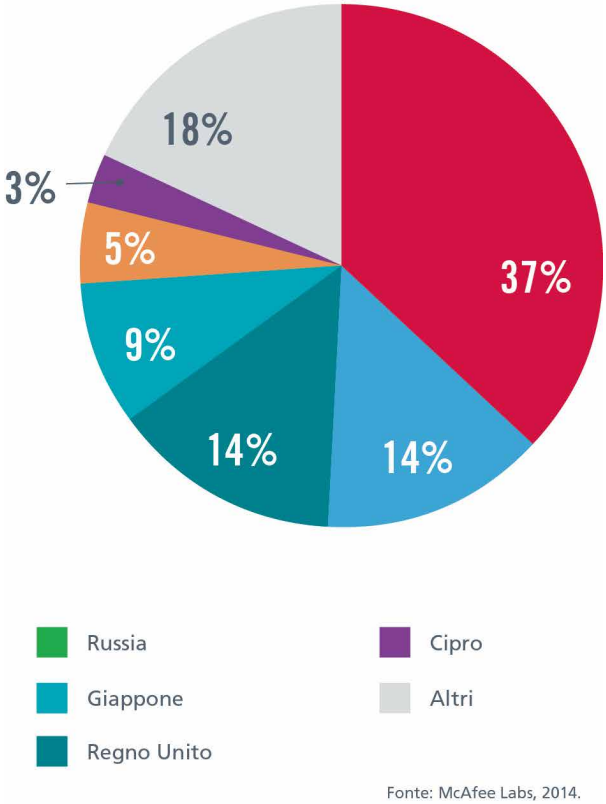
NUOVI URL DI PHISHING

Fonte: McAfee Labs, 2014.

PRINCIPALI NAZIONI CHE OSPITANO URL DI PHISHING



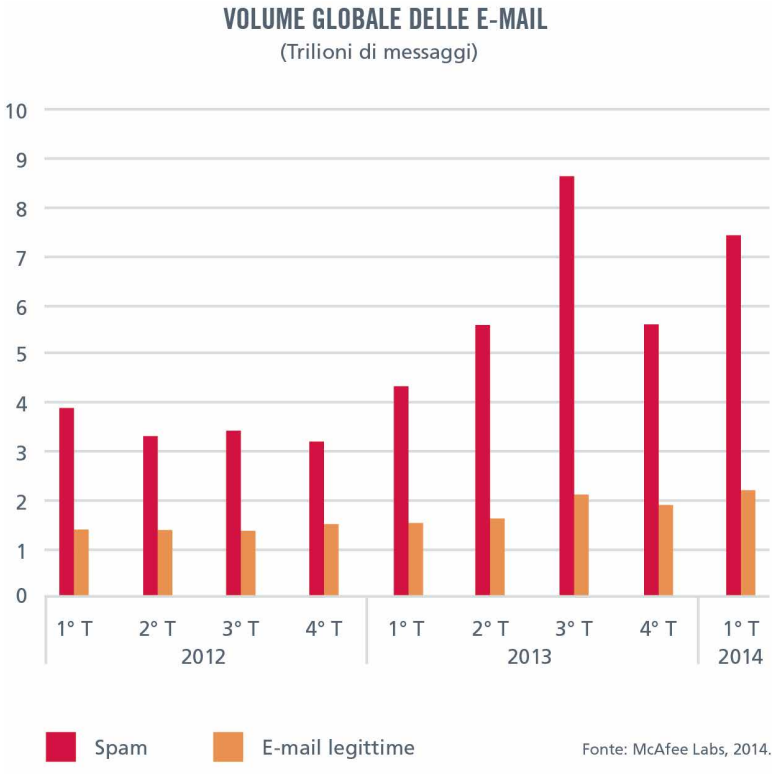
PRINCIPALI NAZIONI CHE OSPITANO URL DI SPAM

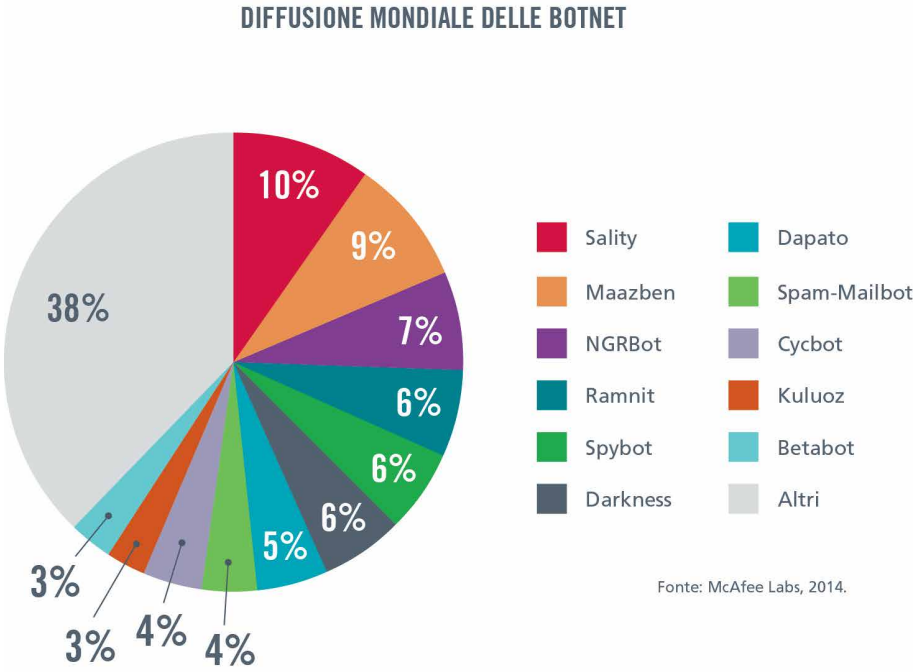


Fonte: McAfee Labs, 2014.

Segui McAfee Labs

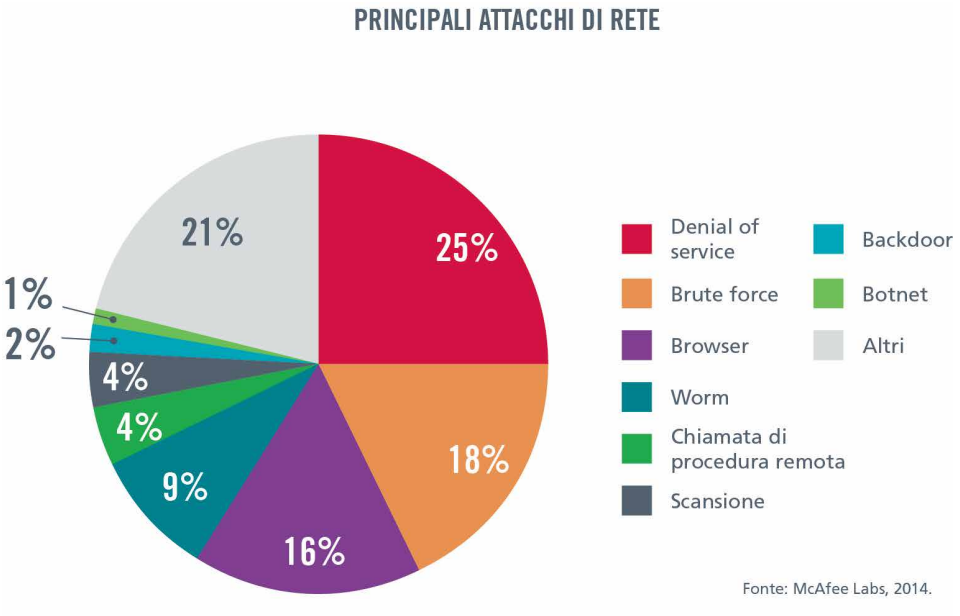
Minacce per la messaggistica





Segui McAfee Labs

Minacce di rete



Segui McAfee Labs

McAFEE

McAfee, parte di Intel Security e società interamente controllata da Intel Corporation (NASDAQ: INTC), consente ad aziende, pubbliche amministrazioni e utenti consumer di usufruire dei vantaggi di Internet in modo sicuro. L'azienda offre prodotti e servizi di sicurezza riconosciuti e proattivi che proteggono sistemi, reti e dispositivi mobili in tutto il mondo. Grazie alla lungimirante strategia Security Connected, a un approccio innovativo alla sicurezza potenziata dall'hardware e all'esclusiva rete Global Threat Intelligence, McAfee è impegnata senza sosta nella ricerca di nuovi modi per garantire protezione ai propri clienti.

http://www.mcafee.com/it

1 La difficoltà è la misura della quantità di lavoro (elaborazione) necessaria per generare catene di blocchi. Il protocollo Bitcoin prevede che la difficoltà sia ricalcolata ogni 2.016 blocchi (circa ogni due settimane).

2 L'hash rate è la misura delle prestazioni dell'hardware in relazione alle operazioni eseguite nella rete di mining.

3 http://blogs.mcafee.com/mcafee-labs/analyzing-uroburos-patchguard-bypass

4 http://blogs.mcafee.com/mcafee-labs/automatic-app-installation-google-play-store-poses-big-risk

5 http://home.mcafee.com/virusinfo/virusprofile.aspx?key=7358408

6 http://blogs.mcafee.com/mcafee-labs/androidballoonpopper-sums-up-mobile-threat-landscape-in-2013

7 http://blogs.mcafee.com/consumer/whatsapp-security-flaw

61158rpt_qtr-q1_0614_fnl