Evoluzione delle minacce informatiche nel primo trimestre del 2014

David Emm
Victor Chebyshev
Roman Unuchek
Marija Garnaeva

Il trimestre in cifre:

- Secondo i dati raccolti tramite il Kaspersky Security Network (KSN), lungo tutto l'arco del primo trimestre del 2014 i prodotti Kaspersky Lab hanno rilevato e neutralizzato 1.131.000.866 attacchi nocivi nei confronti dei computer e dei dispositivi mobile degli utenti.
- Le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 353.216.351 attacchi condotti attraverso siti Internet compromessi dislocati in vari paesi.
- Il nostro anti-virus web ha effettuato il rilevamento di 29.122.849 oggetti nocivi unici (script, pagine web, exploit, file eseguibili, etc.).
- In totale, sono stati individuati e bloccati, da parte del nostro modulo anti-virus web, 81.736.783 URL unici.
- Il 39% degli attacchi web bloccati e neutralizzati grazie all'intervento dei prodotti anti-malware di Kaspersky Lab è stato condotto attraverso siti web nocivi dislocati sul territorio di Stati Uniti e Russia.
- Le nostre soluzioni anti-virus hanno rilevato con successo 645.809.230 attacchi sui computer degli utenti che fanno parte del Kaspersky Security Network. Complessivamente, nel corso di tali incidenti, sono stati registrati ben 135.227.372 oggetti maligni unici o potenzialmente indesiderabili.

Il quadro della situazione

Attacchi mirati / APT

La nebbia continua a diradarsi

Nell'ultima decade del mese di settembre 2013, all'interno del nostro blog dedicato alle tematiche di sicurezza IT, abbiamo riferito in merito ad un intenso e chirurgico attacco informatico di natura mirata, denominato Icefog, volto a colpire principalmente obiettivi nella Corea del Sud e in Giappone. La maggior parte delle campagne APT (Advanced Persistent Threat, minacce informatiche di tipo avanzato e persistente), come è noto, durano diversi mesi, se non addirittura anni interi, sottraendo in continuazione preziosi dati sensibili dai computer-vittima presi di mira. Per contro, gli "attaccanti" che si nascondono dietro l'operazione di spionaggio informatico comunemente definita Icefog sembrano “occuparsi” delle proprie vittime in maniera singola e dedicata, individuando e copiando solo informazioni specifiche, ben mirate. Una volta che le informazioni desiderate sono state ottenute, mediante sofisticati attacchi riconducibili alla tipologia del "mordi e fuggi", il gruppo APT in questione -

una piccola, ma potente, "gang" di criminali informatici - molla rapidamente la presa. La campagna di cyber-spionaggio qui analizzata risulta essere operativa almeno dal 2011; essa ha comportato il dispiegamento di tutta una serie di differenti versioni del malware "Icefog", incluso una versione appositamente sviluppata dai virus writer per colpire il sistema operativo Mac OS X.

Dopo la pubblicazione del nostro report, le operazioni condotte dal gruppo Icefog sono improvvisamente cessate; è stato nella circostanza rilevato come gli "attaccanti" abbiano rapidamente provveduto a smantellare tutti i server C&C (Command and Control Center) sino a quel momento conosciuti. Il team di ricercatori di Kaspersky Lab ha continuato a monitorare con attenzione questa campagna di spionaggio informatico, conducendo vaste operazioni di sinkhole (su una significativa parte degli oltre 70 domini utilizzati dal gruppo Icefog) ed analizzando le connessioni relative alle "vittime" degli attacchi. L'analisi effettuata dai nostri esperti - tuttora in corso - ha rivelato l'esistenza di un'ulteriore generazione di backdoor Icefog; si tratta, nello specifico, di una versione Java del malware, da noi denominata "Javafog". Le connessioni effettuate tramite uno dei domini sottoposti alle procedure di sinkhole, <lingdona[dot]com>, hanno evidenziato che il client avrebbe potuto essere un'applicazione Java; l'indagine successiva ha portato alla luce un sample di tale applicazione (informazioni dettagliate sull'analisi condotta dai nostri esperti sono disponibili qui).

Durante l'operazione di sinkhole sono stati da noi complessivamente osservati otto indirizzi IP relativi a tre vittime uniche del Javabot, tutte quante ubicate sul territorio degli Stati Uniti. Una di esse è risultata essere un'importantissima corporation indipendente, operante nel settore petrolifero e del gas, attiva in numerosi paesi. E' possibile che il malware Javafog sia stato appositamente sviluppato per condurre un'operazione di spionaggio informatico rivolta specificamente agli USA, una campagna APT destinata, tra l'altro, a durare ben più a lungo rispetto alla normale durata degli attacchi portati dal gruppo Icefog. Una delle probabili ragioni che hanno indotto i cybercriminali a sviluppare una versione Java del malware qui analizzato risiede nel fatto che un oggetto maligno del genere è in grado di agire in maniera ancor più subdola e furtiva, ed il suo rilevamento, inoltre, risulta ben più difficile e complesso.

Dietro la maschera

Nello scorso mese di febbraio, il Global Research & Analysis Team (GReAT) di Kaspersky Lab ha pubblicato un dettagliato report riguardo ad una complessa campagna di cyber-spionaggio denominata "The Mask" o "Careto" (termine che, nello slang spagnolo, significa, in effetti, "maschera" o "brutta faccia"). L'operazione, anch'essa riconducibile al quadro delle minacce APT, è stata appositamente progettata per realizzare il furto di preziosi dati sensibili ed ha interessato obiettivi di vario genere. Le vittime di tali sofisticati attacchi mirati, distribuiti in 31 diversi paesi del mondo, sono risultate essere, principalmente, agenzie ed enti governativi, ambasciate, società operanti nel settore energetico, istituti di ricerca, società per azioni private ed attivisti; il quadro completo dei target colpiti da "The Mask" può essere consultato qui.

Gli attacchi informatici in questione iniziano con l'invio di un messaggio e-mail di spear-phishing, contenente un link che conduce la vittima predestinata verso un sito web nocivo contenente numerosi exploit. Una volta infettato, il bersaglio dell'assalto IT viene rediretto

verso il sito legittimo descritto nell'e-mail precedentemente ricevuta (portale di news, servizio video YouTube, etc.). The Mask comprende un sofisticato trojan backdoor in grado di intercettare tutti i canali di comunicazione e di raccogliere, quindi, ogni genere di dati dal computer sottoposto ad attacco. Così come per Red October ed altri precedenti attacchi mirati, il codice del malware utilizzato dai cybercriminali si è rivelato altamente modulare, per cui gli "attaccanti" possono aggiungere in qualsiasi momento nuove funzionalità, a loro piacimento. The Mask è, in sostanza, un potente attack toolkit multipiattaforma; sono state in effetti rilevate sia versioni del backdoor destinate al sistema operativo Windows, sia versioni rivolte alla piattaforma Mac OS X. Alcuni specifici elementi individuati dai nostri esperti indicano poi la possibile esistenza di versioni del malware appositamente sviluppate per attaccare i sistemi operativi Linux, iOS ed Android. Per celare le attività nocive svolte all'interno della macchina sottoposta ad attacco, il trojan qui analizzato si avvale inoltre di tecniche di occultamento particolarmente sofisticate.

Lo scopo principale degli aggressori che si nascondono dietro The Mask consiste nel sottrarre dati sensibili alle proprie vittime. Il potente malware provvede in effetti a raccogliere tutta una serie di dati ed informazioni dal sistema sottoposto a contagio informatico, incluso chiavi crittografiche, configurazioni VPN, chiavi SSH, file RDP ed alcuni tipi di file dall'estensione sconosciuta, che potrebbero essere legati a strumenti di codifica personalizzati, operanti a livello militare/governativo.

Non sappiamo, di fatto, chi si possa nascondere dietro l'enigmatica "maschera", chi siano, in realtà, gli "attori" che tengono sapientemente le fila di tale complessa campagna di cyber-spionaggio. Anche l'uso stesso della lingua spagnola per ciò che riguarda la denominazione alternativa di The Mask non rappresenta un elemento particolarmente significativo nella ricerca di possibili attribuzioni e responsabilità, in quanto si tratta di una lingua ampiamente utilizzata in molte aree del globo. E' probabile che tale fattore sia stato volutamente introdotto per costituire un falso indizio, ovvero per distogliere il più possibile le attenzioni nei confronti dei reali autori del malware. L'elevato grado di professionalità dimostrato dal gruppo che si nasconde dietro questa serie di sofisticati attacchi informatici risulta piuttosto inusuale perché questi ultimi possano essere attribuiti ad una delle classiche ed ordinarie "gang" di cybercriminali; tale elemento indica piuttosto come The Mask possa essere, di fatto, una campagna di cyber-spionaggio sponsorizzata a livello di nazioni.

Le peculiarità che contraddistinguono la campagna di spionaggio cibernetico descritta nel presente capitolo del nostro report trimestrale dedicato all'evoluzione delle minacce IT evidenziano, a tutti gli effetti, come tale operazione sia stata condotta da "attaccanti" professionali, in possesso delle necessarie risorse e competenze per sviluppare al meglio un genere di malware particolarmente complesso, volto a realizzare il furto di preziose informazioni di natura sensibile. L'indagine svolta dai nostri esperti di sicurezza informatica riguardo a The Mask - o Careto - pone ancora una volta in evidenza il fatto che i cosiddetti attacchi mirati sono davvero in grado di non essere rilevati (flying under the radar), in quanto,

al di là delle vittime specificamente designate, essi generano un livello di attività estremamente ridotto - o addirittura nessun tipo di attività dannosa aggiuntiva.

E' tuttavia importante riconoscere come, nonostante il livello altamente sofisticato raggiunto da The Mask, il punto di partenza di tale campagna di spionaggio (così come è avvenuto per numerosi attacchi mirati condotti in precedenza) sia comunque rappresentato dal fatto di "insidiare" ed ingannare singoli individui, inducendo questi ultimi a compiere azioni che, di fatto, vanno poi a minare pesantemente la sicurezza dell'organizzazione per cui lavorano; come abbiamo visto è sufficiente cliccare su un semplice link nocivo per scatenare un processo di particolare complessità.

Al momento attuale, ad ogni caso, tutti i server C&C (Command-and-Control) conosciuti nell'ambito dell'operazione Careto, utilizzati per generare e gestire le infezioni informatiche prodotte sui computer delle vittime, risultano offline. E' tuttavia possibile che, in un prossimo futuro, i responsabili degli attacchi informatici in questione riprendano, con rinnovato vigore, la conduzione di tale campagna di cyber-spionaggio, analizzata in dettaglio dai nostri ricercatori.

Il worm ed il serpente

Nella prima metà del mese di marzo 2014 si è accesa un'ampia discussione all'interno della community degli esperti di sicurezza IT, relativamente ad una campagna di cyber-spionaggio denominata in codice "Turla" (altrimenti conosciuta con l'appellativo di "Snake" od "Uroburos", il nome dell'antico simbolo che raffigura il serpente che si morde la coda). I ricercatori di G-DATA sostengono che il malware di tale operazione di spionaggio informatico possa essere stato creato dai servizi speciali russi. Le ricerche condotte da BAE Systems hanno collegato Turla al malware soprannominato "Agent.btz", risalente al 2007, il quale era stato utilizzato nel corso del 2008 per infettare le reti locali adibite alle operazioni militari statunitensi nello scacchiere mediorientale.

I nostri esperti di sicurezza IT sono venuti a conoscenza della campagna mirata in questione mentre stavano svolgendo un'indagine riguardo ad un incidente che vedeva coinvolto un rootkit altamente sofisticato, poi battezzato con il nome di "Sun rootkit" dagli analisti di Kaspersky Lab. E' così emerso in maniera piuttosto rapida come, in sostanza, "Sun rootkit" e "Uroburos" fossero la stessa identica cyber-minaccia.

Al momento attuale, stiamo ancora conducendo indagini riguardo a Turla, in quanto crediamo che tale malware sia, di fatto, ben più complesso di quanto suggerisca la lettura del materiale informativo sinora pubblicato a tal proposito. La nostra analisi iniziale, tuttavia, ha evidenziato alcuni interessanti collegamenti e relazioni.

Agent.btz è un worm auto-replicante in grado di diffondersi attraverso le unità flash USB, grazie allo sfruttamento di una particolare vulnerabilità che permette di lanciare l'esecuzione di tale software nocivo mediante <autorun.inf>. Copiando se stesso da un flash drive USB

all'altro, il suddetto malware si è così diffuso rapidamente in tutto il mondo. Nonostante per molti anni non siano state create *nuove* varianti del worm e, nel frattempo, la vulnerabilità sopra menzionata sia stata chiusa nelle versioni più recenti di Windows, solo nel corso del 2013 Agent.btz è stato rilevato ben 13.832 volte, in 107 paesi!

Il worm in causa crea un file chiamato <thumb.dll> su tutte le unità flash USB che vengono collegate al computer infetto (file adibito a contenere, a sua volta, i file <winview.ocx>, <wmcache.nld> e <mssysmgr.ocx>). Si tratta, quindi, di un vero e proprio contenitore per i dati sensibili sottratti, i quali vengono salvati sul flash drive nel caso in cui gli stessi non possano essere inviati tramite Internet al server di comando e controllo appositamente predisposto dagli attaccanti. Se il flash drive "contaminato" viene poi inserito in un altro computer, il file <thumb.dll> verrà automaticamente copiato sul nuovo computer, con il nome <mssysmgr.ocx>.

Riteniamo, da parte nostra, che in ragione dell'effettiva portata dell'epidemia informatica descritta nel presente capitolo del report - combinata alla specifica funzionalità qui sopra illustrata - possano al giorno d'oggi esistere, in tutto il mondo, decine di migliaia di unità flash USB contenenti i famigerati file denominati <thumb.dll>, creati dal malware Agent.btz. Attualmente, la maggior parte delle varianti del malware esaminato vengono rilevate dai prodotti Kaspersky Lab come "Worm.Win32.Orbina".

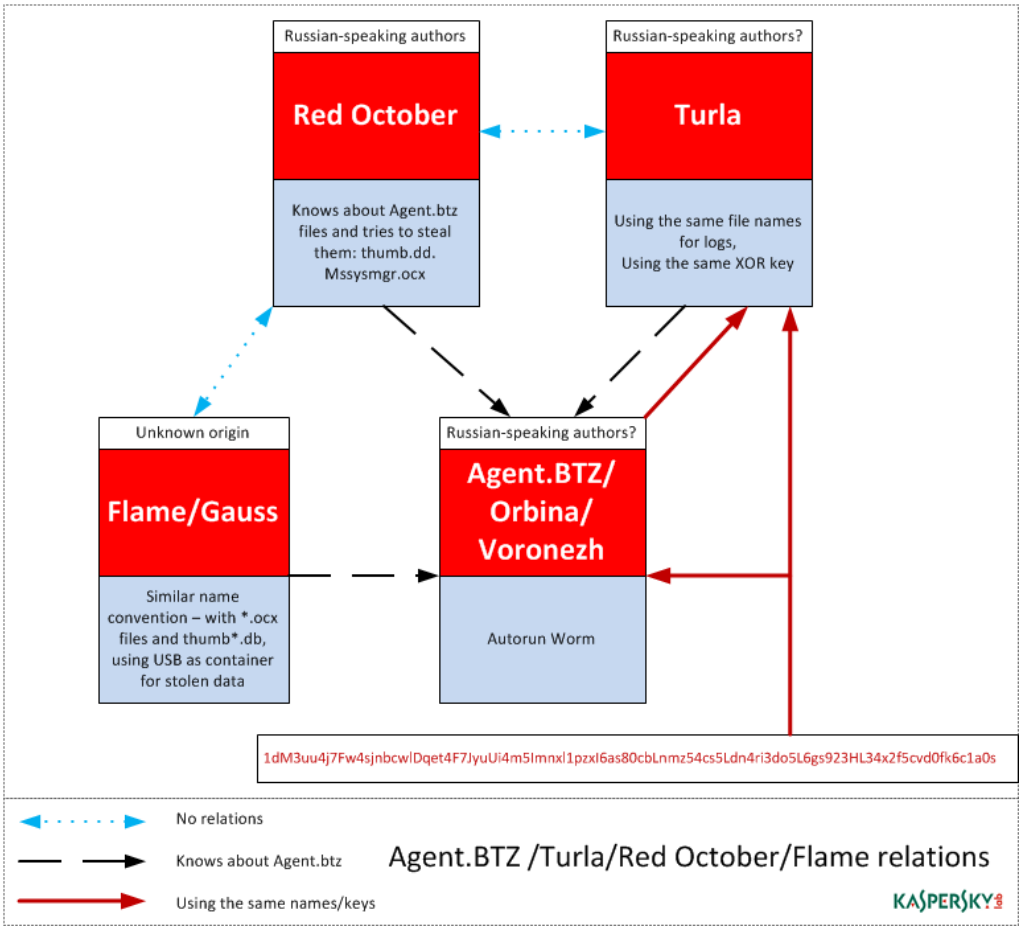
Naturalmente, il worm Agent.btz non costituisce l'unica minaccia informatica in grado di diffondersi tramite le unità flash USB.

Il modulo "USB Stealer", ad esempio, utilizzato nel quadro dell'estesa campagna di cyber-spionaggio denominata Red October (Ottobre Rosso), include uno specifico elenco di file che esso provvede a ricercare sui flash drive USB collegati ai computer infetti. I nostri esperti hanno osservato che questo elenco comprende anche i file <mysysmgr.ocx> e <thumb.dll>, vale a dire due dei file abitualmente trasferiti su flash drive dal malware Agent.btz.

Nel momento in cui i nostri ricercatori hanno provveduto ad analizzare alcuni dei più sofisticati strumenti utilizzati nelle campagne globali di spionaggio informatico - ovvero il malware Flame ed i suoi due illustri "cugini", Gauss e miniFlame - siano ugualmente emerse alcune indiscutibili similarità con il worm Agent.btz. In primo luogo, è risultata del tutto analoga la modalità utilizzata dagli aggressori nel nominare i file, ed in particolar modo il ricorso all'estensione <.ocx>. Oltre a ciò, è stato rilevato come, sia Gauss che miniFlame, "conoscessero" bene, in maniera del tutto evidente, il file <thumb.dll>, da essi costantemente ricercato sui flash drive USB.

E' infine emerso come Turla, per ciò che riguarda i log memorizzati sui computer infetti, utilizzasse gli stessi nomi di file di cui è solito avvalersi Agent.btz: <mswmpdat.tlb>, <winview.ocx> e <wmcache.nld>. Turla, per di più, fa uso della stessa chiave XOR per codificare i propri file di log.

Tutti gli elementi di confronto descritti sono riassunti nel grafico seguente.



Per il momento, tutto ciò che sappiamo è che i programmi malware condividono tra loro alcuni elementi di evidente somiglianza. E' altrettanto chiaro come Agent.btz abbia di sicuro rappresentato un'indiscutibile fonte di ispirazione per i virus writer che hanno creato e sviluppato gli altri malware sopra citati. Non siamo tuttavia in grado di poter affermare con certezza che dietro le "maschere" delle cyber-minacce in questione si nascondano gli stessi identici "attori".

Storie di sicurezza IT: sbucciando la "cipolla"...

Tor (acronimo di "The Onion Router") è un software appositamente progettato per garantire una perfetta condizione di anonimato nel momento in cui si accede ad Internet. Tale sistema di comunicazione è stato creato già da diverso tempo, ma per molti anni è rimasto quasi esclusivamente ad appannaggio di un ristretto pubblico di esperti ed appassionati. L'utilizzo

della rete Tor è considerevolmente aumentato nel corso di questi ultimi mesi, soprattutto a causa delle crescenti problematiche e preoccupazioni riguardo alla delicata questione della privacy. Tor è in pratica divenuta un'utile soluzione per tutti coloro che, per qualsiasi motivo, temono l'applicazione di procedure di sorveglianza, così come la possibile fuga di informazioni di natura confidenziale e riservata. Appare evidente, sulla base delle indagini da noi recentemente condotte, come Tor risulti particolarmente attraente anche per le folte schiere dei cybercriminali che frequentano i meandri della Rete: come era lecito attendersi, anche tale categoria di malintenzionati sembra apprezzare in maniera particolare l'anonimato offerto dall'innovativo sistema di comunicazione.

Nel 2013, ad esempio, abbiamo iniziato ad osservare come un crescente numero di cybercriminali utilizzasse Tor per ospitare infrastrutture nocive dedicate al malware; al tempo stesso, gli esperti di Kaspersky Lab sono riusciti ad individuare vari programmi maligni che si avvalevano specificamente dell'utilizzo di Tor. Le indagini da noi condotte riguardo alle risorse presenti nell'ambito del network Tor hanno di fatto rivelato l'esistenza di un elevato numero di risorse esplicitamente sfruttate per attività di natura cybercriminale, incluso server C&C di comando e controllo, pannelli di amministrazione ed altro ancora. Ovviamente, collocando i propri server all'interno della rete Tor, i criminali informatici rendono particolarmente complessa l'identificazione e la rimozione degli stessi, così come l'inserimento di tali server malevoli in apposite blacklist.

Come è noto, i forum ed i "mercati" online frequentati dai malfattori dediti al cybercrimine sono ormai divenuti, purtroppo, una spiacevole consuetudine nell'ambito dell'Internet "normale". Di recente, tuttavia, è ugualmente emersa l'esistenza di uno specifico mercato underground basato sul sistema Tor. Tutto è iniziato con il famoso mercato clandestino denominato Silk Road; l'evoluzione del "settore" ha poi prodotto la nascita di decine e decine di ulteriori mercati "neri" online, specializzati, tra l'altro, nel commercio di droga, armi e, naturalmente, malware.

Anche gli e-shop “dedicati” al carding si sono ormai saldamente insediati nell'ambito della Darknet; attraverso di essi vengono posti in vendita i dati personali illecitamente carpiti dai malfattori, peraltro con la disponibilità di una vasta gamma di attributi di ricerca, quali paese, banca, etc. I prodotti offerti, tuttavia, non si limitano esclusivamente alle carte di credito; risultano in effetti ugualmente in vendita dump, skimmer ed attrezzatture di vario genere adibite alle attività di carding.

Una procedura di registrazione alquanto semplice, l'utilizzo di appositi rating relativi ai trader operanti, il servizio di assistenza garantito ed un'interfaccia user-friendly costituiscono le caratteristiche standard del tipico mercato underground ospitato all'interno della rete Tor. Alcuni store, tra l'altro, richiedono preventivamente - a chiunque intenda effettuare vendite su tali piattaforme - il versamento di un deposito cauzionale, sotto forma di una somma fissa di denaro. Tale procedura viene imposta allo scopo di garantire l'autenticità e l'affidabilità del

trader, affinché i servizi da quest'ultimo offerti non si rivelino poi essere di scarsa qualità, o addirittura non si trasformino in vere e proprie truffe.

Lo sviluppo della rete Tor ha coinciso con l'emergere, nell'ambito della finanza digitale, del Bitcoin, in grado di garantire trasferimenti di moneta elettronica protetti dall'anonimato. In pratica, al momento attuale, quasi ogni prodotto o servizio offerto attraverso la rete Tor viene acquistato o venduto mediante l'utilizzo del Bitcoin. Risulta quasi impossibile collegare un portafoglio Bitcoin ad una persona reale, per cui, il fatto stesso di eseguire transazioni sulla Darknet in questione avvalendosi della moneta Bitcoin, significa che, in sostanza, le operazioni compiute da un cybercriminale sono destinate a rimanere virtualmente non tracciabili.

Sembra del tutto probabile che la rete Tor, così come altri network anonimi, possa ben presto divenire una peculiarità comunemente accettata dal pubblico di Internet, visto che un numero sempre crescente di utenti del World Wide Web è attualmente alla ricerca di un modo per salvaguardare le proprie informazioni personali. Si tratta tuttavia, al tempo stesso, di un meccanismo che esercita una particolare attrazione anche nei confronti dei cybercriminali, in quanto tale temibile categoria di malfattori può in tal modo celare al meglio le funzionalità dei programmi malware via via sviluppati, effettuare la compravendita di un'ampia gamma di servizi legati alla sfera della criminalità informatica ed infine - elemento non certo trascurabile - riciclare rapidamente il denaro ricavato attraverso i profitti illeciti realizzati. I nostri esperti ritengono, a ragion veduta, che attualmente stiamo soltanto assistendo alla fase iniziale nell'utilizzo dei network "segreti" da parte dei malintenzionati operanti nella sfera del cybercrimine.

Sicurezza web e fughe di dati

Gli alti e bassi del Bitcoin

Il Bitcoin, come abbiamo visto, è una criptovaluta digitale. Esso opera sulla base di un particolare modello peer-to-peer, in cui la moneta elettronica assume le "sembianze" di una catena di firme digitali che vanno a rappresentare determinate porzioni di un Bitcoin. La valuta digitale Bitcoin non prevede né l'esistenza di un'autorità centrale di controllo, né commissioni o addebiti sulle transazioni internazionali effettuate; questi due fattori, combinati tra loro, hanno indubbiamente contribuito a rendere tale criptomoneta uno strumento di pagamento particolarmente attraente. All'interno del nostro sito web Kaspersky Daily si trovano numerose informazioni riguardo al Bitcoin ed alle specifiche modalità di funzionamento di tale moneta elettronica.

Con il progressivo aumento della popolarità acquisita presso il vasto pubblico degli utenti della Rete ed il conseguente incremento esponenziale del numero di transazioni con esso realizzate, il Bitcoin è rapidamente divenuto un obiettivo sempre più appetibile per i cybercriminali.

Nell'ambito delle previsioni da noi effettuate a fine anno riguardo alla possibile evoluzione del malware nel corso del 2014 avevamo anticipato la comparsa di attacchi informatici nei confronti del Bitcoin; avevamo affermato: "Gli attacchi rivolti ai pool e alle borse Bitcoin, così come agli utenti della celebre criptomoneta, diverranno di sicuro uno dei principali temi dell'anno". Avevamo inoltre detto: "Indubbiamente, saranno in particolar modo praticati, da parte dei cybercriminali, gli assalti informatici eseguiti nei confronti delle borse Bitcoin, visto che, nella conduzione di tali attacchi, il rapporto tra spese sostenute e profitti ricavati assume i valori massimi in termini di convenienza".

Di fatto, nell'anno in corso, tali previsioni si sono già ampiamente avverate, peraltro a seguito di eventi particolarmente eclatanti. Il 25 febbraio scorso, ad esempio, è stata posta offline Mt.Gox, la nota piattaforma di trading utilizzata per condurre la maggior parte delle transazioni finanziarie effettuate tramite il sistema Bitcoin. Tale decisione ha fatto seguito ad un mese particolarmente turbolento, nel corso del quale la borsa in questione è stata tormentata da una serie di gravi problemi – problemi che hanno visto il corso del Bitcoin precipitare in maniera clamorosa, per non dire drammatica, all'interno della suddetta piattaforma. E' corsa voce del fatto che il crash di Mt.Gox, e la conseguente insolvenza della più importante piattaforma di scambio della criptovaluta in questione, sia stato generato da una vasta operazione di hacking, la quale avrebbe prodotto la perdita - o per meglio dire il furto - di ben 744.408 Bitcoin, pari ad un valore di circa 350 milioni di dollari; il sito di Mt.Gox è stato in tal modo messo offline, per bloccare ogni ulteriore possibile prelievo di moneta elettronica. Nella circostanza, pare proprio che il problema principale - alla base di quanto avvenuto - sia rappresentato dalla cosiddetta "transaction malleability", o malleabilità delle transazioni. Si tratta di un problema molto noto all'interno del protocollo Bitcoin; in determinate circostanze, in effetti, tale malleabilità può consentire ad un malintenzionato di avvalersi di molteplici ID nell'ambito di un'unica transazione, in maniera tale che la stessa può apparire come mai realizzata, pur essendo stata, di fatto, eseguita. Potete leggere qui, all'interno del blog Kaspersky Daily, le nostre valutazioni e considerazioni complessive riguardo alle tematiche sollevate dall'improvviso crollo di Mt.Gox. La falla di sicurezza rappresentata dall'eccessiva "malleabilità" delle transazioni all'interno del sistema Bitcoin è stata adesso risolta. Naturalmente, come abbiamo riferito verso la fine dello scorso anno, Mt.Gox non è l'unico fornitore di servizi di virtual banking ad aver subito attacchi informatici. Il crescente utilizzo delle valute virtuali comporterà inevitabilmente, in futuro, un numero di attacchi ancora maggiore.

E' di particolare importanza sottolineare come tali attacchi possano essere potenzialmente portati non soltanto nei confronti delle piattaforme di scambio di moneta virtuale. In effetti, possono essere ugualmente prese di mira, da parte dei cybercriminali, le persone che utilizzano le criptovalute. A metà marzo, ad esempio, sono rimasti vittima di episodi di hacking sia il blog personale che l'account Reddit di Mark Karepeles, amministratore delegato (CEO) di Mt.Gox. Tali account sono stati utilizzati per pubblicare un file, denominato <MtGox2014Leak.zip>. Secondo gli autori dell'attacco, il file compresso in questione avrebbe

dovuto contenere preziosi dump di database, nonché software specializzato in grado di consentire l'accesso da remoto ai dati sensibili di Mt.Gox. In realtà, il vero contenuto del suddetto file .zip altro non era se non un malware appositamente progettato per cercare di localizzare e sottrarre i file relativi ai wallet (portafogli) Bitcoin. I risultati dell'analisi effettuata dagli esperti di Kaspersky Lab riguardo a tale malware possono essere consultati qui. Risulta ben chiaro, valutando la portata di tale incidente, come i cybercriminali cerchino costantemente di manipolare a loro favore il naturale interesse manifestato dagli utenti nei confronti dei temi caldi del momento; si tratta di un'astuta modalità per diffondere su scala globale temibili malware.

Una tematica di primaria importanza, evocata da tale tipologia di attacchi informatici, riguarda il modo attraverso il quale tutti coloro che fanno uso di criptovaluta possano agire in effettiva sicurezza, salvaguardando le proprie risorse finanziarie, in un ambiente virtuale in cui, a differenza di quanto normalmente avviene con le valute utilizzate nel mondo reale, non esistono standard, regole o normative applicate da apposite autorità di controllo. Il nostro consiglio è quello di evitare di far uso di servizi online (come, ad esempio, una borsa Internet priva di adeguati track record) per custodire i vostri "risparmi" in moneta elettronica; si dovrebbe invece ricorrere all'utilizzo di un apposito client Bitcoin di tipo open-source, posto rigorosamente offline. Se poi disponete di un'elevata quantità di Bitcoin, conservate la vostra preziosa criptomoneta in uno speciale portafoglio virtuale custodito all'interno di un PC non collegato in Rete. Oltre a ciò, rendete la passphrase per il vostro portafoglio Bitcoin quanto più complessa possibile e fate in modo tale che il vostro computer risulti protetto da un'efficace soluzione di sicurezza Internet.

Gli spammer, da parte loro, si sono dimostrati ugualmente pronti e particolarmente scaltri nell'utilizzare metodi e tecniche di ingegneria sociale per coinvolgere le persone in pericolose truffe, "ispirate" al tema della criptovaluta. Essi hanno ad esempio sfruttato la crescita del corso del Bitcoin, verificatasi nella prima parte del trimestre oggetto del report (e quindi precedente al rovinoso crash della piattaforma Mt.Gox) per cercare di far leva sul desiderio, di molte persone, di potersi arricchire rapidamente. Come abbiamo evidenziato in un post pubblicato nello scorso mese di febbraio all'interno del nostro blog dedicato alle tematiche di sicurezza IT, gli spammer hanno fatto ricorso all'utilizzo di numerose argomentazioni correlate al mondo del Bitcoin. Segnaliamo, tra di esse, le offerte per condividere i segreti di un sedicente milionario sul modo di divenire ricchi investendo in Bitcoin, nonché le proposte relative alla partecipazione ad una speciale lotteria online, attraverso la quale, secondo quanto asserito dagli spammer, si sarebbe potuta vincere una cospicua somma di denaro in Bitcoin.

Un software legittimo che potrebbe essere utilizzato per scopi malevoli

Nel mese di febbraio, in occasione del Kaspersky Security Analyst Summit 2014, tenutosi nella Repubblica Dominicana, abbiamo a più riprese sottolineato come un'implementazione impropria delle tecnologie anti-furto di cui è provvisto il firmware installato nei computer

laptop comunemente utilizzati, nonché in alcuni computer desktop, potrebbe di fatto divenire una potente arma nelle mani dei cybercriminali.

La nostra ricerca in materia ha avuto inizio nel momento stesso in cui un collaboratore di Kaspersky Lab si è trovato di fronte a ripetuti crash del processo di sistema su uno dei suoi laptop personali. La tempestiva analisi del registro degli eventi ed un provvidenziale dump di memoria hanno rivelato come i crash in questione fossero provocati dall'instabilità riscontrata a livello dei moduli denominati <identprv.dll> e <wceprv.dll>, caricati nello spazio degli indirizzi di uno dei processi host del servizio di sistema (<svchost.exe>). E' poi emerso che i moduli in questione erano stati creati da Absolute Software - corporation di primaria importanza, del tutto legittima, operante nel settore IT - e facevano parte del software denominato Absolute Computrace.

Nella circostanza, il nostro collega ha fatto presente come non avesse mai provveduto ad installare tale software e non fosse nemmeno a conoscenza dell'eventuale presenza di quest'ultimo all'interno del proprio laptop. Ovviamente, questo ha destato serie preoccupazioni, poiché, secondo uno specifico white paper pubblicato da Absolute Software sul proprio sito web, l'installazione del suddetto software dovrebbe essere esclusivamente eseguita dal proprietario del computer o, in alternativa, dal servizio IT allestito dalla società in questione. Oltre a ciò, mentre la maggior parte del software pre-installato può essere rimossa o disabilitata in maniera permanente dal proprietario stesso del computer, l'agente Computrace è stato appositamente progettato per "sopravvivere" sia ad operazioni di pulizia del sistema eseguite a livello professionale, sia, addirittura, ad un'eventuale sostituzione del disco rigido. Per di più, non potevamo semplicemente "liquidare" l'episodio come se si fosse trattato di un'evento "una tantum", visto che, nel frattempo, erano emersi ulteriori indizi, del tutto analoghi, riguardo alla presenza del software Computrace sia all'interno di computer privati appartenenti ad alcuni dei nostri ricercatori, sia in vari computer aziendali. Abbiamo così deciso di effettuare un'approfondita analisi in merito a quanto era così sorprendentemente accaduto.

Quando abbiamo esaminato per la prima volta Computrace abbiamo erroneamente pensato che si trattasse di un software dannoso, in quanto si avvale di numerosi "trucchi" e funzionalità particolarmente diffusi nell'ambito del malware attualmente in circolazione. Computrace utilizza, ad esempio, particolari tecniche di debugging ed anti-reverse engineering, si inserisce nella memoria di altri processi, stabilisce comunicazioni segrete, esegue le patch dei file di sistema presenti sul disco, codifica i file di configurazione e rilascia un file eseguibile Windows direttamente dal BIOS/ firmware. Questo è il motivo per cui, in passato, il software in questione è stato a volte rilevato come malware; attualmente, la maggior parte delle società produttrici di soluzioni antivirus colloca tuttavia in whitelist i file eseguibili Computrace.

Riteniamo, da parte nostra, che l'agente Computrace sia stato effettivamente progettato e sviluppato dalla software house sopra menzionata sulla base di ottime intenzioni. Le indagini da noi condotte dimostrano tuttavia come determinate vulnerabilità individuate nel software

potrebbero di fatto consentire ai cybercriminali di effettuare un uso improprio ed illecito dello stesso. A nostro avviso, in un tool così potente, dovrebbero essere giocoforza incorporate tecnologie particolarmente solide a livello di meccanismi di autenticazione e codifica. Precisiamo, ad ogni caso, che non è stata trovata alcuna prova del fatto che i moduli riconducibili al software Computrace siano stati segretamente attivati sui computer da noi sottoposti ad analisi. E' tuttavia evidente come vi sia un elevato numero di computer sui quali risultano attivati gli agenti Computrace. Riteniamo che sia preciso compito dei produttori e, al contempo, di Absolute Software, provvedere ad avvisare gli utenti interessati, spiegando loro come poter disattivare il software nel caso in cui questi ultimi non desiderino farne uso. In caso contrario, questi agenti rimasti "orfani" continueranno ad essere operativi ad insaputa dell'utente, fornendo indesiderate opportunità di sfruttamento da remoto da parte di malintenzionati.

Le minacce IT per dispositivi mobile

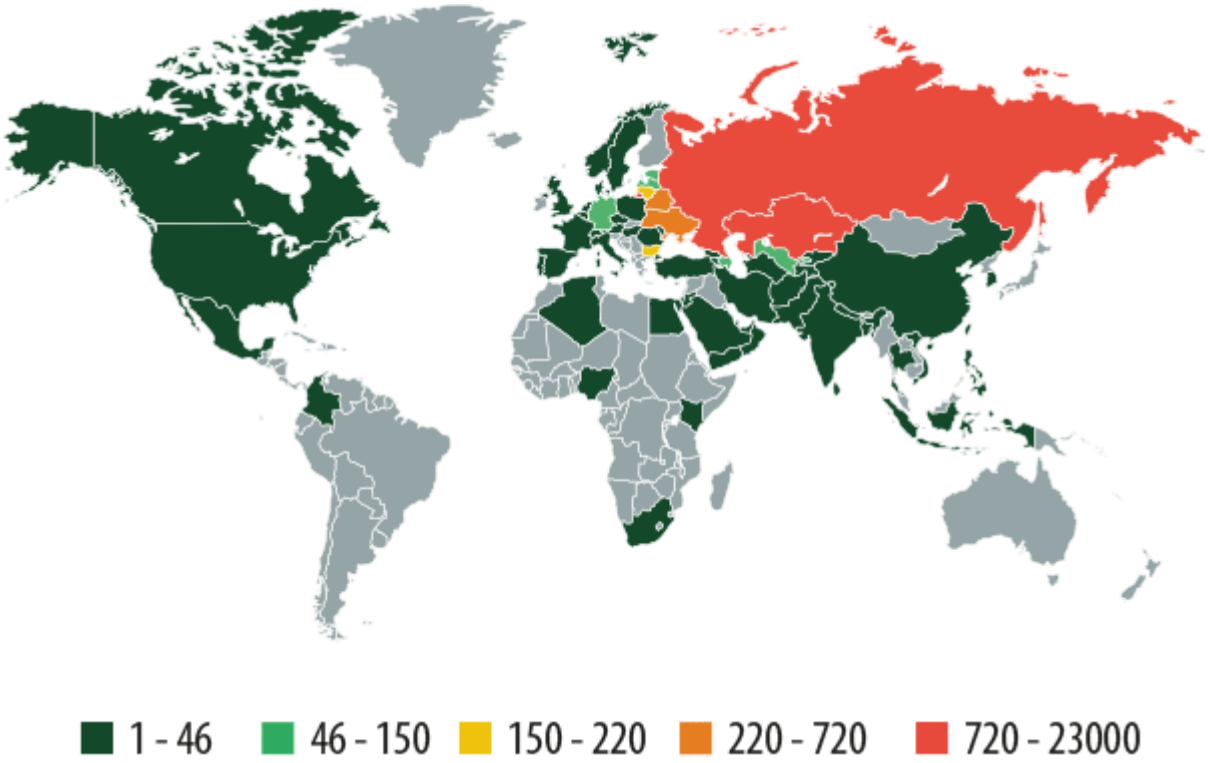
Nel trimestre oggetto del presente report la quota relativa ai software nocivi destinati alla piattaforma Android si è attestata su un valore pari ad oltre il 99% del numero totale di programmi malware per dispositivi mobile complessivamente rilevati. Lungo tutto l'arco del primo trimestre dell'anno sono stati individuati:

- 1.258.436 pacchetti di installazione;
- 110.324 nuove varianti di programmi dannosi specificamente creati dai virus writer per infettare i dispositivi mobile;
- 1.382 nuovi Trojan bancari per piattaforme mobile.

I Trojan bancari mobile

Se all'inizio del primo trimestre del 2014 era nota l'esistenza, in totale, di 1.321 file eseguibili unici relativi a banker mobile, alla fine del periodo qui esaminato il numero complessivo di questi ultimi è addirittura quasi raddoppiato, raggiungendo in tal modo quota 2.503.

Così come in precedenza, tale tipologia di minaccia informatica si è manifestata in particolar modo in Russia, Kazakhstan, Bielorussia ed Ukraina:



Quadro mondiale relativo alla ripartizione geografica dei tentativi di infezione compiuti dai Trojan bancari destinati ai dispositivi mobile - Primo trimestre del 2014

TOP-10 relativa ai paesi maggiormente sottoposti ad attacchi da parte di Trojan-Banker:

Paese	% di attacchi
Russia	88,85%
Kazakhstan	3,00%
Ukraina	2,71%
Bielorussia	1,18%
Lituania	0,62%
Bulgaria	0,60%
Azerbaijan	0,54%
Germania	0,39%
Lettonia	0,34%

Uzbekistan	0,30%

Desideriamo innanzitutto porre in evidenza come uno dei Trojan bancari individuati nel già ampio panorama delle minacce informatiche "dedicate" ai dispositivi mobile, classificato dagli esperti di sicurezza IT con la denominazione di Faketoken, sia entrato a far parte della speciale TOP-20 da noi stilata relativamente ai programmi malware per piattaforme mobile più frequentemente rilevati, nel corso del primo trimestre dell'anno, dalle soluzioni di sicurezza di Kaspersky Lab. Il suddetto software nocivo è stato appositamente creato dai virus writer per compiere il furto dei codici segreti mTAN ((tali codici, trasmessi dalle banche ai propri clienti attraverso appositi messaggi SMS, consentono di confermare l'esecuzione della transazione bancaria in corso); la sua specifica caratteristica è rappresentata dal fatto che esso "opera" in abbinamento con i Trojan bancari preposti a colpire i computer desktop, ovvero le architetture Win-32. Tale combinazione di malware viene di solito utilizzata dai cybercriminali allo scopo di eludere i sistemi di autenticazione a due fattori. I "desktop banker", durante la sessione di banking online condotta dall'utente, utilizzando il metodo della cosiddetta "web injection" (attraverso il quale i malintenzionati sono soliti apportare modifiche non autorizzate a pagine web legittime), introducono segretamente, all'interno della pagina web dell'istituto bancario caricata sul browser, la richiesta di effettuare il download di un'applicazione Android - camuffata sotto forma di utility necessaria per garantire la sicurezza della transazione in corso - e, allo stesso tempo, un link nocivo al banker mobile Faketoken. In seguito, non appena il malware mobile in questione si insedia nello smartphone preso di mira, i malintenzionati, avvalendosi di appositi Trojan bancari "in versione desktop", ottengono l'accesso al conto bancario dell'utente-vittima, mentre il banker mobile Faketoken consente a sua volta, al cybercriminale di turno, di carpire il codice mTAN e di trasferire, quindi, sul proprio account, il denaro illecitamente sottratto all'utente.

Abbiamo più volte riferito, nei nostri precedenti report, di come la maggior parte dei Trojan-banker mobile vengano creati ed inizialmente utilizzati soltanto entro i confini della Federazione Russa; in seguito, tuttavia, i malfattori possono far uso di essi anche in altri paesi del globo. Il banker Faketoken appartiene, indiscutibilmente, a tale novero di programmi nocivi. Nel primo trimestre del 2014 sono stati in effetti registrati attacchi informatici - compiuti attraverso il dispiegamento di tale malware - nei confronti degli utenti di ben 55 paesi, tra cui Germania, Svezia, Francia, Italia, Gran Bretagna e Stati Uniti.

Le novità «presentate» dai virus writer

Un bot controllato tramite la rete TOR

La rete anonima Tor (acronimo di "The Onion Router"), costruita su una rete di proxy server, garantisce una perfetta condizione di anonimato nel momento in cui l'utente accede ad Internet; essa permette inoltre di poter collocare nella zona di dominio < .onion > dei siti web "anonimi", raggiungibili esclusivamente attraverso il sistema Tor. Nello scorso mese di febbraio è stato da noi individuato il primo Trojan per l'OS Android che si avvale, in qualità di C&C (Command and Control Center) di un dominio situato nella pseudo-zona .onion.

Si tratta del malware classificato come Backdoor.AndroidOS.Torec.a, che costituisce, in pratica, una variante del client Tor denominato Orbot, al quale i malintenzionati hanno aggiunto il proprio codice nocivo. Sottolineiamo, nella circostanza, come il malware Backdoor.AndroidOS.Torec.a, per poter utilizzare la rete Tor, necessiti di una quantità di codice sensibilmente maggiore rispetto al codice necessario per espletare le funzionalità originariamente previste per il suddetto client.

Il programma Trojan in questione è in grado di ricevere dal server nocivo C&C i seguenti comandi:

- iniziare/terminare l'intercettazione degli SMS in entrata;
- iniziare/terminare il furto degli SMS in entrata;
- effettuare richieste USSD;
- trasmettere al C&C i dati relativi al telefono (numero telefonico, paese, IMEI, modello, versione del sistema operativo);
- trasmettere al C&C l'elenco delle applicazioni installate nel dispositivo mobile;
- inviare SMS al numero indicato tramite l'apposito comando.

Ma quali sono le ragioni che hanno indotto i malintenzionati ad avvalersi di una rete anonima? La risposta è semplice: il C&C collocato nell'ambito della rete Tor non può essere chiuso, e quindi smantellato. E' di particolare interesse rilevare come, nell'occasione, i creatori di programmi Trojan destinati alla piattaforma Android abbiano ripreso tale specifico approccio direttamente dai virus writer dediti alla scrittura di malware progettati per attaccare il sistema operativo Windows.

Il furto di denaro dai portafogli elettronici

I cybercriminali sono costantemente alla ricerca di nuovi metodi ed espedienti per realizzare il furto di cospicue somme di denaro mediante l'utilizzo di programmi Trojan appositamente progettati per colpire i dispositivi mobile. Nello scorso mese di marzo, gli esperti di Kaspersky Lab hanno individuato un singolare programma nocivo, denominato Trojan-SMS.AndroidOS.Waller.a, il quale, oltre alle attività che tradizionalmente caratterizzano i Trojan-SMS, è in grado di realizzare il furto del denaro custodito nei portafogli elettronici QIWI-Wallet (QIWI è un noto sistema di pagamento elettronico particolarmente diffuso in Russia e nei paesi che attualmente occupano lo spazio geografico post-sovietico) appartenenti ai proprietari degli smartphone infettati da tale malware.

Una volta ricevuto l'adeguato comando dal server C&C, il Trojan in questione verifica il saldo presente sull'account relativo al portafoglio digitale QIWI-Wallet. Per far ciò, esso provvede ad inviare un apposito SMS al numero telefonico corrispondente al wallet elettronico - preso di mira - nell'ambito del sistema QIWI. Il messaggio SMS ricevuto in risposta viene poi intercettato, per essere in seguito inoltrato ai "padroni" del Trojan.

Nel caso in cui il proprietario del dispositivo mobile infetto risulti essere titolare di un QIWI-Wallet, ed il Trojan riceva informazioni riguardo alla presenza di un saldo positivo su tale portafoglio elettronico, il software nocivo in causa realizzerà immediatamente il trasferimento della somma di denaro così individuata dall'account dell'utente-vittima verso l'account QIWI-Wallet specificato nell'occasione dai malintenzionati. Per effettuare tale operazione, su apposito comando impartito dai propri "padroni", il Trojan invia un SMS verso un numero speciale presente nel sistema QIWI; in tale messaggio vengono di fatto indicati il numero del portafoglio elettronico appartenente ai malintenzionati e l'importo relativo al "trasferimento" in atto.

Per il momento, il Trojan attacca esclusivamente gli utenti della Federazione Russa. Tuttavia, i malintenzionati possono ugualmente avvalersi di tale malware mobile per effettuare il furto delle risorse finanziarie degli utenti situati in altri paesi, e più precisamente nelle nazioni in cui si ricorre all'uso dei portafogli elettronici gestibili attraverso i messaggi SMS.

Cattive notizie

Nel corso del primo trimestre del 2014 è stata rilevata l'esistenza di un programma Trojan destinato all'iOS. Si tratta di un software nocivo concepito sotto forma di libreria dinamica, avente funzione di plugin per Cydia Substrate, il popolare framework per dispositivi iOs sottoposti ad operazioni di jailbreaking. Come è noto, nell'ambito di numerosi programmi di partenariato, gli sviluppatori di applicazioni che inseriscono nelle proprie app i cosiddetti moduli AdWare, ricevono un compenso per le pubblicità che vengono in seguito visualizzate dagli utenti. Il suddetto Trojan, individuato da un ricercatore cinese specializzato in sicurezza IT, sostituisce, in alcuni moduli AdWare, gli ID dei creatori del programma pubblicitario con gli ID dei malintenzionati. Il risultato di tutto ciò è che le somme di denaro generate dalla visualizzazione delle réclame vanno in tal modo a finire dritte dritte nelle mani dei cybercriminali.

Un esperto di sicurezza IT turco ha individuato determinate vulnerabilità nel sistema operativo mobile Android, il cui sfruttamento, mediante la conduzione di appositi attacchi DOS (Denial-Of-Service) da parte di malintenzionati può produrre una serie infinita di crash del dispositivo, ed eventualmente la cancellazione di tutti i dati custoditi in quest'ultimo. L'essenza di questa vulnerabilità DOS consiste nella semplice realizzazione, da parte dei cybercriminali, di un'applicazione Android provvista di apposito file <AndroidManifest.xml> contenente all'interno di qualsiasi campo <name> un'elevata quantità di dati (AndroidManifest.xml è un particolare file che si trova in ogni applicazione sviluppata per i dispositivi mobile dotati di OS Android. In tale file vengono custodite le informazioni relative all'applicazione, incluso quelle riguardanti i permessi di accesso alle funzioni di sistema, i puntatori relativi ai gestori dei

vari eventi, etc.). L'installazione di una simile applicazione nel dispositivo sottoposto ad attacco avviene senza problemi di sorta; tuttavia, richiamando il label <activity> con tale nome, si produrrà inevitabilmente il crash del sistema. Può essere ad esempio creato un gestore degli SMS in entrata provvisto di nome non corretto, in maniera tale che, una volta ricevuto un SMS qualsiasi, risulterà di fatto impossibile utilizzare il telefono. In effetti, il dispositivo mobile inizierà a riavviarsi in continuazione, per cui, all'utente, resterà soltanto la possibilità di ripristinare il firmware. Ciò, ovviamente, causerà la perdita di tutti i dati precedentemente memorizzati dall'utente sul proprio dispositivo.

Lo spam nocivo

Uno dei metodi standard utilizzati dai cybercriminali per distribuire i temibili malware mobile è indubbiamente rappresentato dallo spam di natura maligna. Tale metodo risulta particolarmente popolare presso quei malintenzionati che si avvalgono dei famigerati Trojan mobile per realizzare il furto di significative somme di denaro dagli account bancari degli utenti.

Il tipico messaggio SMS nocivo può contenere, in genere, sia l'esplicita proposta di scaricare una determinata applicazione (con tanto di apposito link per effettuare il relativo download), sia un collegamento al sito web preposto alla diffusione del programma malware che i malintenzionati intendono recapitare sul dispositivo mobile dell'utente-vittima, cercando di attirare quest'ultimo, con un pretesto o con l'altro, su tale sito dannoso. Così come avviene per lo spam nocivo diffuso attraverso la posta elettronica, anche in tal caso i malfattori fanno largo uso di varie tecniche di ingegneria sociale allo scopo di attirare al massimo l'attenzione degli utenti presi di mira.

Lo spam "olimpico"

I Giochi Olimpici rappresentano indiscutibilmente un evento di grande importanza, per non dire di portata planetaria. Naturalmente, ogni volta, i malintenzionati della Rete cercano di sfruttare al massimo il naturale interesse abitualmente dimostrato dagli utenti di ogni angolo del globo nei confronti di avvenimenti del genere.

Così, nello scorso mese di febbraio, è stata da noi individuata la conduzione di una campagna di spam realizzata mediante l'invio di messaggi SMS nocivi contenenti dei link che, a detta del mittente, avrebbero dovuto permettere agli utenti di visualizzare sul proprio smartphone la trasmissione delle competizioni previste nel quadro della XXII° edizione dei Giochi Olimpici Invernali, svoltisi a Sochi (Federazione Russa) dal 7 al 23 febbraio 2014. Qualora i proprietari dei dispositivi mobile presi di mira avessero incautamente cliccato sul link in questione, si sarebbe inevitabilmente avviato il tentativo di scaricare sugli smartphone interessati dall'attacco un pericoloso programma Trojan, rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come HEUR:Trojan-SMS.AndroidOS.FakeInst.fb.

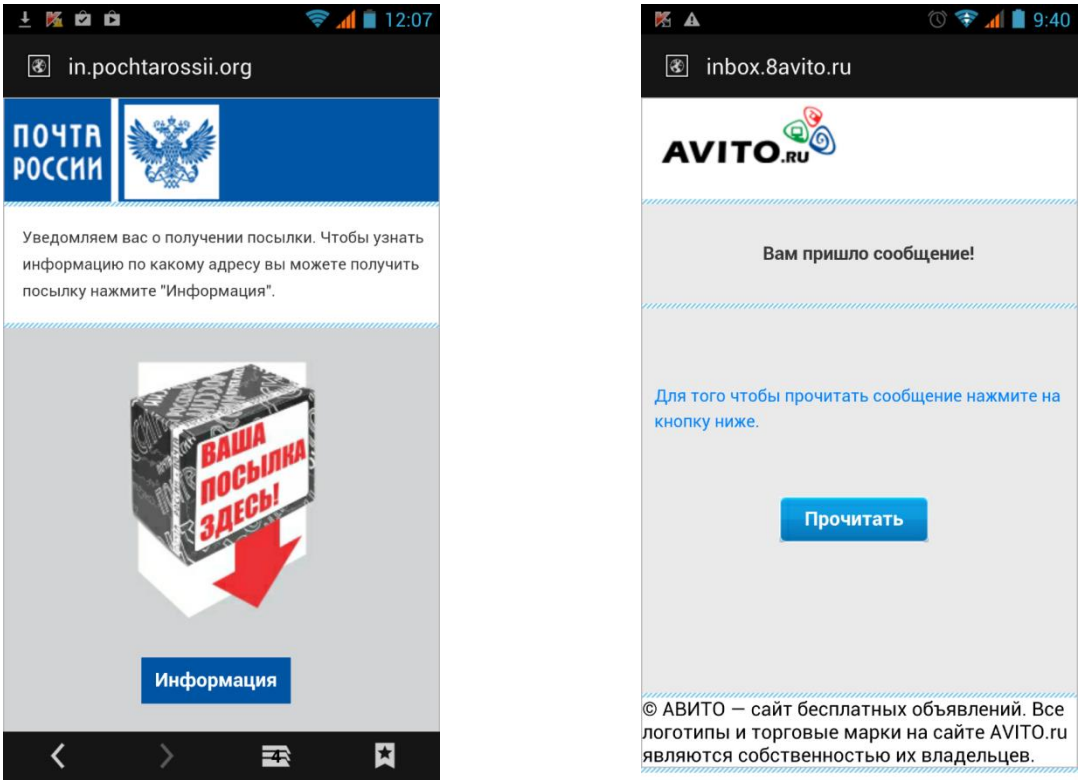
Si tratta, nella fattispecie, di un Trojan che, tramite un apposito comando trasmesso dai malintenzionati, è in grado di inviare un messaggio SMS verso il numero di telefono di uno dei maggiori istituti bancari russi, per poi procedere al trasferimento di un determinato importo di denaro dal conto bancario all'account di telefonia mobile del proprietario dello smartphone infetto. In seguito, i malfattori completano l'operazione malevola trasferendo l'importo in questione dall'account telefonico dell'utente-vittima al proprio portafoglio elettronico. Nella circostanza, tutti i messaggi provenienti dalla banca riguardo al trasferimento di denaro eseguito, vengono subdolamente occultati all'utente.

Spam con link a siti dannosi

Nel corso del trimestre esaminato nel presente report, i cybercriminali dediti alla diffusione del Trojan denominato Opfake hanno distribuito, verso i dispositivi mobile dei potenziali utenti-vittima, un cospicuo numero di messaggi SMS di spam contenenti link a siti web nocivi appositamente allestiti dai malintenzionati.

Attraverso uno di tali messaggi di spam, inoltrati tramite SMS, si comunicava all'utente che quest'ultimo aveva ricevuto un determinato pacco postale; nella circostanza, il link inserito dai malfattori avrebbe condotto il destinatario dell'SMS verso un sito web fasullo, mascherato sotto forma di sito web ufficiale delle Poste Russe.

In altre campagne di spam i malintenzionati hanno invece sfruttato l'elevato livello di popolarità raggiunto dal sito russo di annunci gratuiti denominato Avito.ru. Gli SMS nocivi in questione contenevano il seguente testo: «Hai ricevuto una risposta al tuo annuncio», oppure «Un utente è interessato all'acquisto del tuo prodotto»; ovviamente, nell'occasione, i malintenzionati avevano ugualmente inserito nei loro messaggi appositi link, preposti a condurre gli utenti-vittima verso una pagina web contraffatta, a prima vista appartenente al sito Avito.ru.



Esempi di pagine web contraffatte, dal contenuto nocivo

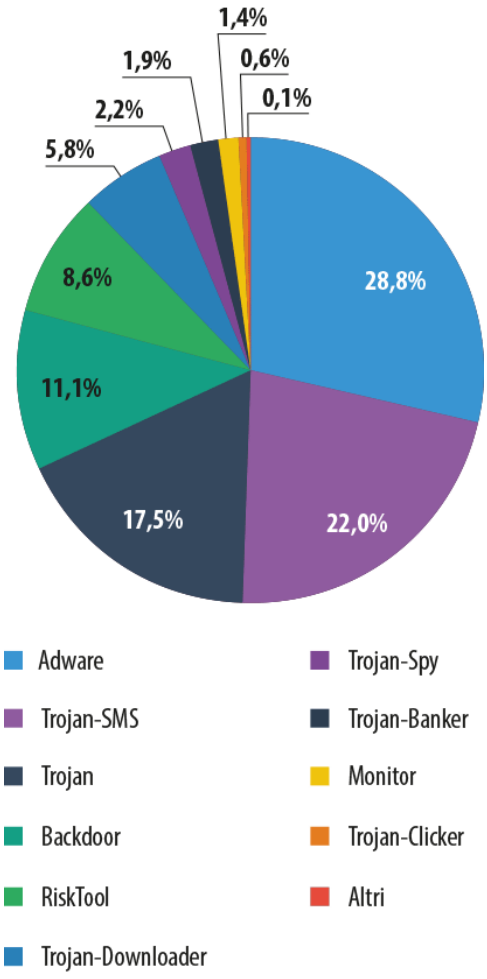
Se gli utenti presi di mira avessero provveduto a cliccare sui link destinati a condurli verso i siti web fasulli predisposti dai cybercriminali, sarebbe stato avviato il tentativo di caricare sugli smartphone coinvolti in tale campagna di spam nocivo il programma Trojan classificato come Trojan-

SMS.AndroidOS.Opfake.a. Oltre che per realizzare l'invio di messaggi SMS verso costosi numeri a pagamento, tale software nocivo viene altresì utilizzato per diffondere ulteriori malware mobile, ed in particolar modo il famigerato malware multifunzionale battezzato dagli esperti di sicurezza IT con il nome di Backdoor.AndroidOS.Obad.a.

L'ingegneria sociale, nelle mani dei malintenzionati della Rete, si è sempre rivelata essere un pericoloso strumento di attacco. Gli utenti debbono pertanto dimostrarsi in ogni frangente particolarmente cauti ed accorti; in primo luogo, come precauzione minima, non bisogna in alcun modo cliccare sui link inseriti in messaggi SMS ricevuti da mittenti sconosciuti. In tali casi, difatti, vi è sempre il rischio di cadere nelle trappole (più o meno) abilmente tese dai malfattori e - come spiacevole conseguenza - perdere importanti somme di denaro.

Le statistiche

Ripartizione del malware mobile per tipologie



Suddivisione delle varianti di malware mobile in base ai loro specifici comportamenti dannosi - Primo trimestre del 2014

Come evidenzia il grafico qui sopra riportato, nel primo trimestre dell'anno in corso la prima posizione della speciale graduatoria da noi stilata è andata ad appannaggio degli AdWare (moduli pubblicitari), la cui unica funzionalità è rappresentata dal mostrare insistentemente all'utente del dispositivo mobile pubblicità moleste. Osserviamo, nella circostanza, come tale genere di moduli goda di particolare popolarità soprattutto in Cina.

I Trojan-SMS, da parte loro, rimasti a lungo nella posizione di leader della graduatoria in questione, sono scesi sul secondo gradino del "podio" virtuale; nell'arco di un trimestre, la quota percentuale ad essi attribuibile è sensibilmente diminuita, passando dal 34% al 22%. Così come in precedenza, tuttavia, tale specifica categoria di software nocivi predomina nettamente all'interno della TOP-20 relativa ai malware mobile rilevati con maggiore frequenza.

TOP-20 relativa ai programmi malware destinati alle piattaforme mobile

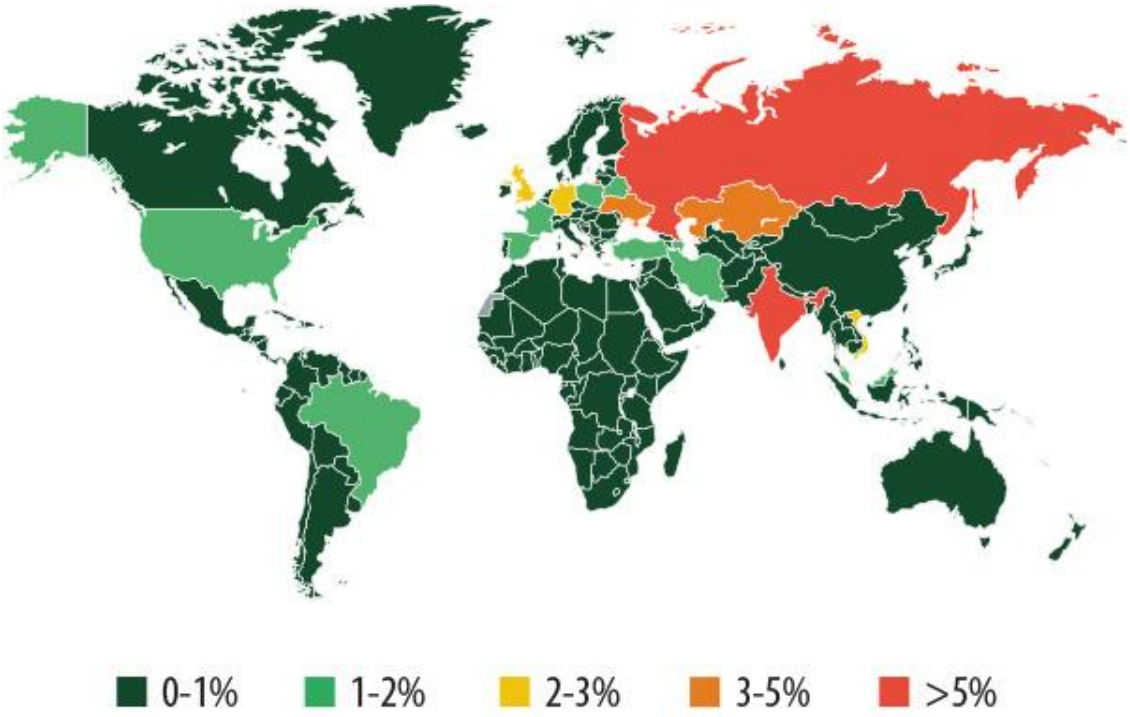
	Denominazione	% di attacchi
1	Trojan-SMS.AndroidOS.Stealer.a	22,77%
2	RiskTool.AndroidOS.MimobSMS.a	11,54%
3	Trojan-SMS.AndroidOS.OpFake.bo	11,30%
4	RiskTool.AndroidOS.Mobogen.a	10,50%
5	DangerousObject.Multi.Generic	9,83%
6	Trojan-SMS.AndroidOS.FakeInst.a	9,78%
7	Trojan-SMS.AndroidOS.OpFake.a	7,51%
8	Trojan-SMS.AndroidOS.Erop.a	7,09%
9	Trojan-SMS.AndroidOS.Agent.u	6,45%
10	Trojan-SMS.AndroidOS.FakeInst.ei	5,69%
11	Backdoor.AndroidOS.Fobus.a	5,30%
12	Trojan-SMS.AndroidOS.FakeInst.ff	4,58%
13	Trojan-Banker.AndroidOS.Faketoken.a	4,48%
14	AdWare.AndroidOS.Ganlet.a	3,53%
15	Trojan-SMS.AndroidOS.Agent.ao	2,75%
16	AdWare.AndroidOS.Viser.a	2,31%
17	Trojan-SMS.AndroidOS.Agent.dr	2,30%
18	Trojan-SMS.AndroidOS.Agent.fk	2,25%
19	RiskTool.AndroidOS.SMSreg.dd	2,12%
20	RiskTool.AndroidOS.SMSreg.eh	1,87%

Nel corso del primo trimestre dell’anno 2014, un "contributo" particolarmente significativo, a livello di aumento del numero di nuove varianti di malware mobile attualmente in circolazione, è stato fornito dalle nuove modifiche del programma Trojan denominato Trojan-SMS.AndroidOS.Stealer.a. Tale malware non si distingue in alcun modo per qualcosa di particolare; esso è difatti provvisto delle funzionalità standard che caratterizzano tutti i Trojan-SMS. Nonostante ciò, il Trojan in causa è andato ad occupare la prima posizione del rating relativo alle minacce IT per dispositivi mobile più frequentemente rilevate, peraltro con un consistente margine percentuale rispetto ai diretti "concorrenti".

Allo stesso tempo, due tra i leader della graduatoria complessiva dello scorso anno, ovvero Opfake.bo e Fakeinst.a, non sembrano ad ogni caso voler cedere in maniera troppo rapida ed evidente le loro posizioni; tali malware stanno in effetti continuando ad attaccare gli utenti dei dispositivi mobile in maniera particolarmente attiva. Questa situazione genera ovviamente, sulla scena del malware mobile, un flusso infinito di nuovi pacchetti di installazione maligni.

E' di particolare interesse ed importanza osservare come sia entrato per la prima volta a far parte della speciale TOP-20 - relativa ai software nocivi per piattaforme mobile rilevati più di frequente dalle soluzioni di sicurezza IT di Kaspersky Lab - un malware riconducibile alla categoria dei Trojan bancari, ovvero Faketoken (13° posto della graduatoria).

Geografia delle minacce mobile



Geografia delle minacce IT per dispositivi mobile - Situazione relativa al primo trimestre del 2014

TOP-10 relativa ai paesi maggiormente sottoposti ad attacchi da parte di malware mobile

	Paese	% di attacchi
1	Russia	48,90%
2	India	5,23%

3	Kazakhstan	4,55%
4	Ukraina	3,27%
5	Gran Bretagna	2,79%
6	Germania	2,70%
7	Vietnam	2,44%
8	Malaysia	1,79%
9	Spagna	1,58%
10	Polonia	1,54%

Le statistiche

Tutti i dati statistici riportati nel presente resoconto trimestrale sono stati ottenuti attraverso le speciali soluzioni anti-virus implementate nel Kaspersky Security Network (KSN), grazie all'attività svolta da vari componenti ed elementi di sicurezza IT, impiegati per assicurare un'efficace e pronta protezione nei confronti dei programmi malware. Essi sono stati ricevuti tramite gli utenti di KSN che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti. A questo sofisticato sistema di scambio di informazioni su scala globale, riguardo alle pericolose attività condotte dal malware, prendono parte vari milioni di utenti dei prodotti Kaspersky Lab, ubicati in 213 diversi paesi e territori del globo.

Programmi malware in Internet (attacchi via Web)

I dati statistici esaminati in questo capitolo del nostro consueto report trimestrale sull'evoluzione del malware sono stati ottenuti sulla base delle attività svolte dall'anti-virus web, preposto alla protezione dei computer degli utenti nel momento in cui dovesse essere effettuato il download di oggetti nocivi da pagine web malevole/infette. I siti Internet dannosi vengono appositamente allestiti dai cybercriminali; possono tuttavia risultare infetti sia le risorse web il cui contenuto viene determinato dagli stessi utenti della Rete (ad esempio i forum), sia i siti legittimi violati.

TOP-20 relativa agli oggetti infetti rilevati in Internet

Come abbiamo visto, nel corso del primo trimestre del 2014 il nostro anti-virus web ha effettuato il rilevamento di **29.122.849** oggetti dannosi unici (script, pagine web, exploit, file eseguibili, etc.).

Fra tutti i programmi malware resisi protagonisti degli attacchi via web nei confronti dei computer degli utenti, abbiamo rilevato i 20 maggiormente attivi. I programmi che compaiono nella TOP-20 qui sotto riportata hanno da soli generato il 99,8% del volume complessivo di assalti informatici condotti dai cybercriminali attraverso i browser web.

	Denominazione*	% sul totale complessivo degli attacchi**
1	Malicious URL	81,73%
2	Trojan.Script.Generic	8,54%
3	AdWare.Win32.BetterSurf.b	2,29%
4	Trojan-Downloader.Script.Generic	1,29%
5	Trojan.Script.Iframer	1,21%
6	AdWare.Win32.MegaSearch.am	0,88%
7	Trojan.Win32.AntiFW.b	0,79%
8	AdWare.Win32.Agent.ahbx	0,52%
9	AdWare.Win32.Agent.aiyc	0,48%
10	Trojan.Win32.Generic	0,34%
11	AdWare.Win32.Yotoon.heur	0,28%
12	Trojan.Win32.Agent.aduro	0,23%
13	Adware.Win32.Amonetize.heur	0,21%
14	Trojan-Downloader.Win32.Generic	0,21%
15	Trojan-Clicker.JS.FbLiker.k	0,18%
16	Trojan.JS.Iframe.ahk	0,13%
17	AdWare.Win32.Agent.aiwa	0,13%
18	Exploit.Script.Blocker	0,12%
19	AdWare.MSIL.DomaIQ.pef	0,12%
20	Exploit.Script.Generic	0,10%

**Oggetti infetti neutralizzati sulla base dei rilevamenti effettuati dal componente anti-virus web. Le informazioni sono state ricevute tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti.*
***Quota percentuale sul totale complessivo degli attacchi web rilevati sui computer di utenti unici.*

Tradizionalmente, la TOP-20 analizzata nel presente capitolo del report annovera, per la maggior parte, la presenza di "verdetti" riconducibili ad oggetti maligni utilizzati dai cybercriminali per la conduzione di attacchi di tipo drive-by e, al tempo stesso, la presenza di un elevato numero di programmi AdWare. I software “pubblicitari” occupano, difatti, quasi la metà delle posizioni all'interno della speciale classifica da noi stilata; peraltro, la loro quantità complessiva è significativamente aumentata rispetto al trimestre precedente, passando da 7 a ben 9 unità.

Tra gli oggetti nocivi che fanno parte della graduatoria spicca la presenza del temibile software dannoso classificato dagli esperti di sicurezza IT con la denominazione di Trojan.Win32.Agent.aduro (12° posto). Si tratta di un programma malware abitualmente diffuso tramite determinati siti web, attraverso i quali si propone all'utente-navigatore di effettuare il download di uno speciale plugin per il proprio browser, in grado - a detta di coloro che lo offrono - di agevolare gli acquisti online e consentire quindi sostanziosi risparmi.

Tuttavia, una volta cliccato sull'appariscente pulsante “Download”, viene avviato il tentativo di scaricare sul computer dell'utente proprio il malware Trojan.Win32.Agent.aduro. Il compito che si prefigge tale Trojan è sì quello di realizzare il download del plugin pubblicitario proposto, ma assieme a quest'ultimo, a totale insaputa dell'utente, viene ugualmente caricato, sul computer-vittima, un programma appositamente progettato per eseguire le operazioni di mining volte a generare la nota criptovaluta Litecoin. In tal modo, i malintenzionati utilizzeranno in seguito il computer sottoposto ad attacco per le attività di generazione della suddetta criptovaluta, poi custodita sul portafoglio elettronico predisposto dai cybercriminali.

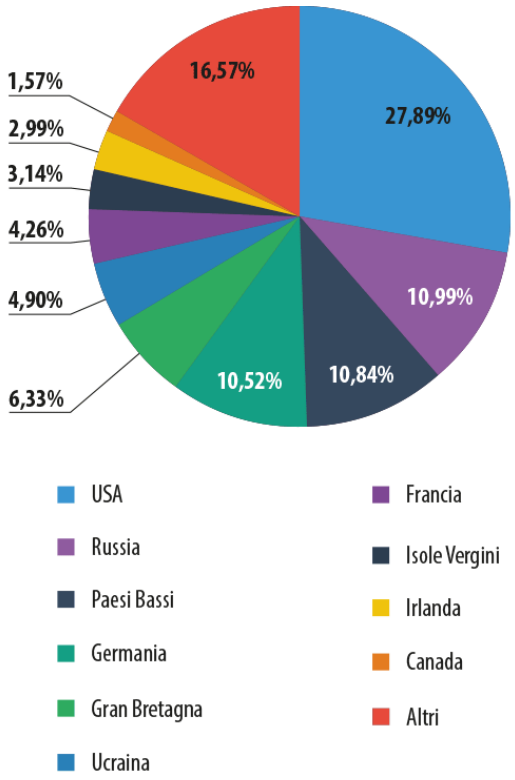
Risulta ugualmente di particolare interesse lo script nocivo classificato come Trojan-Clicker.JS.FbLiker.k (15° posto della graduatoria), che si incontra principalmente su alcuni siti vietnamiti specializzati nell'offrire contenuti e risorse di intrattenimento, ed all'interno dei quali viene proposto, al visitatore, il download di film e programmi. Quando l'utente giunge su uno di tali siti, lo script simula la pressione, da parte del navigatore, del tasto "Mi piace" su una determinata pagina di Facebook, il più esteso social network del pianeta. La pagina di Facebook in questione comparirà, in tal modo, sia all'interno dell'elenco degli amici dell'utente, sia nel profilo di quest'ultimo. Come è noto, la quantità di "Mi piace" ricevuti da una certa pagina nell'ambito del celebre social network, influisce poi sui risultati delle ricerche effettuate dagli utenti su Facebook.

Geografia delle fonti degli attacchi web: TOP-10

Tali dati statistici si riferiscono alla ripartizione per paesi delle fonti degli attacchi web portati nei confronti dei computer degli utenti della Rete, attacchi bloccati e neutralizzati con successo dal modulo Anti-Virus Web (si tratta, più precisamente, di pagine web preposte al redirect degli utenti verso famigerati exploit, di siti Internet imbottiti di exploit ed ulteriori programmi malware, di centri di comando e controllo di estese botnet, etc.). Sottolineiamo, nella circostanza, come ogni host unico preso in considerazione sia stato, di fatto, fonte di uno o più attacchi condotti attraverso Internet.

Per determinare l'origine geografica degli assalti informatici portati tramite web è stato applicato il metodo che prevede la debita comparazione del nome di dominio con il reale indirizzo IP nel quale tale dominio risulta effettivamente collocato; si è allo stesso modo fatto ricorso all'accertamento della collocazione geografica di tale indirizzo IP (GEOIP).

Nel primo trimestre del 2014 le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 353.216.351 attacchi condotti attraverso siti Internet compromessi dislocati in vari paesi. L' 83,4% del numero complessivo di notifiche ricevute riguardo agli attacchi web bloccati e neutralizzati dall'antivirus è risultato attribuibile ad attacchi provenienti da siti web ubicati in una ristretta cerchia di dieci paesi. Tale significativo indice ha fatto registrare una lieve diminuzione, pari a 0,3 punti percentuali, rispetto all'analoga quota rilevata nel trimestre precedente.



Ripartizione per paesi delle fonti degli attacchi web - Situazione relativa al primo trimestre del 2014

Nel corso degli ultimi tre mesi, le posizioni occupate dai vari paesi nel rating sopra riportato non hanno presentato significative variazioni. E' interessante rilevare come il 39% degli attacchi web bloccati e neutralizzati grazie all'intervento dei nostri prodotti anti-malware sia stato condotto attraverso siti web nocivi dislocati sul territorio di Stati Uniti e Russia.

Paesi i cui utenti sono risultati sottoposti ai maggiori rischi di infezioni informatiche diffuse attraverso Internet

Al fine di valutare nel modo più definito possibile il livello di rischio esistente riguardo alle infezioni informatiche distribuite via web - rischio al quale risultano sottoposti i computer degli utenti nei vari paesi del globo - abbiamo stimato il numero di utenti unici dei prodotti Kaspersky Lab che, in ogni paese, nel trimestre qui analizzato, hanno visto entrare in azione il modulo anti-virus specificamente dedicato al rilevamento delle minacce IT presenti nel World Wide Web. Evidenziamo come l'indice percentuale in questione non dipenda, ad ogni caso, dal numero di utenti del Kaspersky Security Network presenti in un determinato paese. Si tratta, in altre parole, di un indice decisamente attendibile riguardo al livello di «aggressività» degli ambienti geografici in cui si trovano ad operare i computer degli utenti.

	Paese*	**% di utenti unici****
1	Vietnam	51,44%
2	Federazione Russa	49,38%
3	Kazakhstan	47,56%
4	Armenia	45,21%
5	Mongolia	44,74%
6	Ukraina	43,63%
7	Azerbaijan	42,64%
8	Bielorussia	39,40%
9	Moldavia	38,04%
10	Kirghizistan	35,87%
11	Tagikistan	33,20%
12	Georgia	32,38%
13	Croazia	31,85%
14	Qatar	31,65%
15	Algeria	31,44%
16	Turchia	31,31%
17	Lituania	30,80%
18	Grecia	30,65%
19	Uzbekistan	30,53%
20	Spagna	30,47%

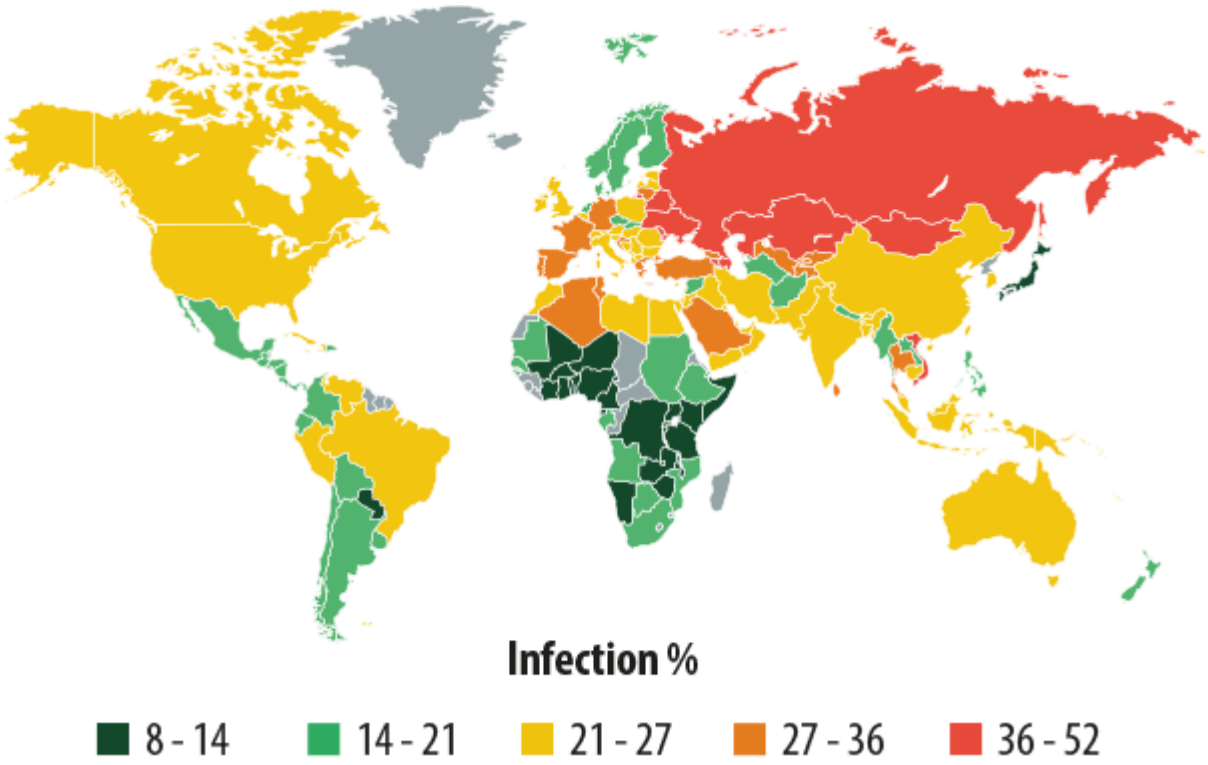
I dati statistici sopra indicati sono stati elaborati sulla base dei rilevamenti effettuati dal modulo Anti-Virus Web; essi sono stati ricevuti tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti.

**Nell'effettuare i calcoli statistici non abbiamo tenuto conto di quei paesi in cui il numero di utenti delle soluzioni anti-virus di Kaspersky Lab risulta ancora relativamente contenuto (meno di 10.000 utenti).*

***Quote percentuali relative al numero di utenti unici sottoposti ad attacchi web rispetto al numero complessivo di utenti unici dei prodotti Kaspersky Lab nel paese.*

Desideriamo innanzitutto porre in evidenza come la speciale TOP-20 del primo trimestre del 2014, relativa ai paesi i cui utenti sono risultati sottoposti con maggior frequenza agli attacchi via Internet, presenti una nuova "leadership": la classifica qui sopra riportata risulta difatti capeggiata dal Vietnam; nel popoloso paese del Sud-Est asiatico è rimasto vittima di tentativi di attacchi via web il 51,4% di utenti unici. Segnaliamo, inoltre, come sia entrata a far parte del rating qui analizzato la Mongolia; il paese asiatico si è subito collocato al 5° posto della graduatoria elaborata dai nostri esperti, facendo registrare un indice pari al 44,7% di utenti unici sottoposti ad attacchi informatici condotti via browser. Le rimanenti posizioni della TOP-10 risultano occupate, come di consueto, dalla Federazione Russa e da vari altri paesi della ex-CSI (Comunità degli Stati Indipendenti), ovvero una parte di quelle nazioni che occupano attualmente lo spazio geografico post-sovietico.

Tra i paesi nei quali la navigazione in Internet è in assoluto più sicura troviamo Singapore (10,5%), Giappone (13,2%), Svezia (14,5%), Sudafrica (15,6%), Taiwan (16,1%), Danimarca (16,4%), Finlandia (16,8%), Paesi Bassi (17,7%) e Norvegia (19,4%).



Complessivamente, a livello mondiale, una consistente porzione degli utenti della Rete (33,2%), anche per una sola volta, è risultata sottoposta ad attacchi informatici provenienti dal web.

Minacce informatiche locali

Si rivelano ugualmente di estrema importanza le statistiche relative alle infezioni locali che si sono manifestate sui computer degli utenti nel corso del primo trimestre del 2014. Tali dati riguardano quindi proprio quelle infezioni che non sono penetrate nei computer attraverso il Web, la posta elettronica o le porte di rete.

Il presente capitolo del nostro consueto report trimestrale dedicato al quadro statistico complessivo delle minacce informatiche, analizza i dati ottenuti grazie alle attività di sicurezza IT svolte dal modulo antivirus (preposto ad effettuare la scansione dei file presenti sul disco rigido al momento della loro creazione o quando si vuole accedere ad essi), unitamente alle statistiche relative ai processi di scansione condotti sui vari supporti rimovibili.

Nell'arco del primo trimestre dell'anno in corso le nostre soluzioni antivirus hanno bloccato 645.809.230 tentativi di infezione locale sui computer degli utenti facenti parte della rete globale di sicurezza Kaspersky Security Network. Complessivamente, nel corso di tali incidenti, sono stati registrati ben 135.227.372 oggetti maligni unici, o potenzialmente indesiderabili.

Oggetti maligni rilevati nei computer degli utenti: TOP-20

	Denominazione	% di utenti unici sottoposti ad attacco*
1	DangerousObject.Multi.Generic	20,37%
2	Trojan.Win32.Generic	18,35%
3	AdWare.Win32.Agent.ahbx	12,29%
4	Trojan.Win32.AutoRun.gen	7,38%
5	AdWare.Win32.BetterSurf.b	6,67%
6	Adware.Win32.Amonetize.heur	5,87%
7	Virus.Win32.Sality.gen	5,78%
8	Worm.VBS.Dinihou.r	5,36%
9	AdWare.Win32.Yotoon.heur	5,02%

10	Trojan-Dropper.Win32.Agent.jkcd	4,94%
11	Worm.Win32.Debris.a	3,40%
12	Trojan.Win32.Starter.lgb	3,32%
13	Exploit.Java.Generic	3,00%
14	AdWare.Win32.Skyli.a	2,80%
15	Trojan.Win32.AntiFW.b	2,38%
16	Virus.Win32.Nimnul.a	2,23%
17	Trojan.WinLNK.Runner.ea	2,22%
18	Adware.Win32.DelBar.a	2,21%
19	AdWare.Win32.BrainInst.heur	2,11%
20	Worm.Script.Generic	2,06%

I dati statistici sopra indicati sono stati elaborati sulla base dei rilevamenti effettuati dai moduli anti-virus OAS (scanner on-access) e ODS (scanner on-demand). Le informazioni sono state ricevute tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti.

**Quote percentuali relative agli utenti unici sui computer dei quali l'anti-virus ha rilevato l'oggetto maligno. Le quote indicate si riferiscono al totale complessivo degli utenti unici dei prodotti Kaspersky Lab, presso i quali sono stati eseguiti rilevamenti da parte dell'anti-virus.*

Il rating qui sopra riportato è relativo ai "verdetti" riconducibili ai programmi AdWare ed ai worm che si diffondono attraverso i supporti di memoria rimovibili, così come, ovviamente, ai virus.

All'interno della speciale TOP-20 da noi stilata, la quota relativa ai virus si mantiene sostanzialmente stabile, pur manifestando una leggera tendenza a diminuire. Come evidenzia la tabella sopra inserita, nel primo trimestre del 2014 la categoria dei virus è rappresentata dai malware classificati dagli esperti di sicurezza IT con la denominazione di Virus.Win32.Sality.gen e Virus.Win32.Nimnul.a; l'indice complessivo ad essi attribuibile si è attestato su un valore pari all' 8%. Per fare un debito confronto, ricordiamo che, nel quarto trimestre dello scorso anno, il valore di tale indice ammontava in totale a 9,1 punti percentuali.

L'oggetto maligno rilevato come Worm.VBS.Dinihou.r (si tratta, in sostanza, di uno script VBS) ha fatto la sua comparsa sulla scena del malware verso la fine dello scorso anno; esso è tuttavia entrato a far parte

del rating in questione soltanto nel primo trimestre del 2014, collocandosi all' 8° posto della graduatoria. Tale worm viene diffuso in particolar modo attraverso lo spam. Provvisto di ampie funzionalità dannose, alla stregua di un programma backdoor vero e proprio, il suddetto worm è in grado, ad esempio, di avviare la riga di comando, così come di realizzare l'upload sul server di un determinato file. Oltre a ciò, esso provvede ad infettare tutti i supporti USB che vengono via via collegati al computer compromesso.

Paesi nei quali i computer degli utenti sono risultati sottoposti al rischio più elevato di infezioni informatiche locali

	Paese*	% di utenti unici**
1	Vietnam	60,30%
2	Mongolia	56,65%
3	Nepal	54,42%
4	Algeria	54,38%
5	Yemen	53,76%
6	Bangladesh	53,63%
7	Egitto	51,30%
8	Iraq	50,95%
9	Afghanistan	50,86%
10	Pakistan	49,79%
11	India	49,02%
12	Sudan	48,76%
13	Tunisia	48,47%
14	Djibouti	48,27%
15	Laos	47,40%
16	Siria	46,94%
17	Birmania	46,92%
18	Cambogia	46,91%
19	Marocco	46,01%
20	Indonesia	45,61%

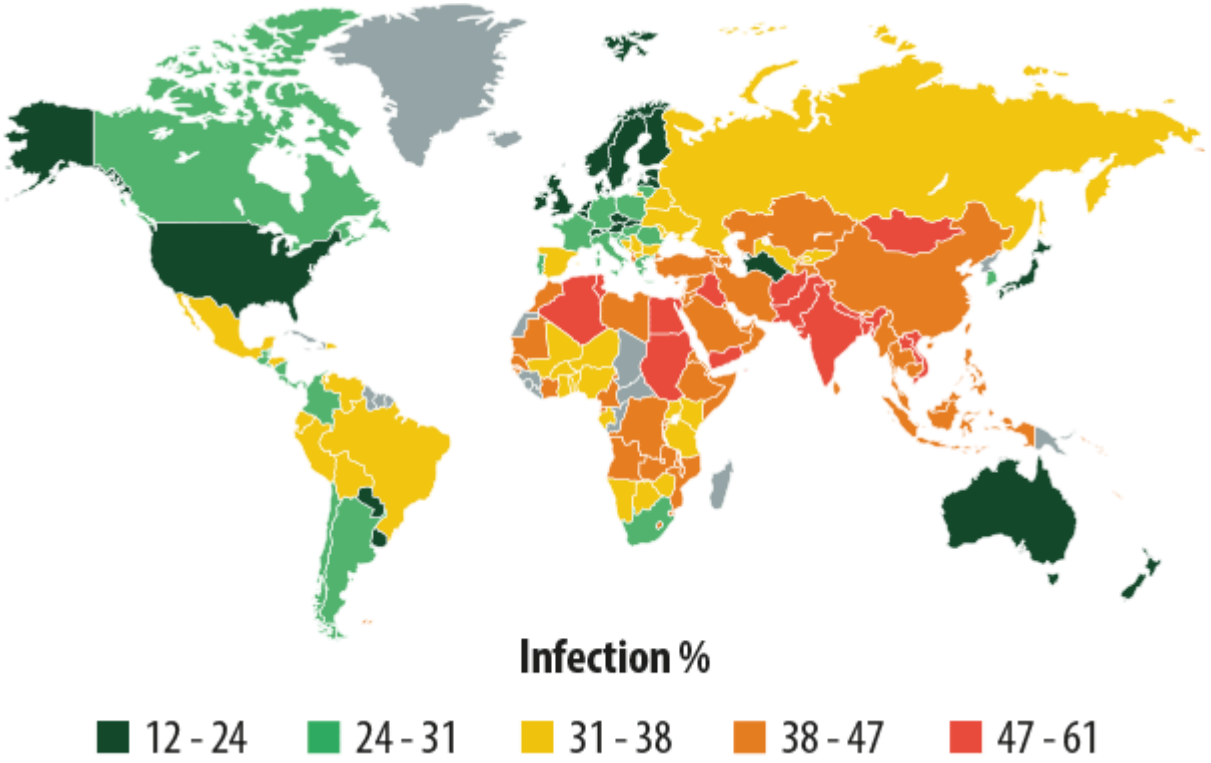
I dati statistici sopra indicati sono stati elaborati sulla base dei rilevamenti effettuati dal modulo anti-virus; essi sono stati ricevuti tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti. Nella circostanza, sono stati presi in considerazione i programmi malware individuati dalle nostre soluzioni anti-virus direttamente sui computer degli utenti, oppure sulle unità rimovibili ad essi collegate (flash drive USB, schede di memoria di telefoni o apparecchi fotografici digitali, hard disk esterni).

**Nell'effettuare i calcoli statistici non abbiamo tenuto conto di quei paesi in cui il numero di utenti delle soluzioni anti-virus di Kaspersky Lab risulta ancora relativamente contenuto (meno di 10.000 utenti).*

***Quote percentuali relative al numero di utenti unici sui computer dei quali sono state bloccate e neutralizzate minacce informatiche locali, rispetto al numero complessivo di utenti unici dei prodotti Kaspersky Lab nel paese.*

Le prime venti posizioni della speciale graduatoria qui sopra riportata risultano quasi interamente occupate da paesi ubicati nel continente africano, in Medio Oriente e nel Sud-Est asiatico. Così come nel trimestre precedente, la leadership della TOP-20 è andata ad appannaggio del Vietnam, mentre la

Mongolia continua ad occupare il secondo gradino del "podio" virtuale. Il Nepal, da parte sua, ha "guadagnato" una posizione in classifica, passando dal quarto al terzo posto della stessa; il Bangladesh, per contro, è sceso dalla terza alla sesta piazza del rating qui analizzato. Segnaliamo, infine, la presenza di una "new entry" in graduatoria, ovvero il Marocco.



Tra i paesi che vantano in assoluto le quote percentuali più basse, in termini di rischio di contagio dei computer degli utenti da parte di infezioni informatiche locali, troviamo: Giappone (12,6%), Svezia (15%), Finlandia (15,3%), Danimarca (15,4%), Singapore (18,2%), Paesi Bassi (19,1%), Repubblica Ceca (19,5%).

In media, nel mondo, durante il primo trimestre del 2014, sono state rilevate infezioni IT di origine locale - perlomeno una volta - sul 34,7% dei computer degli utenti.