Evoluzione delle minacce informatiche nel primo trimestre del 2015

Maria Garnaeva
Victor Chebyshev
Denis Makrushin
Anton Ivanov

Sommario

Il trimestre in cifre

- Secondo i dati raccolti tramite il Kaspersky Security Network (KSN), lungo tutto l'arco del primo trimestre del 2015 i prodotti Kaspersky Lab hanno rilevato e neutralizzato 2.205.858.791 attacchi nocivi condotti nei confronti dei computer e dei dispositivi mobile degli utenti.
- Le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 469.220.213 attacchi condotti attraverso siti Internet compromessi, dislocati in vari paesi.
- Il nostro Anti-Virus Web ha effettuato il rilevamento di 28.483.783 oggetti nocivi unici (script, exploit, file eseguibili, etc.).
- In totale, sono stati individuati e bloccati, da parte del nostro modulo Anti-Virus Web, 93.473.068 URL unici.
- Il 40% degli attacchi web bloccati e neutralizzati grazie all'intervento dei prodotti anti-malware di Kaspersky Lab è stato condotto attraverso siti web dannosi dislocati sul territorio della Russia.
- Il nostro modulo Anti-Virus File ha rilevato con successo 253.560.227 oggetti nocivi unici, o potenzialmente indesiderabili.
- Nel trimestre oggetto del presente report, i prodotti Kaspersky Lab appositamente sviluppati per assicurare la protezione IT dei dispositivi mobile hanno effettuato il rilevamento di:
    - 147.835 pacchetti di installazione;
    - 103.072 nuove varianti di programmi dannosi specificamente creati dai virus writer per infettare i dispositivi mobile;
    - 1.527 Trojan bancari per piattaforme mobile.

Il quadro della situazione

Equation, gli attacchi APT in assoluto più complessi e sofisticati

Probabilmente, la notizia più eclatante del primo trimestre del 2015 è stata quella relativa alle attività condotte dal potente gruppo Equation, specializzato in operazioni di cyber-spionaggio. Esso interagisce, ormai da molti anni, con altri gruppi particolarmente influenti, quali Stuxnet e Flame. Gli attacchi informatici realizzati da Equation, tuttavia, sono forse i più sofisticati in assoluto: uno dei moduli nocivi utilizzati da tale gruppo consente, ad esempio, di poter riprogrammare il firmware dell'hard disk. Dal 2001, il gruppo Equation ha infettato migliaia di computer-vittima, situati in Iran, Russia, Siria, Afghanistan, Stati Uniti ed altri paesi. Nella fattispecie, sono stati coinvolti i seguenti settori: enti governativi, istituzioni diplomatiche, telecomunicazioni, industria aerospaziale, energia e numerosi altri ancora.

Il gruppo in questione ricorre all'utilizzo di una vasta gamma di programmi dannosi, alcuni dei quali addirittura superano, in termini di complessità, i già sofisticati software dispiegati nell'ambito della nota piattaforma "Regin". Tra i metodi utilizzati per generare la diffusione del malware Equation, e le conseguenti infezioni informatiche, citiamo, ad esempio, l'impiego del worm USB Fanny (il quale ha tra l'altro annoverato, nel proprio arsenale, due vulnerabilità zero-day, *successivamente* introdotte in Stuxnet), la presenza di installer nocivi su CD, nonché l'utilizzo di exploit web.

Carbanak, la campagna cybercriminale di maggior successo

Nella primavera del 2014 gli esperti di Kaspersky Lab sono stati coinvolti nella conduzione di un'indagine di tipo forense: di fatto, veniva misteriosamente sottratto denaro dagli apparecchi bancomat di un noto istituto bancario, peraltro senza alcuna interazione "fisica" dell'utente con il dispositivo. È proprio così che ha avuto inizio la lunga storia delle indagini da noi svolte riguardo alla campagna cybercriminale Carbanak, nel corso delle quali sono state eseguite approfondite ricerche ed analisi relativamente all'omonimo malware.

Carbanak è, in sostanza, una backdoor, originariamente scritta sulla base del codice nocivo di Carberp. Si tratta di un malware appositamente progettato per compiere operazioni di spionaggio, eseguire il processo di raccolta ed esfiltrazione dei dati, e condurre attività di controllo remoto sul computer infetto. Una volta che gli attaccanti sono penetrati all'interno della rete-vittima, essi effettuano una sorta di ricognizione manuale, con il preciso intento di compromettere computer di particolare rilevanza (come, ad esempio, quelli inerenti ai sistemi di elaborazione dati, ai sistemi contabili ed ai sistemi bancomat).

Sono state complessivamente individuate tre diverse modalità utilizzate dai cybercriminali per sottrarre cospicue somme di denaro dagli istituti bancari e procedere poi all'incasso delle stesse:

1. tramite gli apparecchi bancomat;
2. attraverso il trasferimento del denaro, per mezzo della rete SWIFT, sui conti bancari posseduti dai criminali informatici;
3. mediante l'alterazione dei database contenenti le informazioni relative agli account, in maniera tale da poter creare account fasulli provvisti di un saldo relativamente elevato, con tanto di successivo utilizzo dei servizi resi dai "muli" per procedere alla raccolta del denaro rubato.

L'infezione dei computer-vittima avviene attraverso le modalità tipiche delle campagne APT, ovvero per mezzo di attacchi di phishing mirati, nel corso dei quali si procede all'invio di messaggi e-mail contenenti, in allegato, un documento preposto a recapitare l'exploit. Le e-mail malevole vengono in genere confezionate in maniera tale da non destare sospetti; in alcuni casi, esse provengono addirittura dagli indirizzi di posta elettronica dello stesso personale della società sottoposta ad attacco.

Secondo le stime prodotte da Kaspersky Lab, il gruppo Carbanak è riuscito a colpire all'incirca 100 istituzioni finanziarie, situate principalmente nell'Europa Orientale. Le perdite complessivamente subite potrebbero addirittura ammontare ad 1 miliardo di dollari, rendendo quindi Carbanak, di gran lunga, la campagna cybercriminale di maggior successo sinora mai vista.

Desert Falcon, attacchi in Medio Oriente

Durante la conduzione di un'indagine in merito ad un incidente informatico prodottosi in Medio Oriente, gli esperti di Kaspersky Lab hanno rilevato le attività svolte da un gruppo sino a quel momento sconosciuto, intento a condurre attacchi di tipo mirato. Il gruppo in questione è denominato "Falco del Deserto" (Desert Falcon); si tratta del primo gruppo arabo impegnato in operazioni di cyberspionaggio, le quali vengono condotte su larga scala e, con ogni probabilità, sono dettate dalla delicata e complessa situazione politica che sta attraversando la regione mediorientale.

I primi segnali dell'attività svolta da Desert Falcon risalgono all'anno 2011; le prime infezioni note hanno poi avuto luogo nel corso del 2013; il picco delle attività di cyberspionaggio svolte dal gruppo in questione è stato infine registrato a cavallo tra la fine del 2014 e l'inizio del 2015. I membri di tale gruppo non sono di sicuro dei neofiti in questo settore, visto che, in pratica, hanno sviluppato da zero

programmi malware destinati a colpire i sistemi operativi Windows ed Android; oltre a ciò, essi hanno abilmente organizzato un complesso attacco in cui è stato fatto uso di messaggi di phishing, siti web contraffatti e falsi account sui social network.

Le vittime di Desert Falcon sono situate, principalmente, in Palestina, Egitto, Israele e Giordania. L'elenco delle vittime colpite include attivisti e leader politici, enti militari e governativi, mass media, istituzioni finanziarie ed ulteriori organizzazioni. Ad oggi si contano oltre 3.000 vittime; si stima che, complessivamente, gli attacker abbiano potuto sottrarre più di un milione di file e documenti.

In aggiunta a sofisticati mailing, peraltro accuratamente pianificati, preposti ad infettare le vittime predestinate, il gruppo Desert Falcon è solito ricorrere ad un ulteriore metodo di attacco: l'utilizzo dell'ingegneria sociale nell'ambito del social network Facebook. È stato in effetti rilevato come gli attacker abbiano appositamente creato account per avviare una corrispondenza con la vittima, guadagnarsi la fiducia di quest'ultima e poi recapitare alla stessa, mediante un servizio di chat, un programma malware, mascherato sotto forma di immagine. Inoltre, per generare infezioni di proporzioni maggiori, tale gruppo si è avvalso di post contenenti link nocivi, pubblicati a nome di account violati o fasulli facenti capo ad esponenti politici.

L'APT Animal Farm

Nel mese di marzo del 2014, il noto quotidiano francese Le Monde pubblicava un articolo sugli strumenti utilizzati nel corso di un'operazione di cyber-spionaggio individuata e svelata dal "Communications Security Establishment Canada" (CSEC), il Centro canadese per la sicurezza nel settore delle telecomunicazioni. Gli strumenti descritti erano stati impiegati nell'ambito dell'operazione Snowglobe, condotta nei confronti di vari mass media del Canada francofono, e rivolta ugualmente a Grecia, Francia, Norvegia ed alcuni paesi africani. Sulla base dei risultati dell'analisi eseguita, il CSEC supponeva che tale operazione potesse essere stata avviata, di fatto, dai servizi di intelligence francesi.

All'inizio del 2015, alcuni ricercatori hanno pubblicato i risultati di uno studio condotto su alcuni programmi malware (1, 2, 3), i quali presentavano molti aspetti del tutto simili o identici alle caratteristiche possedute dai software utilizzati nell'operazione Snowglobe. In particolare, erano stati identificati dei sample di malware contenenti al loro interno il nome Babar, il quale coincideva esattamente con la denominazione del programma menzionato nelle slide del CSEC canadese.

Gli esperti di Kaspersky Lab, dopo aver analizzato i programmi malware utilizzati nell'ambito della suddetta campagna, e dopo aver opportunamente messo in evidenza il collegamento esistente tra di loro, hanno coniato la definizione di Animal Farm per identificare il gruppo che si celava dietro l'impiego di tali software. È stato rilevato, nella circostanza, che due delle tre vulnerabilità zero-day individuate da Kaspersky Lab nel corso del 2014, utilizzate per la conduzione di cyber-attacchi, erano entrate a far parte dell'arsenale di cui disponeva questo gruppo. Ad esempio, l'attacco eseguito dal sito web violato del Ministero della Giustizia siriano, mediante l'impiego di exploit volti a sfruttare la vulnerabilità CVE-2014-0515, conduceva al download di uno degli strumenti utilizzati dal gruppo Animal Farm, malware denominato Casper.

Tra le caratteristiche peculiari di tale campagna, è di particolare interesse rilevare come uno dei programmi a disposizione del gruppo Animal Farm, ovvero NBOT, fosse preposto alla conduzione di attacchi DDoS; si tratta, indubbiamente, di una funzionalità nociva del tutto inconsueta per i gruppi APT di stampo "classico". È infine curioso osservare come uno degli "animali" nocivi in causa fosse provvisto

di uno strano nome, Tafacalou; è possibile che si tratti, nella fattispecie, di un'espressione in lingua occitana, idioma parlato, tra l'altro, anche in Francia.

Upatre, ampia ed attiva diffusione del banker Dyre/Dyreza

Nel trimestre oggetto del presente report, la prima posizione fra i Trojan bancari - a livello di diffusione degli stessi e numero complessivo di utenti attaccati - risulta occupata da Upatre, downloader del malware "finanziario" denominato Dyre, ugualmente noto con l'appellativo di Dyreza. Tale Trojan bancario, comparso sulla scena del malware già nel 2014, è stato appositamente progettato per prendere di mira gli utenti di varie istituzioni finanziarie. Per carpire le informazioni sensibili relative alle operazioni di pagamento esso si avvale di una particolare tecnica malevola, volta a bypassare le connessioni SSL protette. Inoltre, il malware in questione è ugualmente provvisto della funzionalità di RAT (Remote Administration Tool – strumento di amministrazione remota), per far sì che l'attaccante possa realizzare la transazione finanziaria in modalità manuale, a nome del cliente del sistema di banking online preso di mira.

Il Trojan-Downoader Upatre viene recapitato agli utenti-vittima per mezzo di appositi messaggi di spam nocivo, molti dei quali presentano le sembianze di e-mail del tutto legittime, apparentemente provenienti da note istituzioni finanziarie. L'elenco delle banche sottoposte ad attacco da parte del Trojan bancario Dyre, a sua volta caricato sul computer-vittima dal malware Upatre, comprende Bank of America, Natwest, Citibank, RBS e Ulsterbank. I ricercatori hanno rilevato che, al momento attuale, l'attività principale di Dyre si svolge sul territorio della Gran Bretagna.

PoSeidon, attacchi mirati nei confronti dei terminali PoS

È stato individuato un nuovo esemplare di Trojan bancario preposto ad attaccare i terminali PoS. PoSeidon effettua la scansione del contenuto della memoria operativa del dispositivo PoS, per rilevare la presenza di informazioni di pagamento non codificate, e trasmette poi le stesse al malintenzionato in agguato.

I ricercatori di Cisco Security Solutions hanno rilevato tre diverse componenti di un programma malware, le quali, con ogni probabilità, sono proprio in relazione con PoSeidon: si tratta di un keylogger, di un downloader e, di fatto, dello stesso scanner per la memoria operativa, il quale possiede ugualmente apposite funzionalità di verifica delle sequenze dei tasti premuti. Il keylogger è preposto al furto delle credenziali di accesso inerenti al programma LogMeIn, abitualmente utilizzato per eseguire le operazioni di accesso remoto. Esso rimuove in maniera preventiva, da LogMeIn, le password ed i profili cifrati, allo scopo di obbligare l'utente ad inserire di nuovo gli stessi. I ricercatori ritengono, quindi, che la funzione specifica del keylogger in causa consista proprio nel realizzare il furto dei dati originariamente utilizzati per l'accesso remoto, i quali si rivelano poi necessari per compromettere i sistemi PoS ed installare, successivamente, il malware PoSeidon.

Una volta che gli attacker hanno ottenuto l'accesso al terminale PoS, essi provvedono ad installare il downloader nel terminale; tale programma, a sua volta, genera il download, tramite i propri server di comando, dello scanner nocivo denominato FindStr. Quest'ultimo risulta preposto a ricercare, nella memoria operativa del dispositivo PoS, determinate stringhe, corrispondenti al numero della carta di credito. Una caratteristica di particolare interesse risiede nel fatto che, nella circostanza, vengono ricercati esclusivamente i numeri che iniziano con determinate cifre.

Le statistiche del primo trimestre 2015

Tutti i dati statistici riportati nel presente resoconto 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.

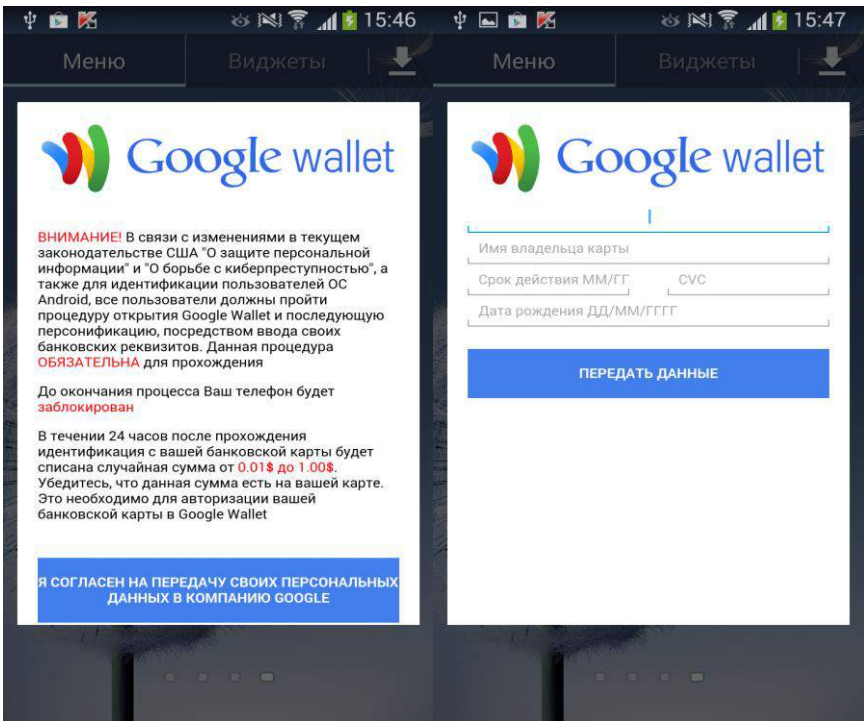
Le minacce IT per dispositivi mobile

La direzione principale nell'evoluzione del malware mobile è rappresentata dall'evidente processo di "monetizzazione" dello stesso: i virus writer, in effetti, cercano di fare in modo che le loro "creature" possano carpire, in vari modi, sia il denaro, sia i dati bancari degli utenti.

Un numero sempre crescente di Trojan-SMS, ad esempio, risulta adesso provvisto della specifica funzionalità nociva che consente di poter attaccare gli account bancari degli utenti-vittima. Così, il malware denominato Trojan-SMS.AndroidOS.OpFake.cc è ora in grado di condurre attacchi nei confronti di almeno 29 applicazioni collegate alla sfera bancaria e finanziaria.

I Trojan-SMS hanno inoltre iniziato ad avvalersi delle funzionalità tipiche dei cosiddetti Trojan "estorsori". Trojan-SMS.AndroidOS.FakeInst.ep, ad esempio, per entrare in possesso dei dati sensibili relativi alla carta di credito della vittima, utilizza uno dei classici metodi praticati dai programmi estorsori: nella circostanza, le finestre aperte sullo schermo del dispositivo mobile da tale software nocivo non possono essere chiuse senza aver prima introdotto i dati in questione.

In pratica, l'utente visualizza una notifica fasulla, emessa (in apparenza) a nome di Google, attraverso la quale si invita, in maniera peraltro pressante, ad aprire un account Google Wallet ed eseguire la procedura di "personalizzazione" dello stesso, introducendo i dati della propria carta di credito (è piuttosto curioso, a tal proposito, il fatto che si affermi, nella notifica, che una delle motivazioni alla base di tale richiesta risiede proprio nella necessità di dover combattere la criminalità informatica). In sostanza, finché la vittima non inserisce i dati confidenziali richiesti, non sarà possibile rimuovere la relativa finestra dallo schermo del dispositivo mobile.



Allo stesso tempo, vengono ugualmente modificati i Trojan-Spy, al pari dei Trojan-SMS; di fatto, gli autori di malware mobile prevedono anche per i primi la possibilità di condurre attacchi rivolti ai conti bancari dei potenziali utenti-vittima. Trojan-Spy.AndroidOS.SmsThief.ay, ad esempio, è adesso in grado di attaccare cinque diverse applicazioni di natura bancaria e finanziaria.

In tal modo, i software nocivi destinati alle piattaforme mobile, per mezzo dei quali i malintenzionati cercano di sottrarre denaro agli utenti - divengono, sempre più di frequente, dei veri e propri programmi multifunzionali. Attualmente, il furto del denaro custodito nei conti bancari degli utenti, realizzato attaccando le applicazioni di banking online, può essere quindi compiuto non soltanto dai famigerati Trojan-Banker, specializzati in questo genere di attività cybercriminale, ma anche da alcuni Trojan-SMS, e persino da certi Trojan-Spy. È possibile che sia proprio questo il motivo per cui, nel primo trimestre del 2015, è stato individuato un numero relativamente limitato di Trojan bancari per dispositivi mobile.

Complessivamente, nel trimestre oggetto del presente report, i malware mobile preposti al furto e all'estorsione del denaro degli utenti (Trojan-SMS, Trojan bancari e Trojan "estorsori") hanno rappresentato il 23,2% delle nuove minacce mobile comparse sulla scena del malware globale. Tutti e tre i tipi di software maligno sopra elencati sono estremamente pericolosi, mentre l'interesse degli scrittori di virus nei confronti del denaro posseduto dalle potenziali vittime ne stimola il continuo sviluppo.

Le novità del trimestre

1) Si è registrata una significativa evoluzione del Trojan bancario denominato Trojan-Banker.AndroidOS.Binka.d. Tale malware mobile, adesso, è provvisto di apposita funzione di "intercettazione" della vittima. Viene in pratica registrato, all'interno di un file, il suono

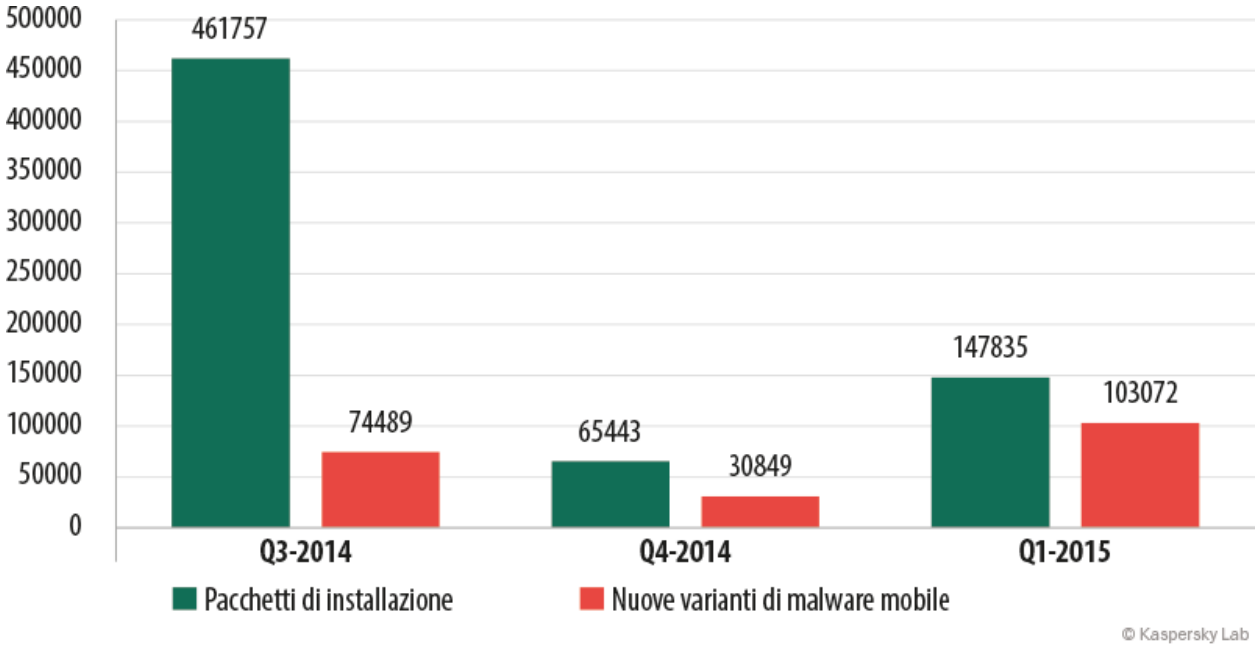
proveniente dal microfono; il file in causa viene poi trasmesso al server allestito dai malintenzionati.

2) La tecnica del "patching" dannoso, con la relativa iniezione di codice maligno, rappresenta, al momento attuale, uno dei principali metodi utilizzati per la diffusione dei Trojan. È proprio in tal modo, ad esempio, che è stato introdotto il malware Trojan-SMS.AndroidOS.Chyapo.a nell'applicazione Unity Launcher Free. La differenza tra l'applicazione "pulita" e quella dannosa può essere notata soltanto al momento della visualizzazione della richiesta di accesso all'elaborazione dei messaggi SMS in entrata. Un'ulteriore interessante peculiarità di tale Trojan è costituita dal relativo centro di comando e controllo, situato nell'hosting <sites.google.com>.
3) I creatori del Trojan-SMS denominato Podec hanno messo in atto un nuovo meccanismo per realizzare la diffusione di questo software nocivo, ovvero attraverso il social network VKontakte. Nella circostanza, il file dannoso è stato caricato sui server del popolare social network russo, utilizzati per custodire i contenuti generati dagli utenti. La conseguenza di tutto ciò è stata che il suddetto programma Trojan è andato a far parte della "trojka" dei malware leader per numero di utenti complessivamente attaccati.
4) Nell'ambito dei software dannosi, il contrapporsi all'azione protettiva svolta dalle soluzioni anti-malware non rappresenta di certo una novità a livello tecnologico; ad ogni caso, tale specifica attitudine sta acquisendo sempre maggiore popolarità presso le folte schiere dei virus writer. Il Trojan bancario denominato Trojan-Banker.AndroidOS.Svpeng.f, individuato nel corso del primo trimestre dell'anno, cerca ad esempio di rimuovere le applicazioni prodotte dalle società Avast, Eset e DrWeb.

Statistiche relative alle minacce mobile

Nel primo trimestre del 2015 i prodotti Kaspersky Lab adibiti alla protezione IT dei dispositivi mobile hanno rilevato **103.072** nuove varianti di malware mobile, ovvero un numero di minacce superiore di ben 3,3 volte rispetto all'analogo valore riscontrato nel quarto trimestre del 2014.

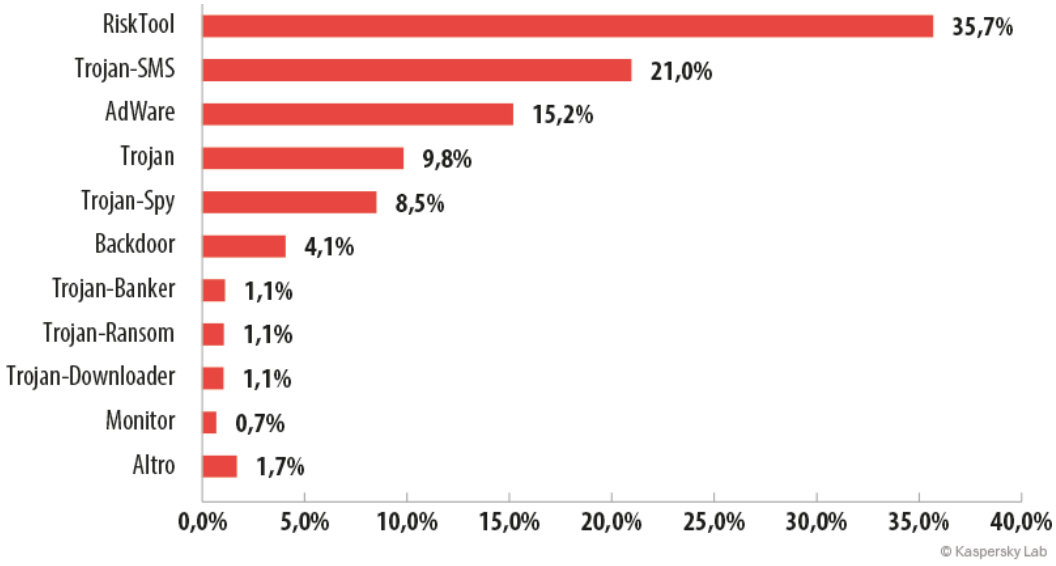
Nel corso del periodo oggetto della nostra analisi sono stati complessivamente individuati 147.835 pacchetti di installazione nocivi, in sostanza un numero di pacchetti dannosi superiore di 2,3 volte rispetto all'analoga quantità rilevata nel trimestre precedente.



Numero complessivo di pacchetti di installazione maligni e di nuove varianti di malware mobile individuati nel periodo 3° trimestre 2014 - 1° trimestre 2015

Abbiamo osservato, in questi ultimi tempi, una significativa diminuzione del valore che identifica la proporzione esistente tra il numero di nuovi programmi malware comparsi sulla scena e la quantità di pacchetti di installazione nocivi individuati. Nel terzo trimestre del 2014, per ogni programma malware destinato a colpire i dispositivi mobile si contavano, in media, 6,2 pacchetti di installazione dannosi; nel quarto trimestre dello stesso anno tale proporzione è diminuita di ben tre volte, scendendo a circa 2 pacchetti dannosi. Nel primo trimestre del 2015 l'indice in questione è ulteriormente diminuito, raggiungendo quota 1,4.

Ripartizione del malware mobile per tipologie



Suddivisione delle nuove varianti di malware mobile in base ai loro specifici comportamenti dannosi – Situazione relativa al primo trimestre del 2015

La speciale graduatoria del primo trimestre del 2015 riservata alla ripartizione degli oggetti maligni per dispositivi mobile in base agli specifici comportamenti nocivi da essi evidenziati, risulta capeggiata dai RiskTool (35,7%), applicazioni potenzialmente pericolose. Si tratta, di fatto, di applicazioni legittime, le quali, tuttavia, possono rivelarsi potenzialmente pericolose per gli utenti; il loro utilizzo inappropriato, da parte del proprietario dello smartphone o del malintenzionato di turno, può in effetti generare perdite di natura finanziaria per l'utente.

I Trojan-SMS, da parte loro, sono andati a collocarsi al secondo posto del rating, con una quota pari al 21%. Desideriamo ricordare come, nel terzo trimestre del 2014, l'indice percentuale ascrivibile ai Trojan-SMS, nell'ambito delle nuove minacce mobile, fosse sensibilmente diminuito, passando dal 22% al 14%. Per la fine dell'anno 2014, tuttavia, tale quota era già tornata ad attestarsi sui precedenti valori. Per ciò che riguarda il relativo tasso di crescita, tale tipologia di malware mobile si posiziona al terzo posto della graduatoria: nel corso dei primi tre mesi del 2015, il numero totale di Trojan-SMS presenti nella nostra "collezione" ha fatto registrare un aumento pari al 18,7%.

Il terzo gradino del "podio" virtuale risulta occupato dagli AdWare, ovvero le fastidiose applicazioni pubblicitarie potenzialmente indesiderate (15,2%). Occorre tuttavia sottolineare come il numero di tali programmi, nel flusso delle nuove minacce mobile, risulti in progressiva diminuzione.

La quota percentuale relativa ai Trojan bancari, nell'ambito del malware mobile rilevato nel primo trimestre dell'anno in corso, appare sensibilmente diminuita; essa ha fatto segnare, nel complesso, un valore pari all' 1,1%. Nell'arco del trimestre qui analizzato, il numero di nuovi Trojan bancari per piattaforme mobile - presenti all'interno della nostra raccolta - ha tuttavia fatto registrare un aumento pari al 6,5%.

Rileviamo ugualmente come i Trojan-Ransom, comparsi nell'arsenale dei cybercriminali in tempi relativamente recenti, evidenzino l'indice di crescita in assoluto più elevato, fra tutte le tipologie di minacce mobile attualmente in circolazione. Nel primo trimestre ne sono stati individuati ben 1.113; ciò significa che, nell'ambito della nostra collezione, il numero di programmi malware mobile provvisti di specifiche funzionalità di "estorsione" è addirittura aumentato del 65%. Si tratta, indubbiamente, di una tendenza alquanto pericolosa, visto che i programmi riconducibili a tale specifica tipologia sono esplicitamente orientati all'estorsione di denaro; l'infezione da essi provocata minaccia di compromettere irrimediabilmente i dati personali custoditi dagli utenti sul proprio dispositivo, così come di bloccare il funzionamento di quest'ultimo.

Un ulteriore genere di minaccia mobile che, attualmente, presenta un elevato indice di crescita è poi rappresentato dai programmi spyware (Trojan-Spy). Nel primo trimestre del 2015, in effetti, la quantità di spyware presenti nella nostra collezione di malware mobile ha fatto registrare un sensibile aumento, pari al 35%.

TOP-20 relativa ai programmi malware destinati alle piattaforme mobile

	Denominazione	% di attacchi*
1	DangerousObject.Multi.Generic	10,90%
2	AdWare.AndroidOS.Viser.a	9,20%
3	Trojan-SMS.AndroidOS.Podec.a	7,92%
4	RiskTool.AndroidOS.MimobSMS.a	7,82%
5	Trojan-SMS.AndroidOS.OpFake.a	6,44%
6	Trojan.AndroidOS.Mobtes.b	6,09%
7	Adware.AndroidOS.MobiDash.a	5,96%
8	Exploit.AndroidOS.Lotoor.be	4,84%
9	RiskTool.AndroidOS.SMSreg.gc	4,42%
10	AdWare.AndroidOS.Xynyin.a	3,31%
11	AdWare.AndroidOS.Ganlet.a	2,63%
12	Exploit.AndroidOS.Lotoor.a	2,19%
13	AdWare.AndroidOS.Dowgin.l	2,16%
14	Trojan-SMS.AndroidOS.Stealer.a	2,08%
15	AdWare.AndroidOS.Kirko.a	2,04%
16	Trojan.AndroidOS.Rootnik.a	1,82%
17	Trojan.AndroidOS.Pawen.a	1,81%
18	Trojan-SMS.AndroidOS.Gudex.f	1,75%
19	RiskTool.AndroidOS.SMSreg.dd	1,69%
20	AdWare.AndroidOS.Kemoge.a	1,52%

** Quote percentuali relative al numero di utenti attaccati da tale malware mobile, sul numero complessivo di utenti unici sottoposti ad attacco*

Il primo posto della speciale graduatoria è andato ad appannaggio del malware classificato come DangerousObject.Multi.Generic (10,90%). L'individuazione delle nuove applicazioni dannose avviene grazie alle sofisticate tecnologie implementate attraverso la rete globale di sicurezza Kaspersky Security Network (KSN), le quali permettono ai nostri prodotti anti-malware di poter reagire in ogni frangente, con la massima rapidità, nei confronti di minacce IT nuove o sconosciute.

Gli AdWare, ovvero le applicazioni pubblicitarie potenzialmente indesiderate, occupano ben sette posizioni all'interno del rating da noi stilato, tra cui anche il secondo posto della classifica, dove spicca la presenza del modulo pubblicitario AdWare.AndroidOS.Viser.a (9,2%).

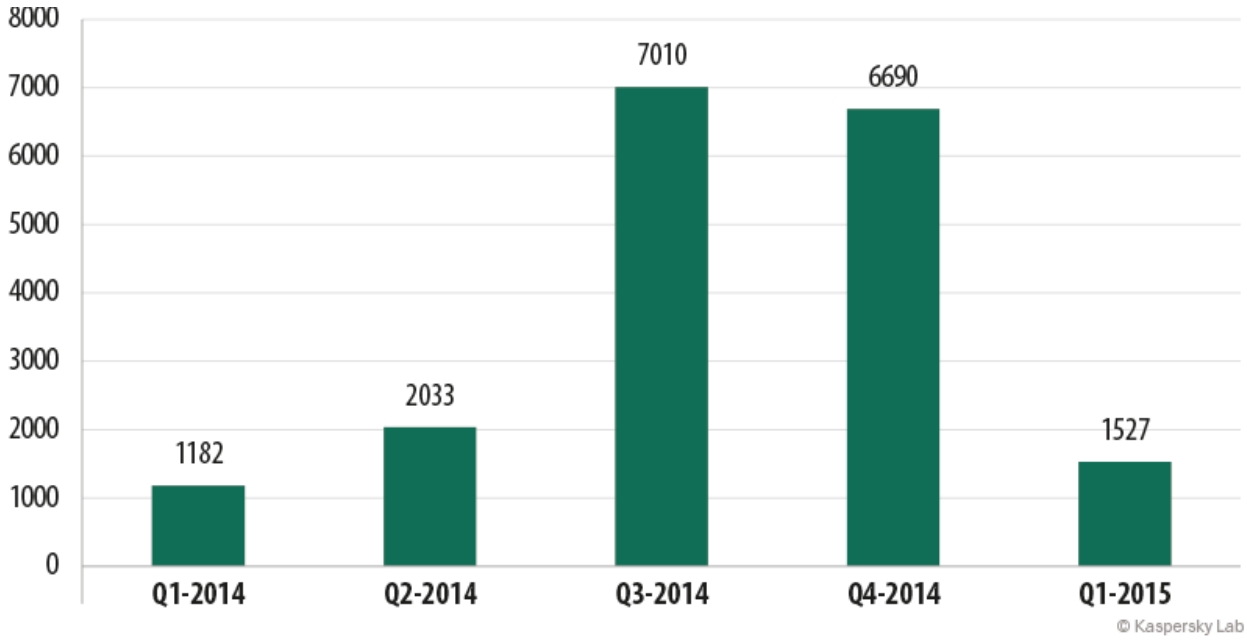
Osserviamo, inoltre, come nell'ambito della TOP-20 relativa alle minacce informatiche destinate ai dispositivi mobile, i Trojan-SMS continuino a perdere progressivamente posizioni: in effetti, mentre nel quarto trimestre del 2014 tali programmi malware occupavano ben nove posizioni all'interno del rating in questione, nel periodo oggetto del presente report i Trojan-SMS presenti in graduatoria risultano essere soltanto in numero di quattro.

Allo stesso tempo, il temibile malware denominato Trojan-SMS.AndroidOS.Podec.a (7,92%) entra a far parte, per il secondo trimestre consecutivo, della TOP-3 relativa alle minacce mobile maggiormente attive; tale circostanza dipende essenzialmente dalla notevole diffusione di cui esso è oggetto. Come abbiamo accennato in precedenza, i malintenzionati hanno provveduto a caricare tale software nocivo nei server adibiti a custodire i contenuti generati dagli utenti di VKontakte, il più esteso e frequentato social network russo. Tra le altre cose, questo Trojan risulta ben noto agli esperti di sicurezza IT proprio per il fatto che utilizza il più potente offuscatore di tipo "commerciale" sinora mai realizzato.

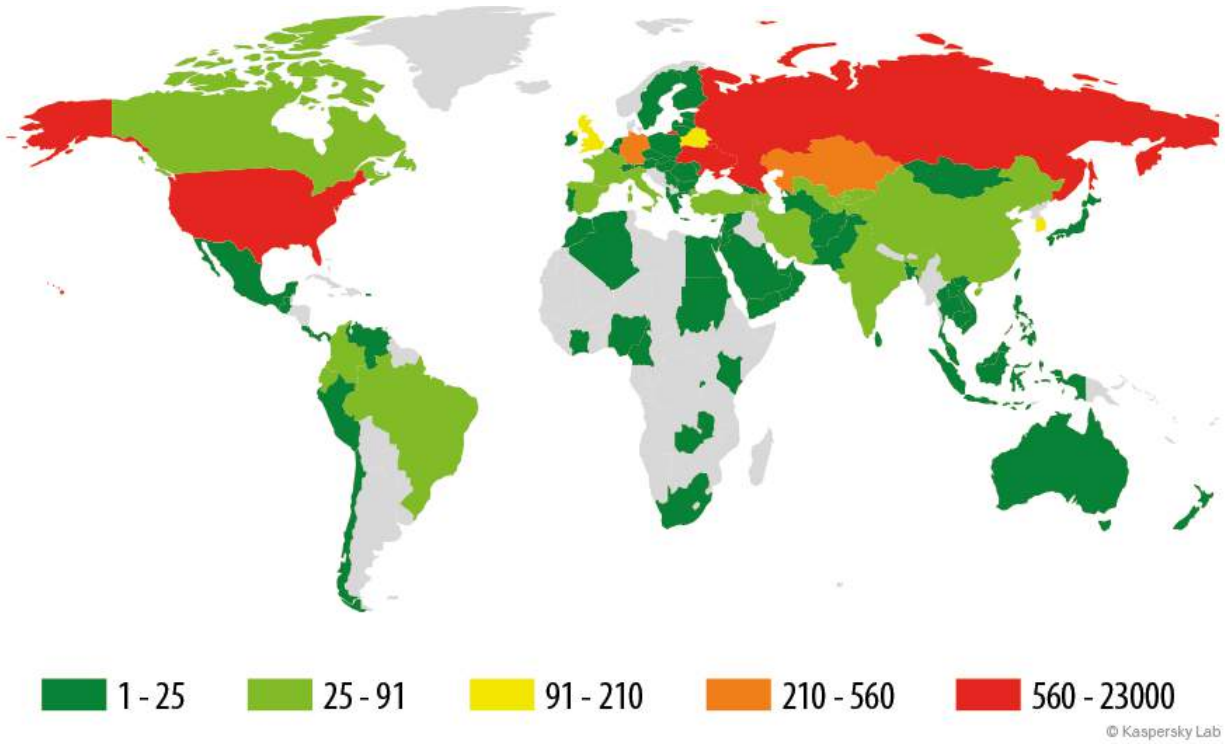
All'interno della speciale graduatoria del malware mobile da noi stilata, troviamo ugualmente alcuni rappresentanti della categoria RiskTool, i quali sono andati ad occupare tre posizioni delle venti disponibili nell'ambito della TOP-20 qui esaminata. Ad esempio, al quarto posto del rating si è insediato il programma RiskTool.AndroidOS.MimobSMS.a, sul quale si è imbattuto il 7,82% del numero complessivo di utenti unici sottoposti ad attacco.

I Trojan bancari per piattaforme mobile

Nel periodo oggetto della nostra analisi sono stati da noi individuati 1.527 Trojan bancari appositamente sviluppati per colpire i dispositivi mobile, ovvero un numero 4,4 volte inferiore rispetto all'analoga quantità rilevata nel trimestre precedente.



Numero di Trojan bancari per piattaforme mobile individuati nel periodo 1° trimestre 2014 - 1° trimestre 2015



Quadro mondiale relativo alla ripartizione geografica dei tentativi di infezione compiuti, nel corso del primo trimestre 2015, dai Trojan bancari destinati ai dispositivi mobile (numero di utenti sottoposti ad attacco)

Il 96% degli attacchi informatici condotti dai cybercriminali mediante il dispiegamento di Trojan bancari per sistemi operativi mobile, si è verificato in soli 10 paesi.

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

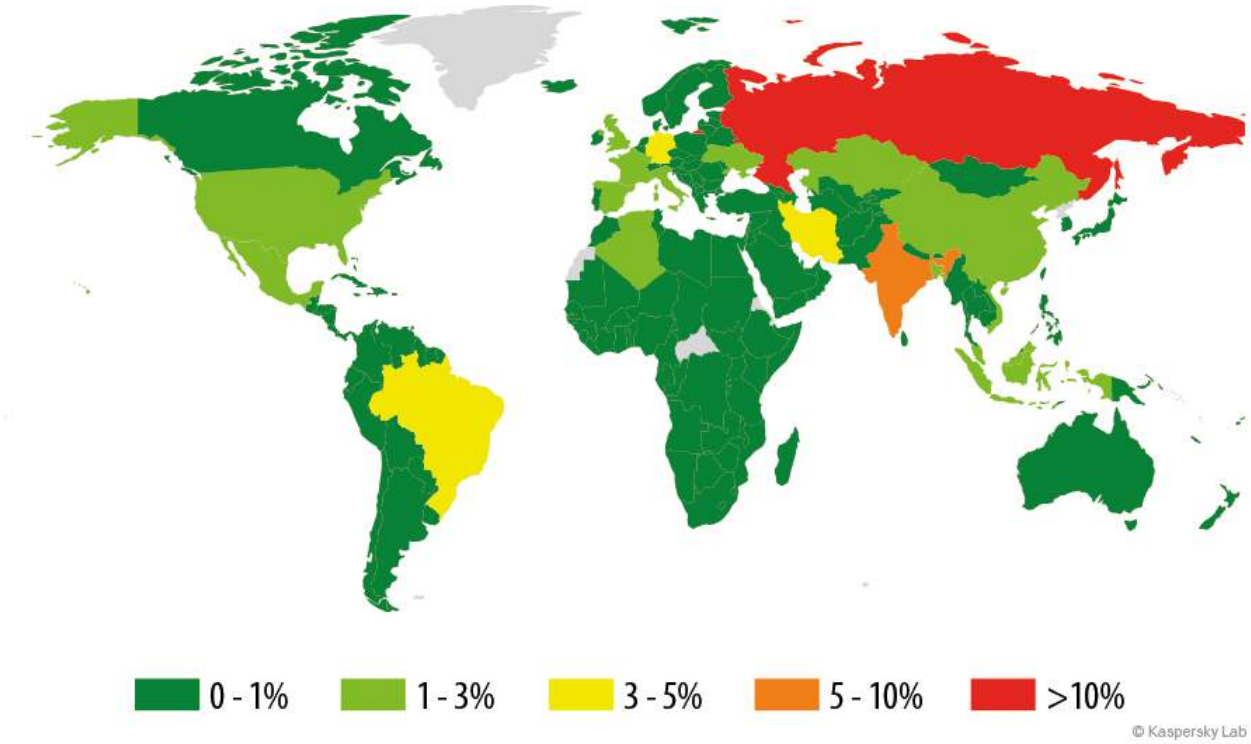
	Paese	**% sul numero complessivo di attacchi***
1	Russia	86,66%
2	Ukraina	2,27%
3	USA	2,21%
4	Kazakhstan	1,87%
5	Germania	0,97%
6	Repubblica di Corea	0,70%
7	Bielorussia	0,64%
8	Gran Bretagna	0,37%
9	Uzbekistan	0,34%
10	India	0,21%

** Quote percentuali relative al numero di utenti attaccati nel paese, in relazione al numero complessivo di utenti sottoposti ad attacco*

Come da tradizione ormai ampiamente consolidata, la leadership del ranking in questione continua ad essere detenuta dalla Federazione Russa. In seconda posizione troviamo poi l'Ukraina, seguita da Stati Uniti e Kazakhstan, paesi collocatisi, rispettivamente, al terzo e al quarto posto della speciale graduatoria. La Bielorussia, da parte sua, è scesa dalla quinta alla settima piazza della classifica.

Geografia delle minacce mobile

Nel primo trimestre del 2015 si sono registrati attacchi informatici da parte di programmi malware destinati ai dispositivi mobile - perlomeno una volta - in ben 213 diversi paesi del globo.



Quadro mondiale relativo alla ripartizione geografica dei tentativi di infezione compiuti, nel corso del primo trimestre del 2015, dai programmi malware specificamente sviluppati per colpire i dispositivi mobile (percentuali calcolate sul numero complessivo di utenti sottoposti ad attacco)

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

	Paese	% di attacchi*
1	Russia	41,92%
2	India	7,55%
3	Germania	4,37%
4	Brasile	3,20%
5	Iran	3,12%
6	Kazakhstan	2,88%
7	USA	2,84%
8	Ukraina	2,53%
9	Malaysia	2,05%

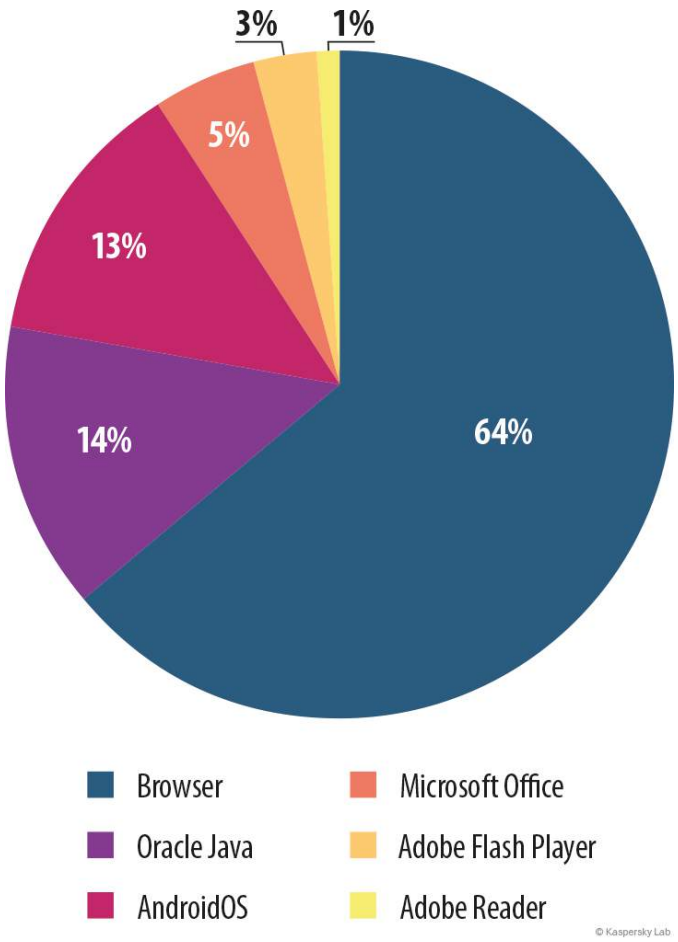
10	Vietnam	1,87%

** Quote percentuali relative al numero di utenti attaccati nel paese, in relazione al numero complessivo di utenti sottoposti ad attacco*

Come evidenzia la tabella qui sopra inserita, leader incontrastato del rating, peraltro con un elevato margine percentuale rispetto agli altri paesi presenti in graduatoria, rimane la Federazione Russa, con una quota pari al 42% del numero complessivo di utenti sottoposti ad attacco da parte di malware mobile. Il secondo gradino del "podio" virtuale risulta occupato dall'India, con una quota pari al 7,5%.

Le applicazioni vulnerabili maggiormente sfruttate dai malintenzionati

La speciale graduatoria delle applicazioni vulnerabili, qui di seguito riportata, è stata elaborata sulla base dei dati statistici da noi raccolti in merito alle operazioni di rilevamento e neutralizzazione degli exploit da parte dei prodotti Kaspersky Lab; il grafico tiene in debita considerazione sia gli exploit utilizzati dai malintenzionati per la conduzione degli attacchi informatici via Web, sia gli exploit impiegati dai malfattori per compromettere le applicazioni custodite "localmente" sui computer o sui dispositivi mobile degli utenti.



Ripartizione degli exploit - utilizzati dai cybercriminali per la conduzione di attacchi informatici - in base alle varie tipologie di applicazioni sottoposte ad attacco - Situazione relativa al primo trimestre del 2015

Al primo posto della speciale classifica da noi stilata, relativa al primo trimestre del 2015, troviamo la categoria "Browser" (64%), la quale comprende gli exploit destinati ad Internet Explorer. Tale categoria ha tra l'altro detenuto la leadership della graduatoria generale inerente al 2014, sulla base degli indici percentuali rilevati nel corso degli ultimi tre trimestri.

Nel primo trimestre dell'anno corrente è stata da noi osservata una significativa diminuzione del numero di exploit appositamente creati per colpire la piattaforma Oracle Java (- 7 punti percentuali rispetto al quarto trimestre del 2014). Ciò trova una logica spiegazione nel fatto che gli exploit volti a sfruttare le vulnerabilità individuate in tali applicazioni sono stati quasi completamente esclusi dalla composizione di tutti gli exploit pack.

Abbiamo inoltre rilevato come nel primo trimestre siano cresciute in maniera significativa le quantità degli exploit rivolti, rispettivamente, a Microsoft Office (+ 2 punti percentuali rispetto al quarto trimestre del 2014) e Adobe Flash Player (+ 1%).

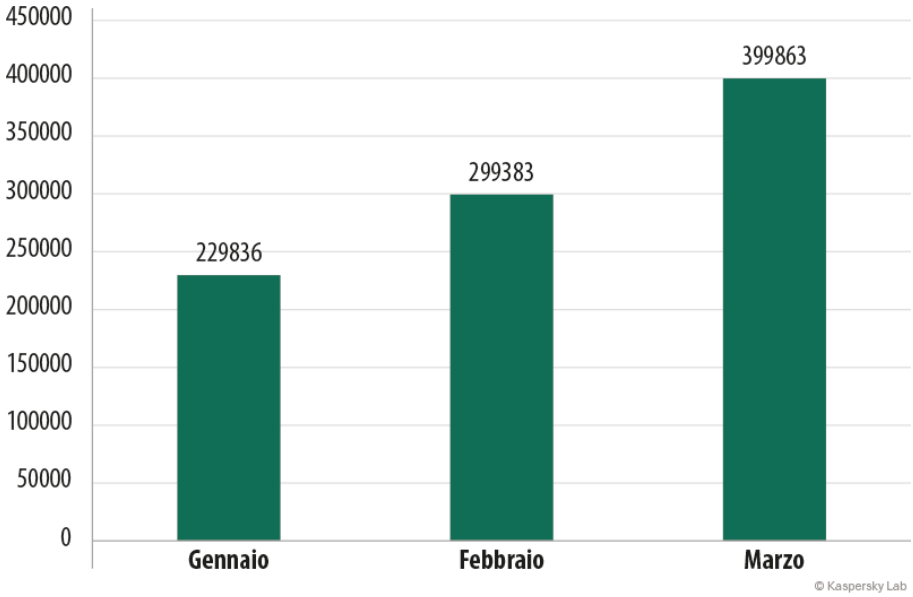
L'aumento del numero di oggetti dannosi destinati a quest'ultima applicazione è dovuto, in primo luogo, all'elevato numero di vulnerabilità rilevate nel primo trimestre del 2015. Attualmente, quasi tutti i kit di exploit ricorrono, di fatto, all'utilizzo di exploit appositamente confezionati per attaccare le vulnerabilità individuate in Adobe Flash Player.

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, modulo di sicurezza 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.

Le minacce online rivolte al settore bancario

Complessivamente, nel primo trimestre del 2015, le soluzioni di sicurezza IT sviluppate da Kaspersky Lab hanno respinto tentativi di infezione informatica, da parte di programmi malware appositamente elaborati dai virus writer per colpire la sfera bancaria - e carpire quindi le risorse finanziarie degli utenti-vittima mediante l'accesso non autorizzato agli account bancari posseduti da questi ultimi - sui computer di ben 929.082 utenti della rete globale di sicurezza Kaspersky Security Network. Desideriamo sottolineare come, rispetto all'analogo valore rilevato nel trimestre precedente (565.515), tale indice abbia fatto registrare un forte incremento, pari al 64,3%.

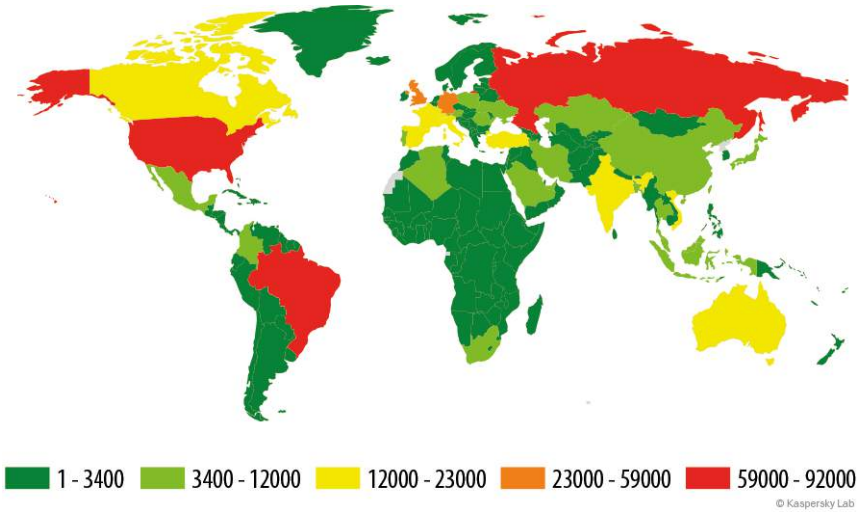


Numero di computer sottoposti ad attacco da parte di malware finanziari - Situazione relativa al primo trimestre del 2015

Come evidenzia il grafico qui sopra riportato, lungo tutto l'arco del trimestre oggetto del presente report il numero degli attacchi condotti mediante l'utilizzo di malware riconducibili alla sfera finanziaria è risultato in progressivo aumento. Rileviamo, in particolar modo, come il numero di tali attacchi informatici sia aumentato in maniera considerevole proprio nel mese di marzo del 2015.

Complessivamente, nel corso del trimestre qui preso in esame, le soluzioni di sicurezza IT sviluppate da Kaspersky Lab ed implementate nei computer degli utenti iscritti al programma di protezione globale KSN, hanno fatto registrare **5.106.804** notifiche relative a tentativi di infezione condotti da parte di programmi malware preposti al furto delle risorse finanziarie degli utenti attraverso l'accesso online (illecito!) ai relativi conti bancari presi di mira.

Geografia degli attacchi



Quadro mondiale relativo agli attacchi informatici condotti dai cybercriminali - nel corso del 1° trimestre 2015 - mediante l'utilizzo di malware bancario (in base al numero di utenti attaccati nei vari paesi del globo)

TOP-10 relativa ai paesi in cui si è registrato il numero più elevato di utenti sottoposti ad attacco informatico da parte di malware bancari

Paesi	Numero di utenti sottoposti ad attacco
Brasile	91.893
Russia	85.828
USA	66.699
Germania	51.670
Gran Bretagna	25.269
India	22.085
Turchia	21.397
Australia	18.997
Italia	17.663
Spagna	17.416

Così come in precedenza, la speciale graduatoria relativa ai paesi in cui si è registrato il maggior numero di utenti sottoposti ad attacco IT da parte del malware bancario, risulta capeggiata dal Brasile; rispetto al trimestre precedente (79.845), la quota relativa al "colosso" del continente latino-americano ha fatto registrare un incremento pari al 15%.

TOP-10 inerente alle famiglie di malware bancario maggiormente diffuse

La speciale TOP-10 relativa alle famiglie a cui appartengono i programmi malware maggiormente utilizzati, nel corso del primo trimestre del 2015, nell'ambito degli attacchi informatici eseguiti dai malintenzionati nei confronti degli utenti dei sistemi di online banking - redatta sulla base del numero totale di utenti sottoposti ad attacco - si presenta nella maniera seguente:

	Denominazione	Numero di notifiche	Numero di utenti sottoposti ad attacco
1	Trojan-Downloader.Win32.Upatre	3.127.365	349.574
2	Trojan-Spy.Win32.Zbot	865.873	182.966
3	Trojan-Banker.Win32.ChePro	355.735	91.809
4	Trojan-Banker.Win32.Banbra	35.182	16.363
5	Trojan.Win32.Tinba	94.972	15.719
6	Trojan-Banker.Win32.Agent	44.640	12.893
7	Trojan-Banker.Win32.Shiotob	60.868	12.283
8	Trojan-Banker.Win32.Banker	39.728	12.110
9	Trojan-Spy.Win32.SpyEyes	57.418	9.168
10	Backdoor.Win32.Papras	56.273	3.062

È di particolare rilevanza sottolineare come la stragrande maggioranza delle famiglie di malware presenti nella composizione della speciale TOP-10 da noi elaborata, riportata nella tabella qui sopra inserita, si avvalga di apposite tecniche di "web injection", utilizzate per iniettare codice HTML arbitrario all'interno della pagina web visualizzata dall'utente tramite il proprio browser; al tempo stesso, i

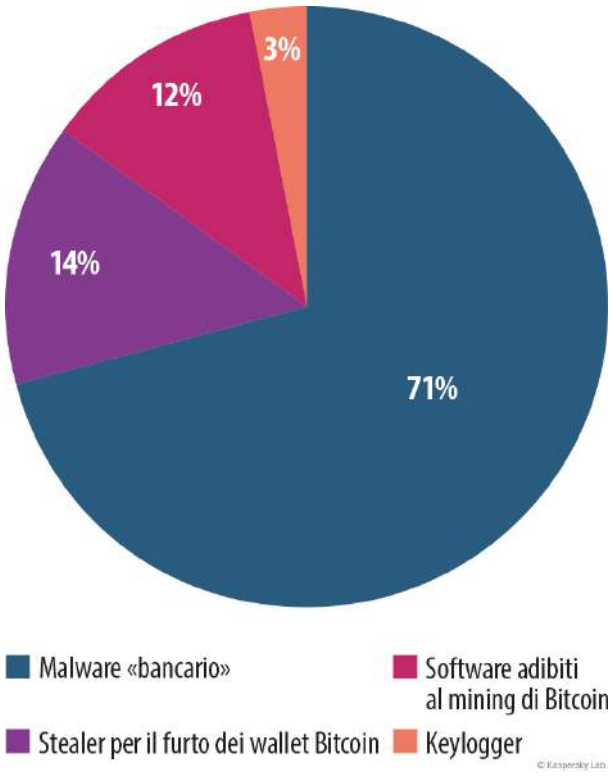
suddetti malware fanno largo uso di sofisticati processi di intercettazione dei dati sensibili relativi alle transazioni finanziarie eseguite in Rete dagli utenti, dati inseriti da questi ultimi nei form appositamente contraffatti, i quali vanno poi a rimpiazzare i moduli originali.

Il famigerato software maligno ZeuS (Trojan-Spy.Win32.Zbot) - il quale era risultato essere il Trojan bancario maggiormente diffuso nel 2014 (nell'ambito dell'apposita graduatoria relativa all'intero anno) - nel primo trimestre del 2015 ha ceduto il primo posto della classifica al malware denominato Trojan-Downloader.Win32.Upatre. I software dannosi riconducibili a tale specifica famiglia sono tutt'altro che complessi e presentano, per di più, dimensioni decisamente esigue (all'incirca non oltre i 3,5 Kb); di solito, i programmi Trojan sopra citati vengono adibiti al download di un temibile Trojan bancario appartenente alla famiglia attualmente nota con tre diversi appellativi - Dyre/Dyzap/Dyreza. L'elenco degli istituti finanziari sottoposti ad attacco da parte di tale banker dipende, naturalmente, dal relativo file di configurazione, trasmesso di volta in volta dal centro di comando e controllo predisposto dai cybercriminali.

Sul terzo gradino del "podio" virtuale troviamo un ulteriore rappresentante dei Trojan bancari, ovvero Trojan-Banker.Win32.ChePro. Tale software nocivo è solito diffondersi tramite appositi messaggi e-mail di spam nocivo, il cui oggetto si "ispira", abitualmente, a temi ed argomentazioni inerenti al banking online (l'oggetto dell'e-mail può essere, ad esempio "Account di Internet banking"). Le suddette e-mail dannose recano, al loro interno, un documento Word contenente una determinata illustrazione; cliccando su quest'ultima, l'ignaro destinatario del messaggio provoca, inconsapevolmente, l'esecuzione del temibile codice nocivo subdolamente "recapitato" dai cybercriminali.

Le minacce «finanziarie»

Le minacce informatiche legate alla sfera finanziaria degli utenti non si limitano al solo malware bancario, appositamente creato e sviluppato dai virus writer per attaccare i clienti dei sistemi di banking online.



Ripartizione percentuale degli attacchi condotti mediante l'utilizzo di malware finanziario

La seconda tipologia di minaccia IT per grado di popolarità e diffusione - tra i vari metodi alternativi praticati dai malfattori per realizzare il furto del denaro elettronico - è rappresentata dagli stealer adibiti al furto dei portafogli virtuali Bitcoin, gli ambiti wallet digitali contenenti criptovaluta. Allo stesso tempo, i malintenzionati non disdegnano affatto di utilizzare le risorse e la potenza di calcolo di cui è provvisto il computer della vittima designata, con il preciso intento di generare la celebre criptomoneta; nella circostanza, i cybercriminali ricorrono all'utilizzo dei Bitcoin miner nocivi, le famigerate applicazioni adibite al mining dei Bitcoin a totale insaputa dell'utente sottoposto ad attacco.

TOP-20 relativa agli oggetti infetti rilevati in Internet

Come abbiamo visto, nel corso del primo trimestre del 2015 il nostro Anti-Virus Web ha effettuato il rilevamento di 28.483.783 oggetti dannosi unici (script, 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 95,9% del volume complessivo di attacchi informatici condotti dai cybercriminali attraverso i browser web.

TOP-20 relativa agli oggetti infetti rilevati in Internet

	Denominazione*	% sul totale complessivo degli attacchi**
1	Malicious URL	37,55%
2	AdWare.JS.Agent.bg	36,06%
3	AdWare.Script.Generic	6,58%
4	Trojan.Script.Iframer	4,49%
5	AdWare.NSIS.AnProt.b	3,83%
6	Trojan.Script.Generic	2,91%
7	AdWare.JS.Agent.an	1,06%
8	AdWare.Win32.Yotoon.bfm	0,81%
9	Trojan.JS.Redirector.ads	0,47%
10	Exploit.Script.Blocker	0,33%
11	AdWare.Win32.Eorezo.eod	0,31%

12	Trojan.Win32.Generic	0,24%
13	Trojan-Downloader.Win32.Generic	0,22%
14	AdWare.Win32.ConvertAd.vo	0,17%
15	Trojan-Downloader.Script.Generic	0,16%
16	AdWare.NSIS.Agent.bx	0,16%
17	AdWare.NSIS.Agent.cv	0,13%
18	AdWare.AndroidOS.Xynyin.a	0,13%
19	AdWare.Win32.Yotoon.heur	0,12%
20	AdWare.Win32.SoftPulse.xvm	0,12%

** 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.*

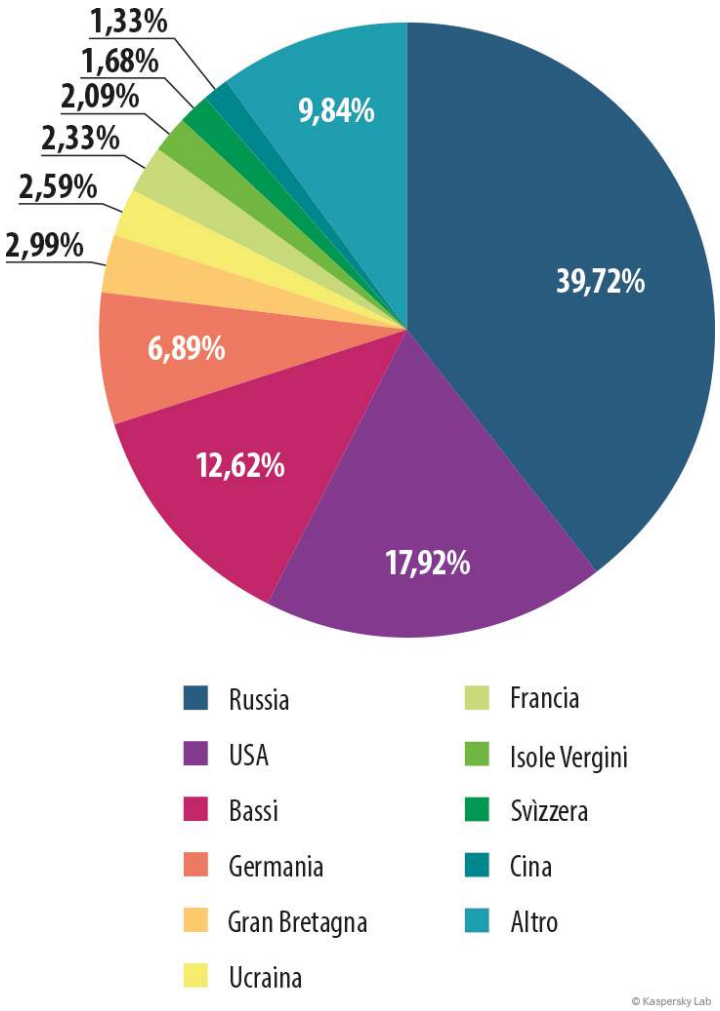
Tradizionalmente, la TOP-20 analizzata nel presente capitolo del report annovera, per la maggior parte, la presenza di "verdetti" riconducibili ad oggetti maligni utilizzati dai cybercriminali per la conduzione di attacchi di tipo drive-by e, al tempo stesso, la presenza di un elevato numero di programmi AdWare. Come si può vedere, al primo posto della speciale TOP-20 dedicata agli oggetti nocivi rilevati in Internet figurano, per l'ennesima volta, proprio gli URL maligni - ovverosia quei link che conducono a programmi malware di vario tipo - con una quota pari al 37,55% del volume complessivo dei rilevamenti effettuati dal modulo Anti-Virus Web. Si tratta, in sostanza, di indirizzi Internet inseriti nella nostra blacklist, relativi ad un consistente numero di siti nocivi verso i quali vengono reindirizzati gli ignari utenti-vittima.

Geografia delle fonti degli attacchi web: TOP-10

Tali dati statistici si riferiscono alla ripartizione per paesi delle fonti degli attacchi web condotti 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 attacchi 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 2015 le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 469.220.213 attacchi condotti attraverso siti Internet compromessi dislocati in vari paesi. Il 90% 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.



Ripartizione per paesi delle fonti degli attacchi web - Situazione relativa al primo trimestre del 2015

La composizione della speciale TOP-10 da noi elaborata - riguardante i paesi che attualmente detengono le posizioni di maggior rilievo nell'ambito dell'apposito rating relativo alle principali fonti degli attacchi informatici condotti via Internet - risulta ormai invariata da tempo; ad ogni caso, nel trimestre qui analizzato, è cambiata la leadership della graduatoria. La prima posizione della classifica da noi stilata è andata in effetti ad appannaggio della Russia, con un indice che sfiora quasi il 40%; in precedenza, la Federazione Russa occupava la quarta piazza del rating. Gli Stati Uniti, che detenevano la leadership dell'analoga graduatoria relativa al trimestre precedente, sono in tal modo scesi in seconda posizione, avendo fatto registrare, complessivamente, una quota pari al 18%.

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. 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 sottoposti ad attacco**
1	Kazakhstan	42,37%
2	Russia	41,48%
3	Azerbaijan	38,43%
4	Ukraina	37,03%
5	Croazia	37,00%
6	Armenia	35,74%
7	Mongolia	33,54%
8	Moldavia	33,47%
9	Bielorussia	33,36%
10	Kirghizistan	32,20%
11	Algeria	32,12%
12	Qatar	31,15%
13	Georgia	30,69%
14	Emirati Arabi Uniti	29,36%
15	Lettonia	28,69%
16	Tagikistan	28,36%
17	Bosnia ed Erzegovina	28,00%

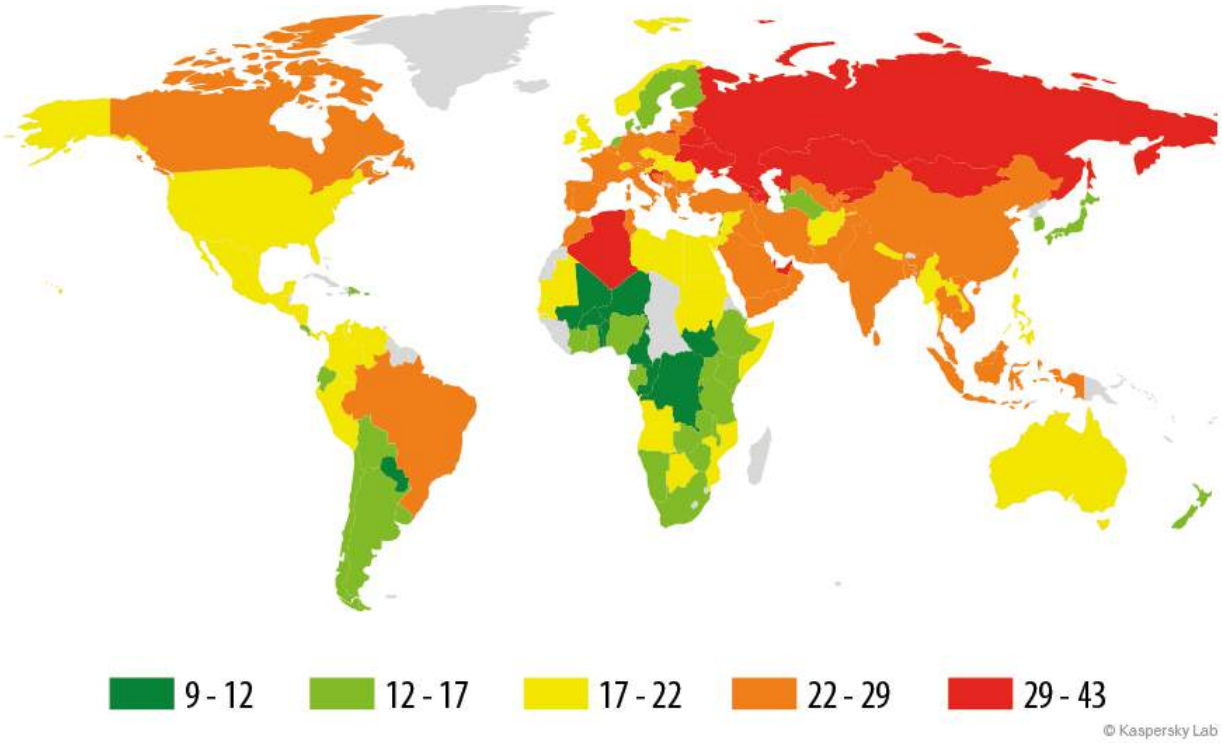
18	Grecia	27,55%
19	Tunisia	27,54%
20	Bulgaria	27,44%

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.*

Nel trimestre qui analizzato, la prima posizione del rating è andata ad appannaggio, per la prima volta, del Kazakhstan; la Russia è in tal modo scesa al secondo posto della graduatoria. Rileviamo inoltre come, rispetto al trimestre precedente, non facciano più parte della TOP-20 né Vietnam, né Portogallo. Le "new entry" del rating sono rappresentate da Bosnia ed Erzegovina (28,00%) e Grecia (27,55%); tali paesi sono andati ad occupare, rispettivamente, il 17° e il 18° posto della graduatoria.

Nel gruppo dei paesi in cui la navigazione in Internet risulta più sicura troviamo Giappone (12,4%), Danimarca (12,7%), Singapore (14,3%), Finlandia (14,9%), Sudafrica (14,8%), Paesi Bassi (15,2%).



Complessivamente, a livello mondiale, nel corso del trimestre oggetto della nostra analisi, una consistente porzione degli utenti della Rete (26,3%), 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 2015. 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.

Lungo tutto l'arco del primo trimestre dell'anno in corso, il nostro modulo Anti-Virus File ha rilevato con successo 253.560.227 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	22,56%
2	Trojan.WinLNK.StartPage.gena	17,05%
3	Trojan.Win32.Generic	15,06%
4	AdWare.Script.Generic	6,12%
5	WebToolbar.Win32.Agent.azm	4,49%
6	WebToolbar.JS.Condonit.a	4,20%
7	AdWare.Win32.Agent.heur	4,15%
8	RiskTool.Win32.BackupMyPC.a	3,83%
9	Downloader.Win32.Agent.bxib	3,74%

10	Trojan.Win32.AutoRun.gen	3,70%
11	Trojan.VBS.Agent.ue	3,64%
12	Downloader.Win32.MediaGet.elo	3,42%
13	AdWare.Win32.SearchProtect.ky	3,34%
14	Worm.VBS.Dinihou.r	3,31%
15	Virus.Win32.Sality.gen	3,18%
16	AdWare.Win32.DealPly.brj	2,86%
17	Trojan.Script.Generic	2,74%
18	AdWare.Win32.NewNext.a	2,70%
19	WebToolbar.JS.CroRi.b	2,66%
20	AdWare.MSIL.Kranet.heur	2,49%

**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 del nostro modulo Anti-Virus File.*

Tradizionalmente, il rating qui sopra riportato è relativo ai "verdetti" riconducibili ai programmi AdWare ed ai loro componenti (come, ad esempio, Trojan.VBS.Agent.ue), così come ai worm che si diffondono attraverso i supporti di memoria rimovibili. Gli oggetti riconducibili a tali specifiche tipologie sono andati ad occupare ben 13 posizioni all'interno del rating.

Rileviamo, inoltre, come sia entrato a far parte, per la prima volta, della TOP-20 in questione - posizionandosi peraltro subito al secondo posto della stessa - il malware denominato Trojan.WinLNK.StartPage.gena. Tale verdetto identifica i file LNK contenenti un link preposto ad attivare il browser Internet, in cui viene indicata la pagina web da aprire. Le pagine in causa, di solito, hanno nomi che imitano la denominazione dei motori di ricerca; esse, in realtà, provvedono a reindirizzare l'utente verso siti web dal contenuto discutibile od equivoco. Alcuni di questi siti possono rivelarsi pericolosi, ed essere quindi rilevati dal modulo Anti-Virus Web. Simili file LNK sono stati individuati in maniera particolarmente attiva nello scorso mese di gennaio.

Il malware classificato dagli esperti di sicurezza IT con la denominazione di Virus.Win32.Sality.gen rimane, di fatto, l'unico rappresentante della categoria dei virus nell'ambito della graduatoria in questione; così come in precedenza, tuttavia, esso continua a perdere posizioni all'interno del rating.

In effetti, ormai da tempo, la quota percentuale inerente ai computer infettati da tale virus continua progressivamente a diminuire. Nel trimestre qui analizzato, il virus Sality si è posizionato al 15° posto della TOP-20, avendo fatto complessivamente registrare un indice pari al 3,18%.

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

È stata calcolata, per ogni paese, la percentuale di utenti dei prodotti Kaspersky Lab che, nel corso del periodo preso in esame nel presente report, ha visto entrare in azione il modulo Anti-Virus File, specificamente dedicato al rilevamento delle minacce IT locali. Tali dati statistici costituiscono, in pratica, il riflesso del grado medio di infezione dei personal computer nei vari paesi del mondo.

TOP-20 relativa ai paesi in cui sono state rilevate le quote percentuali più elevate in termini di rischio di contagio da infezioni informatiche locali

	Paese*	% di utenti unici**
1	Vietnam	60,68%
2	Bangladesh	60,20%
3	Mongolia	57,28%
4	Yemen	55,91%
5	Somalia	55,64%
6	Nepal	55,01%
7	Afghanistan	54,91%
8	Algeria	54,83%
9	Iraq	54,38%
10	Cambogia	52,70%
11	Laos	52,54%
12	Armenia	52,44%
13	Pakistan	51,95%
14	Kazakhstan	51,54%
15	Ruanda	51,36%

16	Etiopia	50,93%
17	Egitto	50,60%
18	Siria	50,11%
19	India	50,00%
20	Tagikistan	49,80%

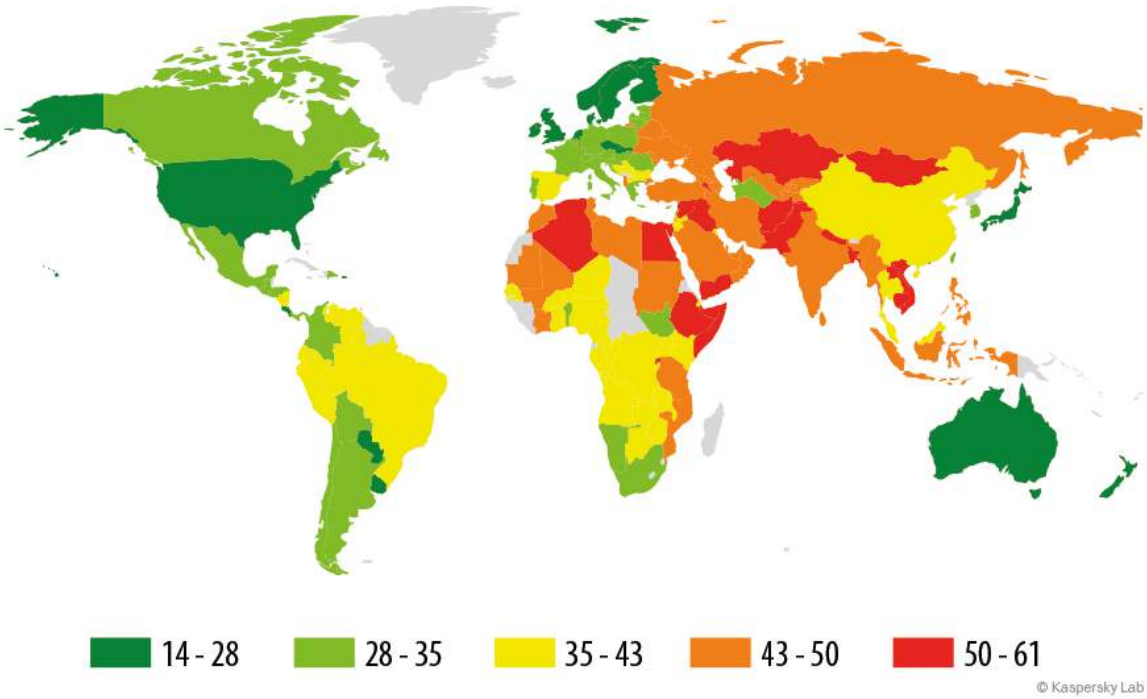
I dati statistici sopra indicati sono stati elaborati sulla base dei rilevamenti effettuati dai moduli anti-virus OAS (scanner on-access) e ODS (scanner on-demand). Le informazioni sono state ricevute tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare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

Da molto tempo, le prime venti posizioni della speciale TOP-20 qui sopra riportata erano interamente occupate da paesi ubicati nel continente africano, in Medio Oriente e nel Sud-Est asiatico. Nel trimestre qui esaminato, spicca invece la presenza, all'interno della classifica, di paesi situati in altre aree geografiche, come l'Armenia (12° posto), il Kazakhstan (14° posto) ed il Tagikistan (20° posto).

Evidenziamo, inoltre, come il Vietnam (60,68%) detenga la leadership della graduatoria ormai da quasi due anni, mentre Bangladesh (60,2%) e Mongolia (57,3%), per il terzo trimestre di fila, conservano le rispettive posizioni in classifica.

In Russia, durante il primo trimestre del 2015, sono state rilevate minacce IT di origine locale sul 49,6% dei computer degli utenti.



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 (14,7%), Danimarca (20,1%), Svezia (21,4%), Hong Kong (21,5%), Finlandia (21,6%).

In media, nel mondo, durante il primo trimestre del 2015, sono state rilevate minacce IT di origine locale - perlomeno una volta - sul 39,8% dei computer degli utenti; tale indice ha fatto pertanto registrare, rispetto al quarto trimestre dell'anno 2014, un aumento pari al 2%.