L’evoluzione delle minacce informatiche nel terzo trimestre del 2014

David Emm
Victor Chebyshev
Roman Unuchek
Maria Garnaeva
Denis Makrushin
Anton Ivanov

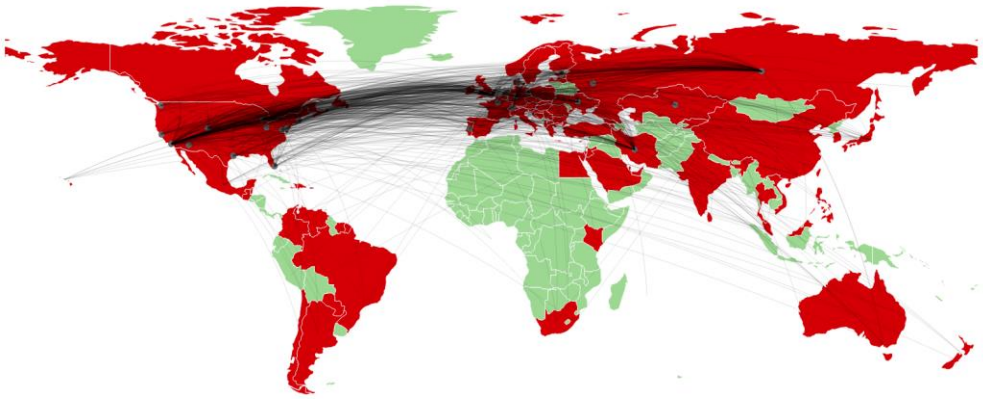
Il quadro della situazione

Attacchi mirati e campagne di malware

Sulle tracce dello Yeti

Nello scorso mese di luglio è stata da noi pubblicata un'approfondita analisi, eseguita dal Global Research and Analysis Team (GReAT) di Kaspersky Lab, riguardo a un'estesa campagna di attacchi informatici mirati, da noi soprannominata “Crouching Yeti” (tale appellativo può essere tradotto in italiano come "lo Yeti acquattato", pronto per balzare all'attacco). La campagna di cyber-spionaggio in questione è ugualmente conosciuta con il nome di “Energetic Bear” (l'espressione inglese significa, letteralmente, "orso energico, attivo"), poiché i ricercatori dell'azienda di cybersecurity CrowdStrike hanno lasciato intendere che i responsabili degli attacchi informatici condotti fossero geograficamente ubicati in Russia (riteniamo, da parte nostra, che non vi siano elementi o prove sufficienti per poter confermare, in un modo o nell'altro, quanto asserito da CrowdStrike a tal proposito).

La campagna Crouching Yeti, il cui inizio risale addirittura alla fine dell'anno 2010, ha sinora preso di mira i seguenti settori: industria/macchinari, manifatturiero, farmaceutico, costruzioni, istruzione e Information Technology (IT). Per il momento, il numero totale delle vittime accertate è di oltre 2.800 in tutto il mondo; tra di esse, i ricercatori di Kaspersky Lab hanno identificato ben 101 diverse organizzazioni, situate, principalmente, sul territorio di Stati Uniti, Spagna, Giappone, Germania, Francia, Italia, Turchia, Irlanda, Polonia e Cina.



L'attuale lista delle vittime sembra proprio indicare che criminali che si celano dietro le quinte della campagna Crouching Yeti stiano perseguendo chiari obiettivi strategici. Gli aggressori, tuttavia, hanno ugualmente dimostrato uno specifico interesse, peraltro non così ovvio, nei confronti di determinate istituzioni. Gli esperti di Kaspersky Lab ritengono che potrebbe trattarsi, in questo caso, di vittime collaterali, per cui potrebbe essere più opportuno considerare Crouching Yeti non alla stregua di una campagna che mira a specifiche aree di interesse, bensì come una campagna di cyberspionaggio dai contorni decisamente più ampi, la quale rivolge il proprio interesse a svariati settori.

Per infiltrarsi all'interno dei computer appartenenti alle vittime designate, i cybercriminali che si nascondono dietro a tali attacchi mirati si avvalgono di varie tipologie di malware (si tratta, nella fattispecie, di software e tool nocivi appositamente creati e sviluppati per infettare i sistemi informatici provvisti di sistema operativo Windows). Il preciso obiettivo della

campagna è quello di estendere progressivamente il proprio raggio d'azione all'interno delle organizzazioni ed istituzioni bersagliate, allo scopo di realizzare il furto di dati sensibili e confidenziali, incluso la proprietà intellettuale ed altre importanti informazioni di natura strategica. I computer compromessi dai suddetti software e strumenti nocivi si connettono poi ad una vasta rete di siti web violati, i quali ospitano vari moduli di malware aggiuntivi, custodiscono informazioni sulle vittime di Crouching Yeti e smistano comandi ai sistemi infetti.

Al fine di generare l'infezione informatica sui computer sottoposti ad attacco, gli aggressori fanno affidamento su tre diversi metodi. Essi ricorrono, in primo luogo, ad un installer di software del tutto legittimo, appositamente riprogettato per includere, allo stesso tempo, un file DLL dannoso. File archivio del genere, autoestraenti e debitamente modificati, possono essere, di fatto, caricati direttamente su un server compromesso, oppure, in alternativa, possono essere direttamente inviati, tramite e-mail, a qualcuno che opera ed agisce all'interno dell'organizzazione presa di mira. In secondo luogo, i criminali si avvalgono della pratica dello spear-phishing, allo scopo di recapitare nelle e-mail box delle potenziali vittime un file XDP (XML Data Package) maligno, contenente un exploit Flash (CVE-2011-0611). In terzo luogo, infine, gli aggressori utilizzano attacchi informatici di tipo "water-hole" (che significa letteralmente, in lingua inglese, “pozza d’acqua", o "abbeveratoio"). Nello specifico, il termine “watering-hole” viene applicato ad un sito web che, con buona probabilità, sarà in seguito visitato dalle potenziali vittime degli attacchi mirati durante la navigazione condotta da queste ultime in Rete. Si tratta di siti già violati in precedenza dai cybercriminali, mediante apposite iniezioni di codice nocivo, volte a generare l'installazione di malware sui computer di tutti coloro che visiteranno il sito compromesso. Nella fattispecie, i siti web sottoposti ad operazioni di hacking fanno uso di numerosi exploit (CVE-2013-2465, CVE-2013-1347 e CVE-2012-1723) per reindirizzare poi i visitatori verso file dannosi provvisti di estensione JAR o HTML, file ospitati a loro volta su altri siti Internet, gestiti direttamente dagli aggressori.

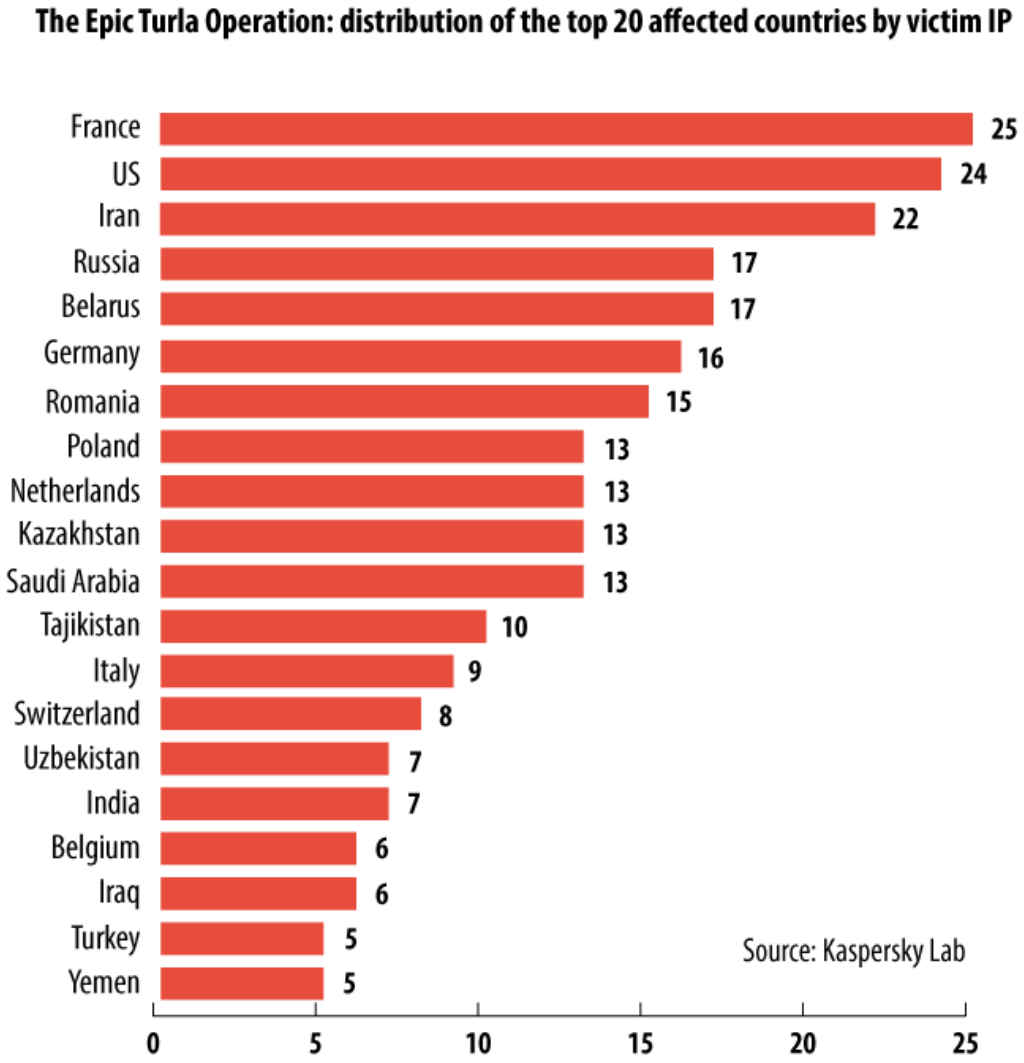
Un pericoloso software maligno utilizzato dagli aggressori che operano nell'ambito della campagna Crouching Yeti è il programma Trojan denominato Havex, il quale comprende speciali moduli aggiuntivi finalizzati alla raccolta di dati provenienti da specifici ambienti IT adibiti al controllo industriale. Il primo di essi è il modulo scanner OPC. Si tratta di un modulo nocivo progettato per raccogliere dati estremamente dettagliati relativamente ai server OPC in esecuzione sulla rete locale. I server OPC (Object Linking and Embedding (OLE) for Process Control) vengono di solito utilizzati negli ambienti in cui operano molteplici sistemi di automazione industriale. Il modulo in questione è accompagnato da uno strumento di scansione della rete. Il modulo esegue, pertanto, la scansione della rete locale, ricercando tutti i computer collegati alle porte relative al software OPC/SCADA (Supervisory Control and Data Acquisition) e provando a connettersi a tali host, per individuare quale potenziale sistema OPC/SCADA risulti al momento in esecuzione. Tutti i dati raccolti dal modulo sopra menzionato vengono poi trasmessi ai server di comando e controllo (C2) utilizzati dai criminali per gestire la campagna di cyberspionaggio qui esaminata.

Nell'analizzare il codice dannoso utilizzato per la conduzione della campagna di cyber-spionaggio, descritta nel presente capitolo del nostro consueto report trimestrale dedicato all'evoluzione delle minacce IT, gli esperti di Kaspersky Lab hanno ugualmente ricercato specifici indizi che avrebbero potuto, in un modo o nell'altro, svelare l'identità degli aggressori. In particolare, il GReAT team ha eseguito l’analisi della marcatura oraria di ben 154 file, concludendo che la maggior parte dei campioni erano stati compilati tra le 6:00 e le 16:00 UTC;

ciò potrebbe corrispondere, in pratica, a qualsiasi paese situato nell'Europa Occidentale, cosi come nell'Europa dell'Est. I nostri esperti hanno inoltre analizzato la lingua utilizzata dagli aggressori. Il malware contiene, di fatto, stringhe compilate in lingua inglese; risulta tuttavia ben evidente come gli autori delle stesse non possano essere in alcun modo di madrelingua inglese. Sono stati inoltre scovati determinati indizi che potrebbero far pensare ad una possibile provenienza francese o svedese. A differenza di numerosi altri ricercatori che si sono occupati di questa particolare campagna, gli specialisti di Kaspersky Lab non hanno potuto reperire nessun elemento che potesse in qualche modo consentire di concludere con certezza che il gruppo criminale di Crouching Yeti sia di origine russa. I quasi 200 codici binari dannosi e il relativo contenuto operativo non presentano, infatti, alcun elemento redatto in caratteri cirillici (o eventuali traslitterazioni), a differenza, invece, di quanto precedentemente osservato da Kaspersky Lab durante la ricerche condotte in merito a Red October (Ottobre Rosso), MiniDuke, CosmicDuke, Snake e TeamSpy.

Un «epico» racconto di cyber-spionaggio

Da oltre un anno gli esperti di Kaspersky Lab stanno conducendo approfondite indagini riguardo a una sofisticata e complessa campagna di cyber-spionaggio, denominata in codice “Epic Turla”. Tale campagna, avviata già nel corso dell'anno 2012, mira a colpire, in particolar modo, le istituzioni governative, le ambasciate, le organizzazioni operanti in campo militare, nell'ambito della ricerca e dell'istruzione, nonché le aziende farmaceutiche. La maggior parte delle vittime di Epic Turla risulta ubicata in Medio Oriente e in Europa, sebbene siano state da noi rilevate vittime anche in altre aree geografiche mondiali, incluso gli Stati Uniti. Complessivamente, i ricercatori di Kaspersky Lab hanno identificato diverse centinaia di indirizzi IP, dislocati in oltre 45 paesi, sottoposti agli attacchi IT lanciati nell'ambito di tale persistente operazione di spionaggio informatico.



Al momento in cui erano stati pubblicati i risultati della nostra ricerca iniziale riguardo alla campagna mirata in questione, non risultavano ancora chiare le modalità attraverso le quali le vittime dell'attacco venivano infettate dal malware dispiegato dagli aggressori. Nella nostra ultima indagine, pubblicata dal GReAT team nello scorso mese di agosto, sono stati invece delineati i meccanismi utilizzati nell'ambito di Epic Turla per generare la pericolosa infezione informatica sui computer via via sottoposti ad attacco; i nostri ricercatori hanno ugualmente descritto le modalità con cui tali meccanismi si inseriscono nella struttura complessiva di tale campagna.

Per infettare le potenziali vittime, i criminali ricorrono a specifici metodi di ingegneria sociale, e più precisamente ad attacchi di tipo watering-hole, così come ad insistite pratiche di spear-phishing.

Alcuni dei messaggi e-mail di spear-phishing distribuiti dagli aggressori includono exploit zero-day. Il primo di tali exploit, appositamente creato dai virus writer per colpire il programma Acrobat Reader di Adobe (CVE-2013-3346), permette agli aggressori di eseguire codice

arbitrario sul computer della vittima designata. Il secondo exploit, preposto a sfruttare una vulnerabilità individuata in Windows XP e Windows Server 2003 (CVE-2013-5065), falla di sicurezza che consente di scalare i privilegi, consegna in pratica alla backdoor di Epic Turla i diritti di amministratore sul computer della vittima. Inoltre, gli aggressori cercano di indurre le loro vittime ad eseguire specifici programmi di installazione del malware, provvisti di estensione SCR, talvolta compressi nel formato RAR. Così, nel momento in cui le ignare vittime provvedono ad aprire un file infetto, sul loro computer viene automaticamente installato un insidioso programma backdoor, il quale consente ai criminali di ottenere il pieno controllo del sistema informatico preso di mira.

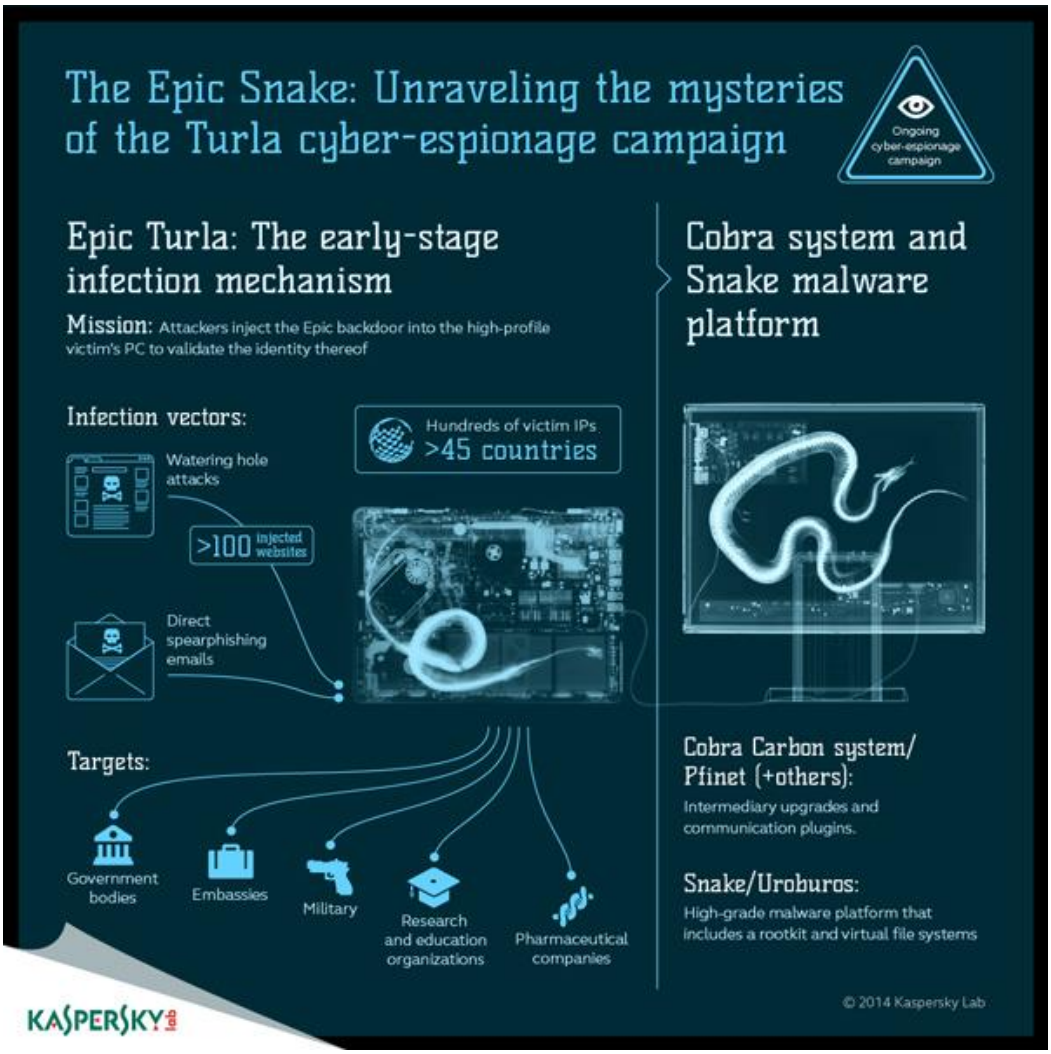
I cybercriminali che si celano dietro le quinte della vasta operazione di spionaggio Epic Turla fanno ugualmente ricorso agli attacchi di tipo watering-hole, nel corso dei quali vengono dispiegati vari exploit, e più precisamente un exploit destinato a colpire la piattaforma Java (CVE-2012-1723), exploit destinati al programma Flash di Adobe ed exploit diretti al browser Internet Explorer. Altri, poi, si avvalgono dell'ingegneria sociale per far sì che le loro vittime eseguano sul proprio computer programmi di installazione del malware camuffati sotto forma di installer di 'Flash Player'. A seconda dell'indirizzo IP della vittima, i criminali distribuiscono exploit specificamente destinati a Java o al browser, un software fasullo - provvisto comunque di firma - in veste di Adobe Flash Player, oppure una falsa versione di Microsoft Security Essentials. I ricercatori del team di Kaspersky Lab hanno complessivamente individuato oltre 100 siti Internet oggetto di "web injection" - mediante codice nocivo - da parte dei cybercriminali. Non costituisce ovviamente motivo di particolare sorpresa il fatto che la scelta dei siti web violati rifletta in pieno gli specifici interessi manifestati di cybercriminali (così come gli interessi delle vittime dell'estesa operazione di cyber-spionaggio). Ad esempio, numerosi siti Internet di lingua spagnola appartengono direttamente agli enti governativi locali.

Una volta che il computer è stato infettato, la backdoor Epic Turla (ugualmente conosciuta con gli appellativi di 'WorldCupSec', 'TadjMakhal', 'Wipbot' e 'Tadvig') provvede immediatamente a stabilire la connessione con il server di comando e controllo (C2), allo scopo di inviare un pacchetto di dati contenente varie informazioni relative al sistema informatico preso d'assalto. Sulla base delle informazioni riepilogative trasmesse al server C2, i criminali recapitano alle loro vittime determinati file di batch preconfigurati, i quali contengono una serie di comandi da eseguire, successivamente, sul computer infetto. I cybercriminali provvedono ugualmente all'operazione di upload, sul computer-vittima, di strumenti di supporto, ovvero tool personalizzati di "lateral movement" (incluso uno specifico keylogger ed un archiviatore RAR) - così come di utility standard, quali un tool Microsoft per le query DNS.

L'estesa ricerca condotta dal Global Research and Analysis Team di Kaspersky Lab ha permesso di rivelare come la backdoor Epic Turla rappresenti soltanto il primo stadio di un più vasto processo di infezione. In effetti, il malware in questione viene utilizzato dai criminali per distribuire un programma backdoor ancor più sofisticato, conosciuto come 'Cobra/Carbon system' (denominato 'Pfinet' da alcuni prodotti anti-malware). Dopo qualche tempo, i cybercriminali si sono quindi spinti decisamente oltre, utilizzando, di fatto, l'impianto Epic Turla per aggiornare il file di configurazione Carbon con un diverso set di server C2 di comando e controllo. Le peculiarità, davvero uniche, riscontrate nello specifico modo di operare tramite le due backdoor in causa indicano, in tutta evidenza, una connessione chiara e diretta tra queste ultime: una di esse viene di fatto utilizzata dagli aggressori per ottenere una sorta di solido punto d'appoggio e ottenere conferma del potenziale alto profilo della vittima. Qualora

venga comprovato che la vittima presa di mira risulta essere di effettivo interesse per i criminali, sul computer compromesso dal malware viene immediatamente eseguito l'upgrade all'intero sistema Carbon.

Cliccando sul link qui riportato si può accedere ad un'analisi completa dell'intera campagna di cyber-spionaggio denominata Epic Turla.



Attribuire un'origine ben precisa a tale genere di attacchi informatici risulta sempre particolarmente difficile e complesso. Ad ogni caso, alcuni specifici aspetti ed elementi del codice nocivo analizzato dagli esperti di Kaspersky Lab sembrano rivelarci qualcosa riguardo ai criminali in questione. E' chiaro, in primo luogo, che non si tratta di persone di madrelingua inglese. Gli aggressori, in effetti, commettono evidenti errori ortografici e grammaticali, relativamente a singole parole e frasi in inglese, quali:

'Password it's wrong!' (La password è errata)
'File is not exists' (Il file non esiste)
'File is exists for edit' (Il file esiste per le operazioni di editing)

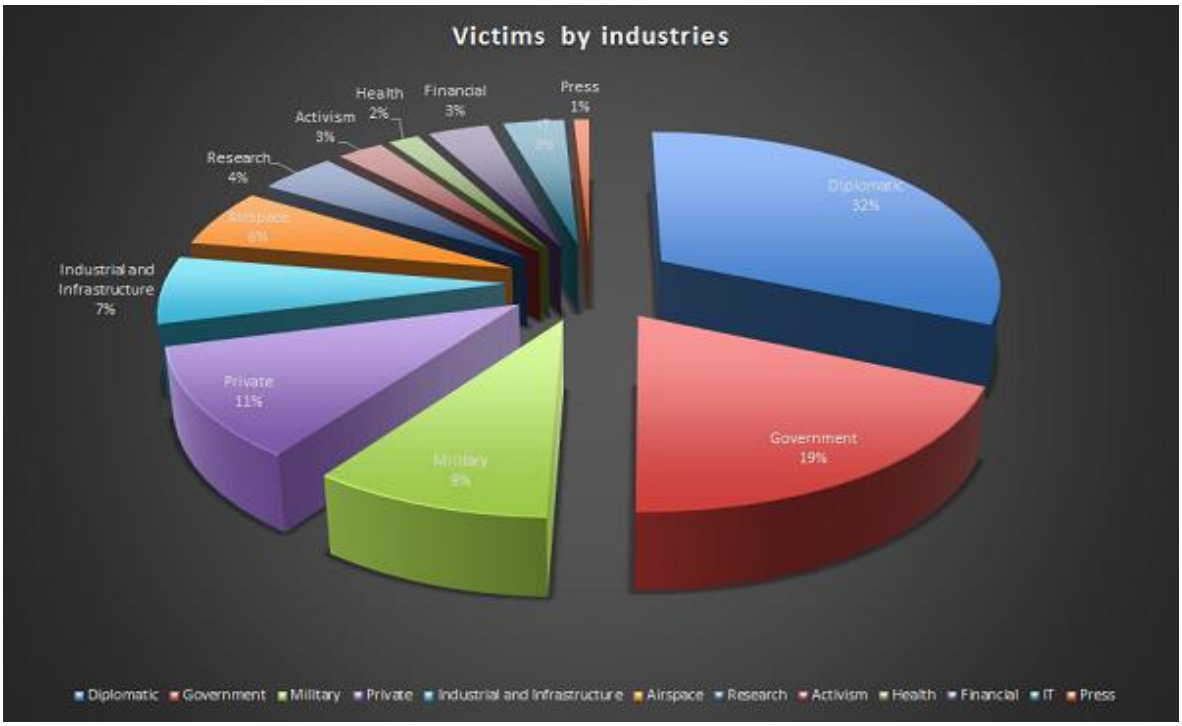
Sono stati ugualmente individuati ulteriori indizi e specifiche caratteristiche che sembrano suggerire l'effettiva provenienza dei cybercriminali. Alcune delle backdoor, ad esempio, sono state compilate tramite un particolare sistema in cui si fa uso della lingua russa. Oltre a ciò, il nome interno di una delle backdoor utilizzate nell'ambito della campagna Epic Turla risulta essere 'Zagruzchik.dll', che in russo significa "bootloader" o "programma di caricamento". E' stato infine rilevato come il pannello di controllo 'mother ship' di Epic Turla imposti il codice pagina su 1251, valore abitualmente utilizzato proprio per i caratteri cirillici.

NetTraveler cambia faccia in occasione del suo 10° «compleanno»

Abbiamo già riferito e discusso, in numerose occasioni, riguardo a questa persistente campagna di cyber-spionaggio, caratterizzata da attacchi informatici ben mirati e particolarmente sofisticati, i quali prevedono, tra l'altro, l'utilizzo di un potente toolkit di attacco; l'operazione NetTraveler si contraddistingue ugualmente per la sua marcata longevità, visto che risulta ormai attiva da oltre 10 anni.

Qualche mese fa è stato da noi osservato un significativo aumento del numero degli attacchi effettuati nei confronti di attivisti uiguri e tibetani, mediante l'utilizzo di una versione aggiornata della backdoor NetTraveler. Per adescare le proprie vittime, gli aggressori ricorrono, in primo luogo, alle famigerate e-mail di spear-phishing: nella fattispecie, tali messaggi di posta elettronica malevoli recano al destinatario un documento Microsoft Word contenente il pericoloso exploit CVE-2012-0158. In tal modo, viene riversato sul computer-vittima il modulo nocivo principale ('net.exe'), il quale, a sua volta, provvede ad installare vari altri file dannosi, tra cui il modulo C2 primario, relativo al server di comando e controllo. Quest'ultimo modulo viene registrato in qualità di servizio ('Windowsupdata'), mediante un apposito file di batch Windows, denominato 'dot.bat'. E' stato ugualmente sottoposto ad aggiornamento il formato del file di configurazione del malware in causa; risulta ben evidente come i criminali abbiano specificamente operato con il preciso intento di testare e cercare di occultare la configurazione applicata (il sistema crittografico da essi utilizzato appare tuttavia piuttosto debole).

Gli obiettivi che i criminali si prefiggono di colpire sono progressivamente mutati con il trascorrere degli anni. Come è noto, per gran parte dell'esistenza della minaccia APT qui descritta, sono state chiaramente le organizzazioni operanti in campo diplomatico, governativo e militare, a rappresentare i principali target dell'estesa campagna di cyber-spionaggio NetTraveler. Più di recente, le attività di spionaggio informatico condotte dagli aggressori si sono prevalentemente concentrate su organizzazioni attive nei seguenti settori: esplorazione spaziale, nanotecnologie, produzione di energia, settore nucleare, apparecchiature laser, medicina e telecomunicazioni.



Gli attacchi informatici nei confronti degli attivisti uiguri e tibetani continuano tuttavia a rimanere uno dei target principali delle attività svolte dai criminali nell'ambito della campagna di cyber-spionaggio NetTraveler.

Il castello di carte del malware siriano

La tecnologia è ormai parte integrante della nostra vita; non costituisce quindi motivo di particolare sorpresa il fatto che i conflitti presenti in varie aree del pianeta acquisiscano in misura sempre maggiore una vera e propria "cyber-dimensione". Tale definizione si rivela particolarmente calzante per la macro-area medio-orientale, zona del mondo in cui i conflitti geo-politici hanno purtroppo conosciuto un'ulteriore preoccupante escalation ed intensificazione nel corso di questi ultimi anni. Il Global Research and Analysis Team di Kaspersky Lab ha provveduto ad analizzare il recente aumento dell'attività del malware manifestatosi in Siria.

Le persone che si nascondono dietro tali attacchi informatici ricorrono a vari metodi e trucchi di ingegneria sociale per indurre le proprie potenziali vittime ad aprire i file infetti via via distribuiti. Nella fattispecie, per raggiungere tale preciso scopo, gli aggressori si avvalgono, di volta in volta, della posta elettronica, dei messaggi via Skype, dei post su Facebook e, persino, di appositi video collocati all'interno della celebre piattaforma di hosting YouTube.

Essi utilizzano un'ampia varietà di trappole e tranelli, contando in particolar modo sulla naturale fiducia riposta dalle proprie vittime nei confronti dei forum tenuti sui social network, sulla curiosità manifestata riguardo alle notizie relative al conflitto in Siria, così come

sull'eventuale paura nutrita nei confronti del governo locale, o nella mancanza di preparazione e specifiche conoscenze a livello tecnologico.

Tra gli esempi più eclatanti in tal senso, possiamo citare un inquietante video, appositamente collocato su YouTube, in cui vengono mostrate persone ferite nel corso dei recenti bombardamenti; video in cui, oltre alle immagini cruente, si invitano gli utenti a scaricare un particolare programma malware tramite un sito web di file-sharing, pubblicamente accessibile. I nostri analisti, nel corso dell'indagine effettuata, hanno ugualmente individuato una serie di file compressi situati all'interno di un popolare sito di social networking; tali file, una volta eseguito il relativo processo di estrazione, hanno rivelato un database contenente una lista di attivisti e persone ricercate in Siria. Il link per effettuare il download di tale applicazione database era stato inserito all'interno della sezione informazioni di un video pubblicato in data 9 novembre 2014. Per cercare di ingannare le loro vittime, i criminali in questione sono inoltre soliti fare uso di false soluzioni di sicurezza IT - incluso un programma anti-virus fasullo denominato “Ammazon Internet Security” ed una versione "trojanizzata" di un tool di monitoraggio rete in origine del tutto legittimo. Gli aggressori non si limitano a diffondere esclusivamente applicazioni di sicurezza fasulle; abbiamo in effetti rilevato la presenza di false versioni delle note applicazioni di messaggistica istantanea Whatsapp e Viber.

I cybercriminali si avvalgono, inoltre, di tutta una serie di ben noti strumenti per ottenere l'accesso remoto (RATs, Remote Access Tools), programmi malevoli che consentono ad un operatore remoto di poter agevolmente controllare un computer compromesso dal malware, come se tale operatore avesse fisicamente accesso alla macchina violata. Si tratta di strumenti ampiamente utilizzati nella conduzione degli attacchi cybercriminali, di tool impiegati persino in alcuni attacchi informatici sponsorizzati a livello di stati nazionali. Tra i RATs utilizzati dagli aggressori nel corso di tale campagna spiccano “ShadowTech”, “Xtreme”, “NjRAT”, “Bitcoment”, “Dark Comet” e “Blackshades”. Il malware dispiegato dai criminali ha la funzione di monitorare l'attività delle vittime, raccogliere informazioni su queste ultime; in alcuni casi, tramite esso, si cerca di porre fine alle operazioni eventualmente condotte dai profili presi di mira.

Le vittime di tali attacchi non risultano ubicate esclusivamente in territorio siriano. In effetti, gli attacchi informatici qui sopra descritti sono stati ugualmente riscontrati in Turchia, Arabia Saudita, Libano, Palestina, Emirati Arabi Uniti, Israele, Marocco, Francia e Stati Uniti.

Siamo stati inoltre in grado di ricondurre i server C2 di comando e controllo utilizzati dagli aggressori a specifici indirizzi IP situati in Siria, Russia, Libano, Stati Uniti e Brasile. Abbiamo complessivamente individuato 110 file, 20 domini e 47 indirizzi IP associati a tali attacchi.

Il numero degli attacchi informatici ascrivibili al malware siriano è notevolmente cresciuto proprio nel corso di questo ultimo anno. E' inoltre evidente come i gruppi coinvolti negli attacchi in questione siano, di fatto, bene organizzati. Sino ad ora i criminali si sono avvalsi di strumenti malware già sviluppati e disponibili sul mercato, anziché crearne di propri (sebbene essi facciano uso di numerosi metodi di offuscamento, nel tentativo di eludere i rilevamenti basati sulle semplici firme del malware). Riteniamo tuttavia, a ragion veduta, che sia il numero, sia il livello di complessità e sofisticatezza dei programmi malware dispiegati in tale regione dello scacchiere mediorientale, siano con ogni probabilità destinati ad accrescersi.

Il report completo stilato dagli esperti di Kaspersky Lab in merito al malware qui sopra esaminato può essere consultato a questo link.

Le «storie» di sicurezza IT più significative del trimestre

Shylock – una libbra della *tua* carne

Alcuni mesi fa, Kaspersky Lab ha fatto parte di una speciale task force composta da forze dell'ordine ed imprese, coordinata dalla National Crime Agency (NCA) del Regno Unito, volta a smantellare le infrastrutture cybercriminali sulle quali poggiava il famigerato Trojan Shylock. Tale partnership ha chiaramente dimostrato come la cooperazione globale, a livello di lotta nei confronti del cybercrimine, possa produrre risultati decisamente positivi.

Il Trojan bancario Shylock - che deve il nome ai brani tratti da *Il Mercante di Venezia* di Shakespeare contenuti all'interno del proprio codice - è stato scoperto già nell'anno 2011. Al pari di altri noti Trojan-banker, quali Zeus, SpyEye e Carberp, Shylock provvede a lanciare un attacco del tipo "man-in-the-browser", attacco informatico appositamente progettato per realizzare il furto sui computer dei clienti degli istituti bancari delle credenziali di login utilizzate nel corso delle operazioni di banking online. Il Trojan in questione si avvale di un elenco preconfigurato di banche target, situate in vari paesi del pianeta.

In sostanza, Shylock inietta campi fasulli, preposti all'inserimento dei dati sensibili dell'utente, all'interno delle pagine web, quando le stesse vengono caricate sul browser della vittima. Nella maggior parte dei casi, le vittime vengono infettate attraverso link nocivi che, una volta cliccati, generano il download e l'esecuzione del malware, all'insaputa dell'utente. Il Trojan Shylock, a questo punto, tenta di accedere al denaro custodito sui conti bancari aziendali o personali violati, per poi trasferire le somme illecitamente carpite verso i sistemi di controllo allestiti dai cybercriminali.

Gli obiettivi presi di mira dai criminali informatici sono cambiati nel corso del tempo. Quando Shylock ha fatto la sua prima apparizione sulla scena del malware bancario, il Trojan qui analizzato bersagliava soprattutto gli utenti situati entro i confini del Regno Unito; nel corso dell'anno 2012, tuttavia, il suo raggio di azione si è esteso sia ad altri paesi europei, sia agli Stati Uniti. Entro la fine del 2013, poi, i cybercriminali si sono interessati in misura maggiore allo sviluppo di nuovi mercati, quali Brasile, Russia e Vietnam. Ulteriori informazioni sul Trojan Shylock, incluso i dati relativi alla diffusione geografica degli attacchi informatici condotti mediante tale malware, sono disponibili al presente link.

Tutti i Trojan bancari - e il malware Shylock non fa certo eccezione in tal senso - prendono di mira i clienti delle banche, cercando di approfittare al massimo di quello che può essere spesso ritenuto l'elemento meno protetto nel processo di esecuzione di qualsiasi transazione finanziaria, vale a dire l'essere umano. E' questo il preciso motivo per cui si rivela di estrema importanza, per ogni utente, far sì che la propria sicurezza IT abbia inizio già in casa propria;

tutti noi, senza distinzione, abbiamo bisogno di proteggere efficacemente i nostri computer nei confronti dei malware attualmente in circolazione, sempre più temibili ed insidiosi.

O la borsa o... i tuoi file!

Il numero dei cosiddetti programmi "estorsori", o ransomware, presenti sulla scena del cybercrimine, è progressivamente cresciuto nel corso di questi ultimi anni; non tutti i programmi ransomware, poi, prendono di mira esclusivamente i computer provvisti di sistema operativo Windows. Alcuni di essi, incluso quelli specificamente destinati ai dispositivi Android, tendono semplicemente a bloccare l'accesso al dispositivo da parte dell'utente-vittima, per poi richiedere a quest'ultimo il pagamento di un vero e proprio riscatto, per poter procedere allo sblocco del dispositivo sottoposto ad attacco informatico.

Molti programmi ransomware, tuttavia, si spingono decisamente oltre, arrivando addirittura a criptare i dati custoditi sul computer della vittima. Un recente esempio di tale tipologia di malware è rappresentato dal ransomware denominato ZeroLocker.

A differenza della maggior parte dei programmi estorsori, in grado di criptare solo un elenco predefinito di tipi di file, ZeroLocker provvede invece a cifrare quasi tutti i file che si trovano sul computer-vittima, aggiungendo poi l'estensione ".encrypt" ai file da esso codificati. E' di particolare interesse osservare come il ransomware ZeroLocker non effettui il criptaggio dei file custoditi nelle directory contenenti i termini "Windows", "WINDOWS", "Program Files", "ZeroLocker" o "Destroy" e, al tempo stesso, non codifichi file aventi dimensioni superiori ai 20MB.

Al fine di cifrare tutti i file, ZeroLocker genera una chiave AES a 160 bit. Lo spazio della chiave è, di fatto, piuttosto limitato, a causa del modo stesso con cui quest'ultima viene generata, ma risulta tuttavia sufficientemente esteso per rendere in pratica infattibile qualsiasi operazione generale di brute–forcing. Una volta crittografati i file, il malware in questione provvede a lanciare l'esecuzione dell'utility 'cipher.exe', allo scopo di rimuovere dal drive tutti i dati inutilizzati, rendendo in tal modo molto più complesso e difficile l'eventuale ripristino dei file stessi. La chiave di crittografia, unitamente ad un CRC32 dell'indirizzo MAC del computer sottoposto ad attacco, ed al wallet Bitcoin associato (il "portafoglio" virtuale nel quale viene custodita, sul computer dell'utente, la nota criptovaluta), viene poi trasmessa al server maligno utilizzato dai cybercriminali. Desideriamo sottolineare come siano stati raccolti specifici indizi che dimostrano in maniera inequivocabile come la configurazione del server di comando e controllo (C2) allestito dai malintenzionati contenga alcuni errori, i quali potrebbero poi impedire il buon esito della successiva operazione di decodifica dei dati criptati; si tratta, indubbiamente, di un'ulteriore buona ragione per sostenere, con ancora maggior forza, che provvedere al pagamento del riscatto richiesto dai cybercriminali non è di sicuro una buona idea.

La chiave di crittografia, al pari delle altre informazioni, viene trasmessa attraverso una richiesta GET, anziché POST. Tale peculiarità si traduce, tuttavia, in un errore 404 sul server. Ciò potrebbe significare che il server non provvede a custodire le informazioni, suggerendo

quindi che, probabilmente, le vittime del ransomware ZeroLocker non otterranno mai la restituzione ed il ripristino dei loro file, anche nel caso in cui esse paghino il riscatto.

E' stato inoltre osservato come numerosi altri URL, ai quali il malware tenta di accedere, producano ugualmente un errore 404. Questa specifica circostanza sembra suggerire che l'operazione ZeroLocker possa ancora trovarsi nella sua fase iniziale. Se e quando tali errori verranno risolti, potremmo di fatto assistere ad un dispiegamento di tale ransomware su una scala decisamente più ampia.

Per decriptare i file precedentemente cifrati, i cybercriminali che agiscono dietro al malware ZeroLocker richiedono una cifra iniziale corrispondente a 300 dollari USA, in Bitcoin. Se la vittima non provvede in maniera tempestiva al pagamento, il costo sale prima a 500 dollari, poi a 1.000 dollari, man mano che il tempo passa.

All'interno del file binario si trova un wallet Bitcoin "hard-coded"; il malware, tuttavia, cerca ad ogni modo di recuperare un nuovo indirizzo del wallet dal server C2, probabilmente allo scopo di rendere più difficile e complessa la tracciatura dell'operazione, affinché non si possa poi determinare agevolmente se quest'ultima è andata in porto e, in particolar modo, non si venga in seguito a conoscere il "luogo" di destinazione della somma di denaro illecitamente sottratta. Nessuno degli indirizzi di wallet Bitcoin analizzati dai nostri esperti presentava transazioni ad esso associate. Dal momento che il server C2 di comando e controllo fornisce informazioni riguardo al portafoglio Bitcoin, si prospetta l'ipotesi che i criminali utilizzino un wallet unico per ogni vittima da essi presa di mira.

Un altro programma ransomware da noi recentemente analizzato è Onion. Tale software nocivo utilizza il medesimo metodo, ormai ampiamente collaudato, di cui si avvalgono ulteriori ransomware comparsi piuttosto di recente sulla scena del cybercrimine; tale metodo consiste, come abbiamo visto in precedenza, nel criptare innanzitutto i dati della vittima, per poi richiedere il pagamento di un cospicuo riscatto in Bitcoin, la nota criptovaluta.

Onion, tuttavia, presenta ugualmente interessanti aspetti innovativi, rispetto ai propri simili. Per occultare i propri server C2, esso fa uso, in primo luogo, della rete anonima TOR (The Onion Router). Ciò rende indubbiamente più difficile poter tracciare l'attività cybercriminale che si cela dietro al malware in questione ed assumere, di conseguenza, il controllo dei server dannosi. In passato, la rete TOR è stata utilizzata da altri programmi malware; tale Trojan, tuttavia, rappresenta un caso a parte, in quanto esso è in grado di supportare una piena interazione con TOR, senza peraltro ricevere alcun input da parte dell'utente-vittima. Altri programmi riconducibili a tale specifica tipologia sono soliti comunicare con la rete anonima TOR lanciando l'esecuzione (talvolta iniettando codice all'interno di altri processi) del file legittimo "tor.exe". Onion, al contrario, implementa questo genere di comunicazione come parte integrante dello stesso codice del malware.

Il Trojan Onion utilizza ugualmente un algoritmo crittografico non ortodosso, il quale rende impossibile l'operazione di decodifica dei file criptati, anche nel caso in cui venga intercettato il traffico che abitualmente intercorre tra il Trojan ed il server nocivo C2. Onion si avvale non soltanto della crittografia asimmetrica; esso utilizza ugualmente uno speciale protocollo crittografico conosciuto come ECDH (Elliptic Curve Diffie-Hellman). Ciò rende impossibile il processo di decodifica, senza l'utilizzo della "master key privata", la quale, peraltro, non abbandona mai il server controllato dai cybercriminali. Ulteriori dettagli in merito possono essere reperiti nel nostro report dedicato al Trojan Onion.

Tutti gli elementi sopra descritti, combinati tra loro, rendono il Trojan Onion particolarmente avanzato dal punto di vista tecnologico, nonché estremamente pericoloso.

Le operazioni cybercriminali che prevedono il dispiegamento di temibili programmi ransomware si basano proprio sull'auspicato pagamento del riscatto da parte degli utenti-vittima. Non fatelo assolutamente! Eseguite, piuttosto, dei backup regolari dei vostri dati. In questo caso, se mai doveste cadere vittima di un programma ransomware, o doveste magari incontrare un problema hardware che vi impedisce di accedere ai vostri file, non perderete nessuno dei vostri dati.

Ecco perché uno dei nostri ricercatori nel campo della sicurezza IT ha hackerato la propria abitazione

Possiamo senza ombra di dubbio affermare che Internet, al giorno d'oggi, si stia letteralmente intrecciando, sempre di più, con il tessuto delle nostre vite; in numerosi casi, in effetti, la connettività risulta ormai essere un elemento fondante degli oggetti di uso quotidiano. Tale specifica tendenza, conosciuta con l'appellativo di “Internet delle cose” (IoT, acronimo dell'espressione inglese “Internet of Things”) sta attirando in misura sempre maggiore le attenzioni - ovviamente contrapposte - di hacker e ricercatori, impegnati nel sondare e testare le sofisticate tecnologie attualmente integrate nelle autovetture, nei sistemi alberghieri, nei sistemi di allarme domestici ed altro ancora - con il preciso obiettivo di individuare la presenza di eventuali vulnerabilità critiche.

L'Internet delle cose, talvolta, può apparire come qualcosa di remoto e poco tangibile. In realtà, l'IoT è spesso molto più vicino a noi di quanto possiamo immaginare. Le abitazioni moderne, in effetti, sono di frequente corredate da tutta una serie di dispositivi connessi alla rete locale, senza che si tratti, necessariamente, dei tradizionali computer, tablet o telefoni cellulari; parliamo, nella fattispecie, di dispositivi quali smart TV, stampanti, console di gioco, dispositivi di archiviazione in rete o di alcuni tipi di media player/ricevitore satellitare.

Uno dei nostri ricercatori operanti nel campo della sicurezza IT, David Jacoby, ha condotto un’indagine nella propria abitazione, al fine di stabilire se quest'ultima fosse realmente "cyber-sicura". Egli ha esaminato vari elementi tecnologici, incluso i dispositivi NAS (Network Attached Storage), smart TV, router e ricevitore satellitare, per vedere se gli stessi risultassero vulnerabili ad eventuali attacchi. I risultati dell'indagine condotta sono stati a dir poco sorprendenti. Difatti, David ha individuato ben 14 vulnerabilità sui dispositivi "network-attached storage" (memorie connesse alla rete), una a livello di smart TV, così come numerose potenziali funzioni di controllo remoto nascoste nel router.

Le vulnerabilità più gravi sono state rilevate a livello di dispositivi NAS. Molte di esse, in effetti, avrebbero potuto agevolmente consentire ad un malintenzionato di eseguire in modalità remota vari comandi di sistema, peraltro ottenendo il massimo dei privilegi di amministratore. E' inoltre emerso come i dispositivi sottoposti a test fossero provvisti di password di default alquanto deboli, password memorizzate in formato testo, e come i file di configurazione inclusi presentassero permessi errati. Per uno dei dispositivi analizzati, poi, la password di amministratore di default risultava addirittura composta da una sola cifra! Ed ancora: è

persino risultato che un altro dei dispositivi presenti nell'abitazione del nostro ricercatore condivideva l'intero file di configurazione, contenente le password criptate, con tutti gli altri utenti della rete!

Utilizzando una vulnerabilità isolata, David è stato ugualmente in grado di eseguire l'upload di un file in una particolare area della storage memory (memoria di archiviazione), di fatto inaccessibile per l'utente ordinario. Quindi, se un malintenzionato riuscisse a caricare un file maligno all'interno di tale area, il dispositivo violato dal malware diverrebbe una pericolosa fonte di infezione per altri dispositivi connessi a tale NAS - un PC domestico, ad esempio - e potrebbe addirittura esercitare la funzione di bot DDoS (Distributed Denial of Service) nell'ambito di una botnet. Per di più, visto che la vulnerabilità sopra descritta permetteva di effettuare l'upload del file in un'area speciale del file system del dispositivo, l'unico modo per eliminare tale file sarebbe stato quello di utilizzare la vulnerabilità stessa, rilevata in precedenza. Ovviamente, non si tratta di un compito semplice, persino per un tecnico specializzato, figurarsi per l'utente medio di un dispositivo per l'intrattenimento domestico.

Esaminando poi il livello di sicurezza della sua smart TV, David ha scoperto che, a livello di comunicazione tra la propria TV ed i server del produttore dell'apparecchio televisivo stesso, non veniva di fatto utilizzata alcuna tipologia di criptaggio. Tale specifica circostanza avrebbe quindi potuto aprire, potenzialmente, la strada ad insidiosi attacchi del tipo "Man-in-the-Middle", i quali, nel momento in cui l'utente avesse cercato di acquistare contenuti tramite la propria TV, avrebbero in realtà potuto trasferire denaro ai cybercriminali, in maniera per nulla sospetta. A dimostrazione di tutto ciò, il nostro ricercatore è riuscito a sostituire con un'immagine una delle icone presenti nell'interfaccia grafica della propria smart TV. Normalmente, i widget e i thumbnail vengono scaricati dai server del vendor; tuttavia, in assenza di una specifica connessione criptata, tali informazioni possono essere agevolmente modificate da una terza parte. David Jacoby, nel corso della sua ricerca sperimentale, ha inoltre scoperto che la smart TV è in grado di eseguire codici scritti in Java, che, assieme alla capacità di intercettare lo scambio di traffico tra la TV ed Internet, potrebbero causare attacchi maligni condotti mediante l'utilizzo di exploit.

Da parte sua, il router DSL utilizzato da tutti gli altri dispositivi domestici per ottenere l'accesso wireless ad Internet, conteneva numerose funzionalità pericolose, nascoste al suo possessore. Alcune di tali funzioni potrebbero potenzialmente fornire ad un aggressore l'accesso remoto a qualsiasi dispositivo connesso ad una rete privata. L'aspetto indubbiamente più importante è che, secondo i risultati ottenuti dal ricercatore di Kaspersky Lab, alcune sezioni dell'interfaccia web del router, denominate "Web Cameras", "Telephony Expert Configure", "Access Control", "WAN-Sensing" e "Update" risultano invisibili e non possono essere in alcun modo modificate dal proprietario del dispositivo. L'accesso ad esse può essere ottenuto solo sfruttando una vulnerabilità piuttosto comune, la quale permette di spostarsi tra le sezioni dell'interfaccia (si tratta, fondamentalmente, di pagine web, ciascuna con il proprio indirizzo alfanumerico) forzando brutalmente i numeri presenti nella parte finale dell'indirizzo. Originariamente, tali funzionalità sono state implementate per cercare di agevolare il possessore del dispositivo: la funzione di accesso da remoto rende in effetti semplice e veloce, per un ISP (Internet Service Provider), poter risolvere eventuali problemi tecnici che si dovessero manifestare sul dispositivo stesso; l'apparente situazione di comodità potrebbe tuttavia trasformarsi in un evidente rischio per la sicurezza, qualora i comandi ed i controlli cadessero nelle mani sbagliate.

In linea con la propria policy aziendale, Kaspersky Lab non ha diffuso i nomi dei vendor dei prodotti presi in esame nel corso dell'indagine condotta dal nostro ricercatore. Tutti i produttori dei dispositivi oggetto della ricerca sperimentale eseguita da David Jacoby nella propria abitazione, sono stati ad ogni caso debitamente informati riguardo all'esistenza delle suddette vulnerabilità; gli specialisti di Kaspersky Lab stanno inoltre operando a stretto contatto con i vendor in questione per aiutare gli stessi a porre rimedio ad ognuna delle vulnerabilità scoperte.

E' davvero di fondamentale importanza che tutti quanti, sia gli utenti privati che gli utenti corporate, comprendano i potenziali rischi di sicurezza associati all'utilizzo dei dispositivi in rete. Dobbiamo anche tenere bene a mente il fatto che le nostre informazioni non sono al sicuro solo perché utilizziamo password solide, oppure ci avvaliamo di software specifici in grado di fornire un'adeguata protezione nei confronti dei codici maligni. Vi sono in effetti molti fattori ed elementi sui quali non possiamo esercitare alcun controllo diretto; riguardo a ciò siamo, in una certa misura, nelle mani dei produttori di software e hardware. Non tutti i dispositivi includono, ad esempio, controlli automatici degli eventuali aggiornamenti disponibili, rilasciati dal produttore; accade, talvolta, che ai consumatori venga richiesto di provvedere direttamente al download e all'installazione di un nuovo firmware. Questo, come è noto, non è sempre un compito agevole. Peggio ancora: non risulta sempre possibile procedere all'aggiornamento di un dispositivo; è in effetti emerso come l'abituale supporto - in termini di update rilasciati dal vendor - per la maggior parte dei dispositivi analizzati nel corso della ricerca qui descritta, fosse stato interrotto già da più di un anno.

Alcuni utili consigli, su come ridurre il rischio del prodursi di temibili attacchi informatici, si trovano in questo compendio dell'articolo di David Jacoby.

Sicurezza web e fughe di dati: ShellShock

Nello scorso mese di settembre, il mondo della sicurezza IT si è trovato a dover fronteggiare un vero e proprio allarme rosso, a seguito della scoperta della vulnerabilità 'Bash' (ugualmente conosciuta come 'ShellShock'). Bash (acronimo di 'Bourne again shell', dal nome del suo autore originario, Stephen Bourne), una shell Unix sviluppata da GNU Project nel lontano 1989, è, in sostanza, la shell di default nell'ambito dei sistemi operativi Linux e Mac OS X. Si tratta, in pratica, di un linguaggio di script utilizzato per inviare e interpretare dei comandi. La relativa falla di sicurezza (CVE-2014-6271), o bug che dir si voglia, consente all'ipotetico hacker di collegare un file maligno ad una variabile che viene eseguita quando viene utilizzato l'interprete di comandi Bash. In altre parole, dopo aver confezionato un exploit di successo, un criminale potrebbe ottenere il controllo completo dei sistemi interessati. L'alto impatto di tale vulnerabilità, unitamente alla facilità con cui Bash può essere sfruttata, la rende estremamente potente. Alcuni esperti di sicurezza IT hanno addirittura paragonato il bug in questione alla famigerata vulnerabilità 'Heartbleed'. Tuttavia, Bash risulta molto più facile da sfruttare rispetto ad Heartbleed e, mentre quest'ultimo consente al cybercriminale di realizzare esclusivamente il furto dei dati custoditi nella memoria del computer vulnerabile, Shellshock può fornire, al malintenzionato, il controllo completo del sistema sottoposto ad attacco informatico.

Non è trascorso molto tempo prima che qualche aggressore cercasse di sfruttare per i propri fini la vulnerabilità sopra descritta; peraltro, i primi esempi di utilizzo di tale bug sono stati da noi esaminati poco dopo la scoperta stessa di Shellshock. Nella maggior parte dei casi i cybercriminali hanno provveduto ad attaccare da remoto dei server web adibiti all'hosting di script CGI (Common Gateway Interface) compilati in linguaggio Bash, o preposti a passare valori agli script di shell. La suddetta vulnerabilità, tuttavia, potrebbe indirettamente costituire una minaccia anche per un'infrastruttura basata sull'OS Windows.

Allo stesso modo, il problema non risulta confinato esclusivamente ai server web. In effetti, Bash viene largamente utilizzata nel firmware di alcuni dei dispositivi la cui sicurezza, nella nostra vita di tutti i giorni, viene ormai data per scontata. Si tratta, nella fattispecie, di router, elettrodomestici e punti di accesso wireless. Per alcuni di tali dispositivi può essere difficile, o addirittura impossibile, reperire l'indispensabile patch di aggiornamento, come abbiamo sottolineato in precedenza.

Cliccando sul presente link troverete precise istruzioni riguardo alle modalità di aggiornamento previste per i sistemi potenzialmente vulnerabili.

Le statistiche del terzo trimestre 2014

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 dai cybercriminali prendono parte milioni di utenti dei prodotti Kaspersky Lab, ubicati in 213 diversi paesi e territori del pianeta.

Il trimestre in cifre

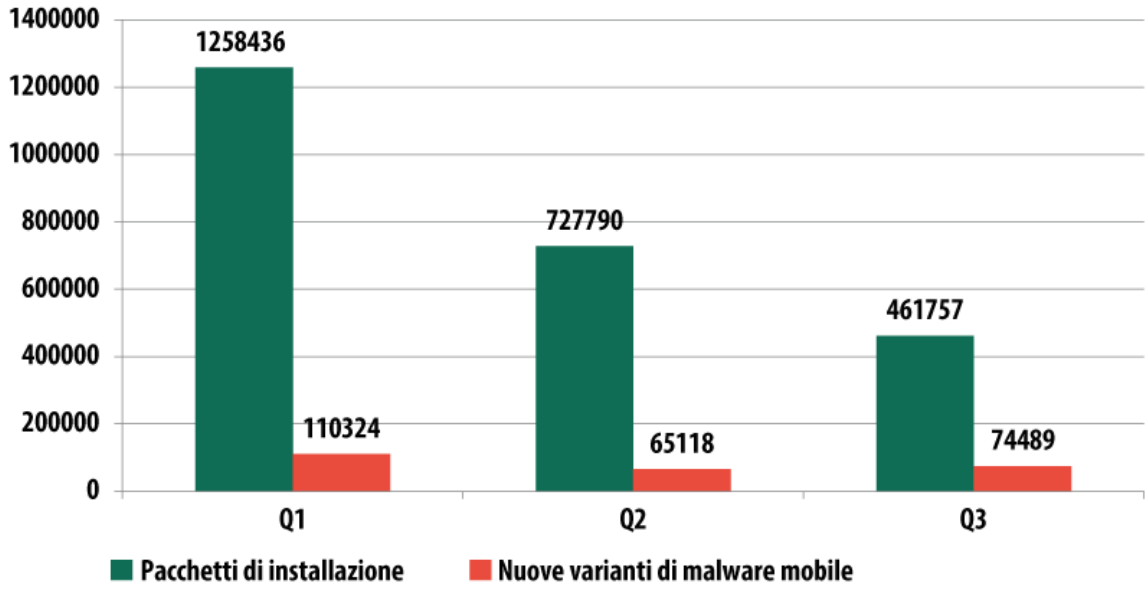
- Secondo i dati raccolti tramite il Kaspersky Security Network (KSN) - l'estesa rete globale di sicurezza da noi implementata attraverso specifiche infrastrutture "in-the-cloud" - lungo tutto l'arco del terzo trimestre del 2014 i prodotti Kaspersky Lab hanno rilevato e neutralizzato 1.325.106.041 attacchi dannosi rivolti ai computer e ai dispositivi mobile degli utenti.
- Le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 367.431.148 attacchi condotti attraverso siti Internet compromessi, dislocati in vari paesi.
- Il nostro Anti-Virus Web ha effettuato il rilevamento di 26.641.747 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, 107.215.793 URL unici.
- Un terzo (33%) 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 degli Stati Uniti.

- Il nostro modulo Anti-Virus File ha rilevato con successo 116.710.804 oggetti maligni 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:
    - **461.757** pacchetti di installazione;
    - **74.489** nuove varianti di programmi dannosi specificamente creati dai virus writer per infettare i dispositivi mobile;
    - **7.010** Trojan bancari per piattaforme mobile.

Le minacce IT per dispositivi mobile

Nel terzo trimestre del 2014 i prodotti Kaspersky Lab adibiti alla protezione IT dei dispositivi mobile hanno rilevato **74.489** nuove varianti di malware mobile - ovvero il 14,4% in più rispetto all'analogo valore riscontrato riguardo al trimestre precedente.

Al contempo, risulta diminuito il numero complessivo dei pacchetti di installazione nocivi individuati nel corso del periodo oggetto della nostra analisi.



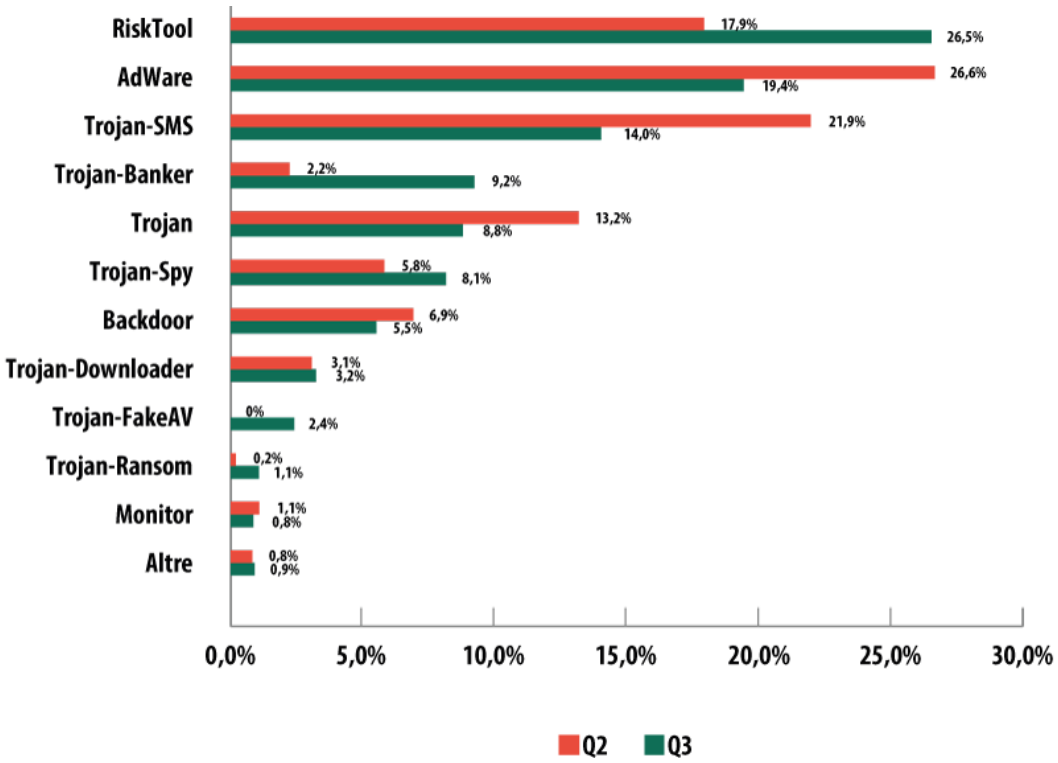
Numero complessivo di pacchetti di installazione maligni e di nuove varianti di malware mobile individuati nel periodo 1° trimestre - 3° trimestre 2014

Mentre nel primo semestre del 2014, per ogni programma malware destinato a colpire i dispositivi mobile si contavano, in media, oltre 11 pacchetti di installazione dannosi, nel terzo trimestre tale proporzione si è quasi dimezzata, scendendo a 6,2 pacchetti nocivi.

L'utilizzo di un elevato numero di pacchetti di installazione per ogni singolo malware mobile rappresenta una connotazione tipica del processo di distribuzione e diffusione dei famigerati Trojan-SMS. Basti pensare che, per una sola versione del malware denominato Stealer.a, i cybercriminali possono arrivare ad utilizzare sino a 70.000 diversi pacchetti. Probabilmente, il sensibile decremento del numero dei

pacchetti di installazione dannosi è legato al fatto che, in seno ai flussi delle nuove varianti di malware mobile, risulta notevolmente diminuita la quota ascrivibile ai suddetti programmi malevoli (vedi sotto).

Ripartizione del malware mobile per tipologie



Suddivisione delle varianti di malware mobile in base ai loro specifici comportamenti dannosi - Secondo e terzo trimestre del 2014 a confronto

La graduatoria del terzo trimestre del 2014 riservata alla ripartizione degli oggetti maligni per dispositivi mobile in base agli specifici comportamenti nocivi da essi evidenziati, risulta capeggiata dai Risktool, la cui quota, rispetto al trimestre precedente, ha fatto registrare un aumento di 8,6 punti percentuali, attestandosi, in tal modo, su un valore pari al 26,5%. 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.

Il secondo gradino del podio virtuale risulta occupato dagli AdWare, ovvero le fastidiose applicazioni pubblicitarie potenzialmente indesiderate (19,4%). Osserviamo, tuttavia, come l'indice relativo a tali programmi abbia manifestato una flessione del 7,9% rispetto all'analogo valore riscontrato nel secondo trimestre dell'anno in corso.

I Trojan-SMS, da parte loro, sono andati a collocarsi al terzo posto del rating, passando, nell'arco di un trimestre, dalla seconda alla terza posizione della graduatoria qui sopra riportata. La quota percentuale ad essi ascrivibile risulta in effetti sensibilmente diminuita rispetto al trimestre precedente (- 7,2%).

Sottolineiamo, ad ogni caso, come nel terzo trimestre del 2014, nel già vasto panorama delle nuove minacce IT per dispositivi mobile, alla marcata diminuzione degli indici percentuali attribuibili agli AdWare ed ai Trojan-SMS, faccia da contraltare un pronunciato aumento della quota relativa ai Trojan bancari mobile, repentinamente passata dal 2,2% al 9,2%, e quindi più che quadruplicata rispetto al trimestre precedente. Tale categoria di malware si è in tal modo insediata al quarto posto del ranking qui analizzato.

TOP-20 relativa ai programmi malware destinati alle piattaforme mobile

	Denominazione	% di attacchi*
1	Trojan-SMS.AndroidOS.Stealer.a	15,63%
2	RiskTool.AndroidOS.SMSreg.gc	14,17%
3	AdWare.AndroidOS.Viser.a	10,76%
4	Trojan-SMS.AndroidOS.FakeInst.fb	7,35%
5	RiskTool.AndroidOS.CallPay.a	4,95%
6	Exploit.AndroidOS.Lotoor.be	3,97%
7	DangerousObject.Multi.Generic	3,94%
8	RiskTool.AndroidOS.MimobSMS.a	3,94%
9	Trojan-SMS.AndroidOS.Agent.ao	2,78%
10	AdWare.AndroidOS.Ganlet.a	2,51%
11	Trojan-SMS.AndroidOS.OpFake.a	2,50%
12	RiskTool.AndroidOS.SMSreg.de	2,36%
13	Trojan-SMS.AndroidOS.FakeInst.ff	2,14%
14	Trojan-SMS.AndroidOS.Podec.a	2,05%
15	Trojan-SMS.AndroidOS.Erop.a	1,53%
16	RiskTool.AndroidOS.NeoSMS.a	1,50%
17	Trojan.AndroidOS.Agent.p	1,47%
18	Trojan-SMS.AndroidOS.OpFake.bo	1,29%
19	RiskTool.AndroidOS.SMSreg.hg	1,19%
20	Trojan-Ransom.AndroidOS.Small.e	1,17%

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

Osserviamo, in primo luogo, come nell'ambito della TOP-20 relativa alle minacce informatiche destinate ai dispositivi mobile, i Trojan-SMS stiano progressivamente perdendo posizioni: infatti, mentre nel secondo trimestre del 2014 tali programmi malware occupavano ben quindici posizioni all'interno del rating in questione, nel periodo oggetto del presente report i Trojan-SMS presenti in graduatoria risultano essere "soltanto" in otto. Sottolineiamo, inoltre, come nel trimestre precedente l'indice percentuale attribuibile al leader della TOP-20 - il malware mobile classificato dagli esperti di sicurezza IT con la denominazione di Trojan-SMS.AndroidOS.Stealer.a - risultasse pari al 25,42% del volume totale di

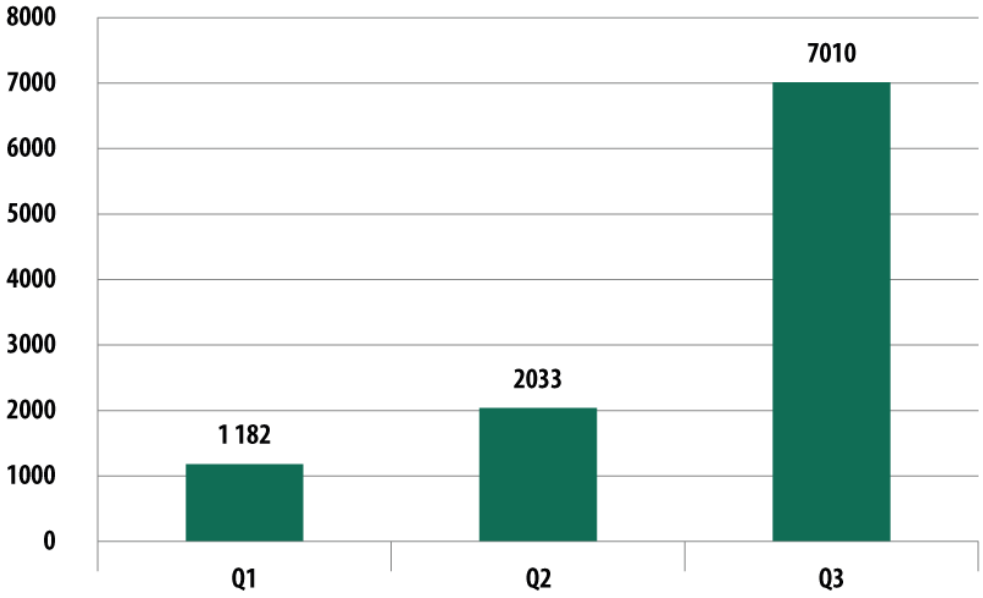
attacchi, mentre nel terzo trimestre del 2014 la quota ascrivibile al suddetto programma nocivo ha fatto complessivamente registrare un valore pari al 15,63%.

All'interno della graduatoria del malware mobile da noi stilata, troviamo ugualmente numerosi rappresentanti della categoria RiskTool, i quali sono andati ad occupare ben sei posizioni delle venti disponibili nell'ambito della TOP-20 qui esaminata. La seconda posizione del rating, ad esempio, è andata ad appannaggio di RiskTool.AndroidOS.SMSreg.gc, con una quota pari al 14,17% del numero complessivo di attacchi informatici rilevati nei confronti degli utenti dei dispositivi mobile.

Al settimo posto della graduatoria, poi, spicca la presenza del malware classificato come DangerousObject.Multi.Generic (3,94%). 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 reagire in ogni frangente, con la massima rapidità, nei confronti di minacce IT nuove o sconosciute.

I Trojan bancari mobile

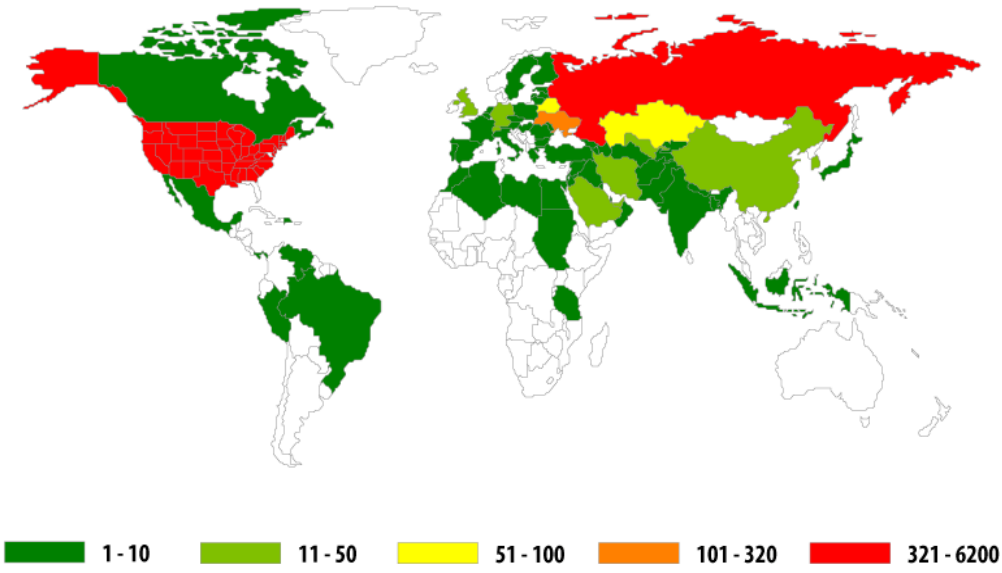
Nel periodo oggetto della nostra analisi sono stati da noi individuati ben **7.010** Trojan bancari mobile, ovvero un numero 3,4 volte superiore rispetto all'analoga quantità rilevata nel secondo trimestre dell'anno corrente.



Numero di Trojan bancari per piattaforme mobile individuati nel periodo 1° trimestre - 3° trimestre 2014

Sta ugualmente crescendo, di pari passo, il numero dei paesi in cui si registrano attacchi informatici a danno degli utenti mobile mediante il dispiegamento di questi pericolosi programmi malware: mentre nel secondo trimestre dell'anno in corso erano stati registrati attacchi, da parte di Trojan-Banker mobile - perlomeno una volta - in 31 diversi paesi, nel terzo trimestre del 2014 tale cifra è sensibilmente aumentata (in sostanza più che raddoppiata); i famigerati Trojan bancari appositamente creati dai virus

writer per attaccare i dispositivi mobile hanno difatti cercato di colpire potenziali utenti-vittima ubicati in ben 70 paesi del pianeta.



Quadro mondiale relativo alla ripartizione geografica dei tentativi di infezione compiuti, nel corso del terzo trimestre 2014, dai Trojan bancari destinati ai dispositivi mobile (numero di utenti sottoposti ad attacco)

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

	Paese	% sul numero complessivo di attacchi*
1	Russia	83,85%
2	USA	7,09%
3	Ukraina	1,79%
4	Bielorussia	1,18%
5	Kazakhstan	0,92%
6	Repubblica di Corea	0,68%
7	Germania	0,62%
8	Cina	0,50%
9	Gran Bretagna	0,50%
10	Arabia Saudita	0,35%

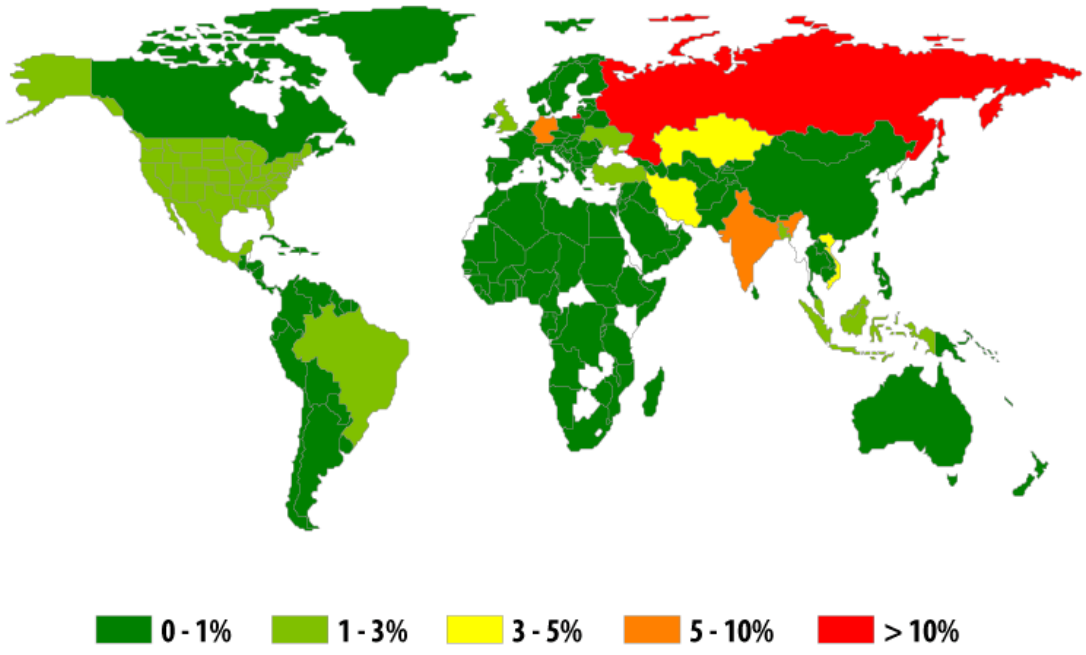
** Quote percentuali relative al numero di utenti attaccati nel paese da parte di Trojan bancari mobile, in relazione al numero complessivo di utenti unici sottoposti ad attacco*

Desideriamo sottolineare, in primo luogo, come non faccia più parte della TOP-10 qui sopra riportata l'Italia (quarta nell'analoga graduatoria relativa al trimestre precedente), mentre rileviamo la presenza nel rating dell'Arabia Saudita, collocatasi in decima posizione.

Come da tradizione ormai ampiamente consolidata, la leadership del ranking in questione continua ad essere detenuta dalla Federazione Russa, nonostante l'indice ad essa ascrivibile abbia fatto registrare una significativa flessione, pari a 7,85 punti percentuali. Allo stesso tempo, le quote relative agli altri paesi presenti nella TOP-10 in causa risultano lievemente aumentate: di fatto, pare proprio che, al giorno d'oggi, i cybercriminali “mobile” stiano gradualmente espandendo il raggio e la portata delle attività illecite da essi condotte.

Geografia delle minacce mobile

Lungo tutto l'arco del terzo trimestre dell'anno 2014, si sono registrati attacchi informatici da parte di programmi malware destinati ai dispositivi mobile - perlomeno una volta - in ben 205 diversi paesi.



Quadro mondiale relativo alla ripartizione geografica dei tentativi di infezione compiuti, nel corso del terzo trimestre del 2014, 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 mobile:

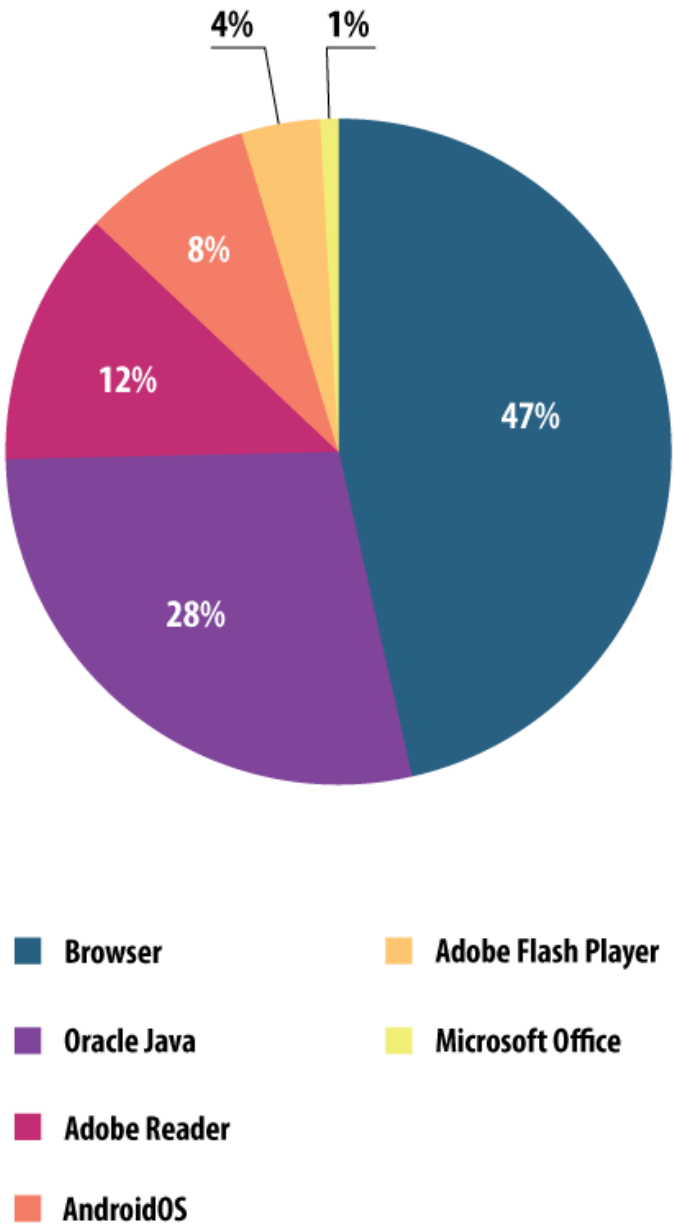
	Paese	% di attacchi*
1	Russia	44,0%
2	India	7,6%
3	Germania	5,6%
4	Iran	3,4%
5	Vietnam	3,1%
6	Kazakhstan	3,1%
7	Ukraina	2,7%
8	Malaysia	1,9%
9	Brasile	1,7%
10	USA	1,7%

** Quote percentuali relative al numero di utenti attaccati nel paese da parte di malware mobile, 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 44% di utenti sottoposti ad attacco da parte di malware mobile. Il secondo gradino del podio virtuale relativo al terzo trimestre dell'anno risulta occupato dall'India, paese tornato a far parte delle posizioni di vertice della graduatoria qui esaminata; la quota attribuibile al gigante del sub-continente indiano si è in effetti attestata su un valore medio piuttosto elevato, pari al 7,6%. Per la prima volta, nel corso del 2014, hanno fatto la loro comparsa - all'interno della TOP-10 qui sopra riportata - paesi quali Iran (3,4%) e Stati Uniti (1,7%), posizionatisi, rispettivamente, al quarto e al decimo posto della graduatoria inerente ai paesi sottoposti con maggior frequenza ad attacchi da parte di malware mobile. Per contro, non fanno attualmente più parte della TOP-10 in questione i seguenti paesi: Polonia, Francia, Spagna e Messico.

Le applicazioni vulnerabili maggiormente sfruttate dai malintenzionati

La 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 3° trimestre del 2014

E' stato innanzitutto osservato come, nel periodo oggetto del presente report statistico, il 47% dei tentativi di sfruttamento di vulnerabilità da noi rilevati abbia di fatto visto l'utilizzo, da parte dei cybercriminali, di exploit appositamente creati per colpire vulnerabilità, o falle di sicurezza che dir si voglia, individuate all'interno dei browser (i programmi comunemente utilizzati per la navigazione in Internet) ed in primo luogo in Internet Explorer. E' stato rilevato dai nostri esperti come, in pratica, nell'ambito di ogni kit di exploit venga utilizzato almeno un exploit specificamente elaborato dai virus writer per attaccare il programma di navigazione Internet Explorer.

Al secondo posto della graduatoria qui sopra presentata troviamo poi gli exploit destinati alla piattaforma Java. Le vulnerabilità Java vengono abitualmente sfruttate nel corso degli attacchi di tipo "drive-by download", condotti dai malintenzionati attraverso Internet. Gli exploit correlati a Java fanno attualmente parte della composizione di un elevato numero di exploit pack, anche se, ormai quasi da un anno a questa parte, non si hanno di fatto notizie di nuove vulnerabilità rilevate all'interno di Java. Complessivamente, nel terzo trimestre del 2014, le vulnerabilità della piattaforma Java sono state oggetto del 28% dei tentativi di sfruttamento di vulnerabilità da parte di malintenzionati; nel trimestre precedente la quota percentuale ascrivibile ad Oracle Java si era attestata su un valore medio leggermente superiore, pari al 29%, mentre nel primo trimestre dell'anno in corso tale indice era risultato pari al 54%.

Ricordiamo, a tal proposito, che nell'anno 2013, addirittura il 90,5% dei tentativi di sfruttamento di vulnerabilità da noi rilevati si era dimostrato rivolto a vulnerabilità individuate all'interno di Java. Nel 2014, poi, la popolarità di cui godono gli exploit Java presso gli ambienti cybercriminali ha iniziato progressivamente a manifestare pronunciati segni di flessione, sino a raggiungere i valori attuali, decisamente più contenuti rispetto al recente passato.

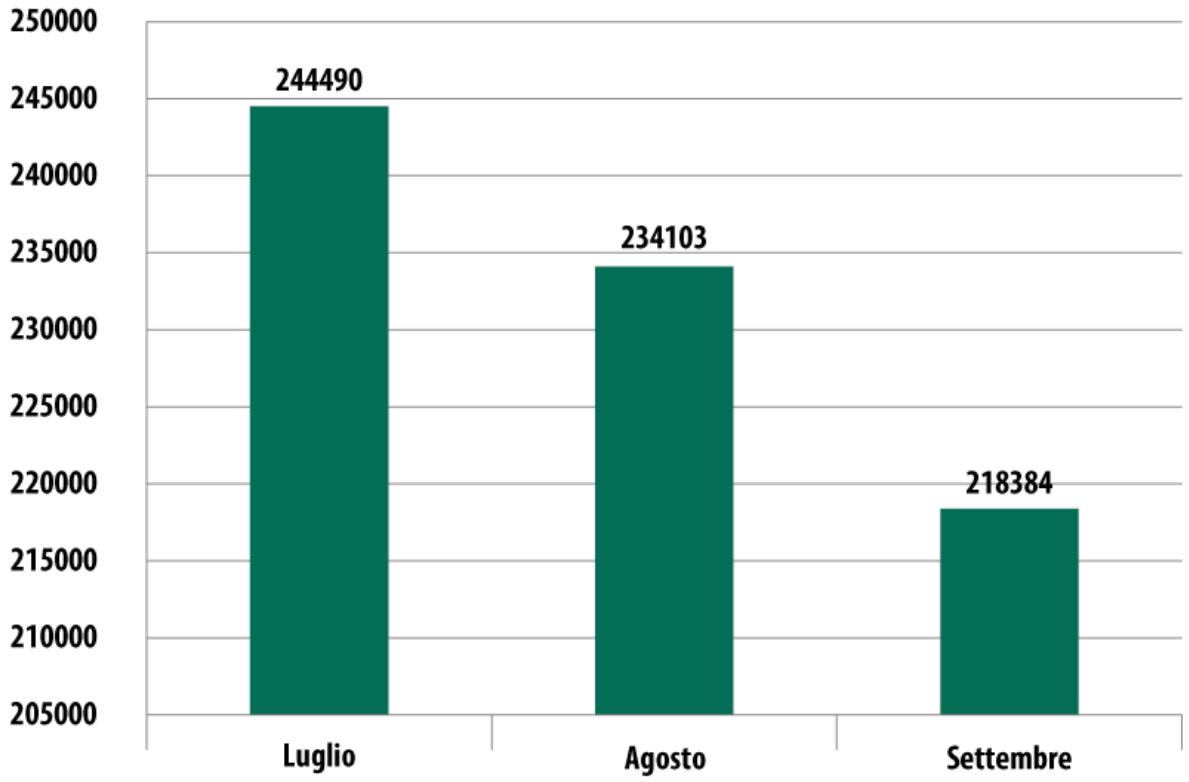
Come evidenzia il grafico precedentemente riportato, il terzo posto del rating in questione risulta occupato dagli exploit appositamente sviluppati dai virus writer per attaccare l'applicazione Adobe Reader (12%). Tali vulnerabilità vengono ugualmente utilizzate per la conduzione di attacchi via Internet, di tipo drive-by; gli exploit PDF, al pari di quelli destinati alla piattaforma Java, fanno anch'essi parte della composizione di una moltitudine di kit di exploit.

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 infette. I siti Internet dannosi vengono appositamente allestiti dai cybercriminali e possono 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 terzo trimestre del 2014, 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 delle vittime mediante l'accesso non autorizzato agli account bancari posseduti da questi ultimi - sui computer di ben **696.977** utenti della rete globale di sicurezza Kaspersky Security Network. Desideriamo sottolineare come, rispetto all'analogo valore rilevato riguardo al periodo analizzato nel precedente resoconto trimestrale dedicato all'evoluzione del malware (**927.568** computer degli utenti KSN sottoposti ad attacco nel corso del 2° trimestre del 2014), tale indice abbia ad ogni caso fatto registrare un sensibile decremento, pari al **24,9%.**

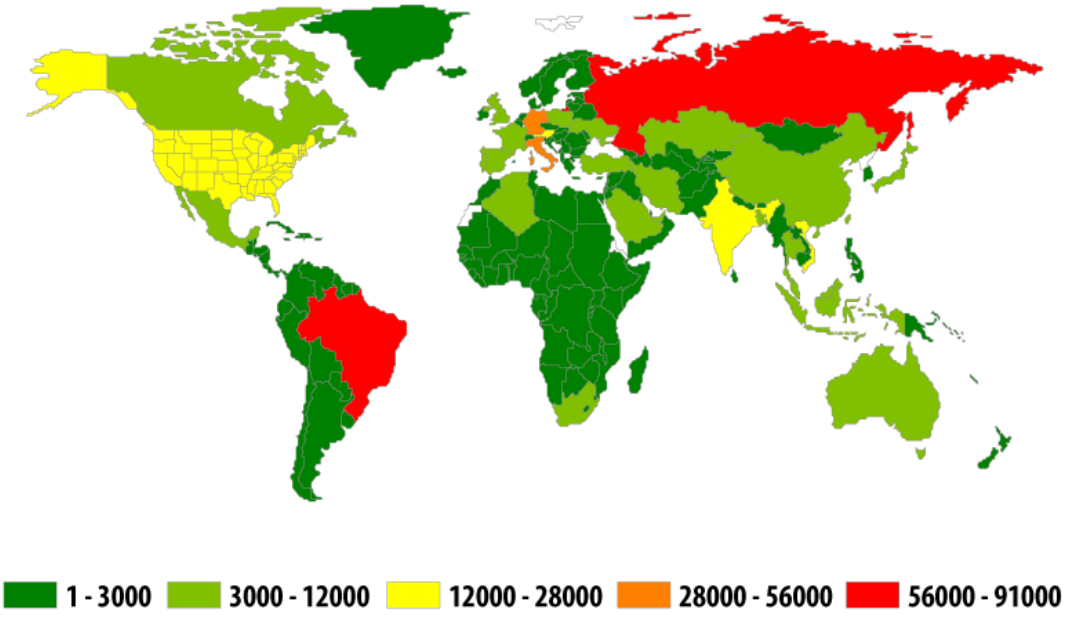


Numero di computer sottoposti ad attacco da parte di malware finanziari - Situazione relativa al terzo trimestre del 2014

E' di particolare interesse osservare come, lungo tutto l'arco del trimestre oggetto del presente report, il numero degli attacchi portati dai malware riconducibili alla sfera finanziaria sia progressivamente diminuito, come traspare in tutta evidenza dal grafico qui sopra inserito. In effetti, mentre nel mese di luglio 2014 sono stati registrati 244.490 attacchi finanziari, nel successivo mese di settembre il numero complessivo di tale genere di attacchi informatici è risultato pari a 218.384 unità, facendo quindi segnare un decremento di ben 11 punti percentuali.

Complessivamente, nel corso del trimestre qui preso in esame, le soluzioni di sicurezza IT sviluppate da Kaspersky Lab e implementate nei computer degli utenti iscritti al programma di protezione globale KSN, hanno fatto registrare **2.466.952** 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 3° trimestre 2014 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	90176
Russia	57729
Germania	55225
Italia	32529
India	24975
USA	22340
Austria	22013
Vietnam	13495
Gran Bretagna	11095
Cina	9060

Così come in precedenza, la 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, sebbene, rispetto al secondo trimestre dell'anno in corso, la quota relativa al colosso del continente latino-americano sia diminuita di oltre una volta e mezzo. Il secondo gradino del podio virtuale risulta occupato, così come

nel trimestre precedente, dalla Federazione Russa. Da parte sua, l'Italia ha perso una posizione nell'ambito della classifica relativa all'attuale diffusione geografica del malware bancario, collocandosi alla quarta posizione della graduatoria da noi stilata. Al terzo posto del rating si è così insediata la Germania, paese in cui, rispetto al secondo trimestre dell'anno in corso, il numero di utenti sottoposti ad attacco da parte di malware legati alla sfera finanziaria è aumentato di una volta e mezzo.

TOP-10 inerente alle famiglie di malware bancario maggiormente diffuse

La TOP-10 del terzo trimestre del 2014 relativa alle famiglie a cui appartengono i programmi malware maggiormente utilizzati nell'ambito degli attacchi informatici eseguiti dai malintenzionati nei confronti degli utenti dei sistemi di online banking - redatta sulla base del numero di notifiche emesse riguardo ai tentativi di infezione perpetrati dai suddetti software nocivi, così come del numero di utenti sottoposti ad attacco - si presenta nella maniera seguente:

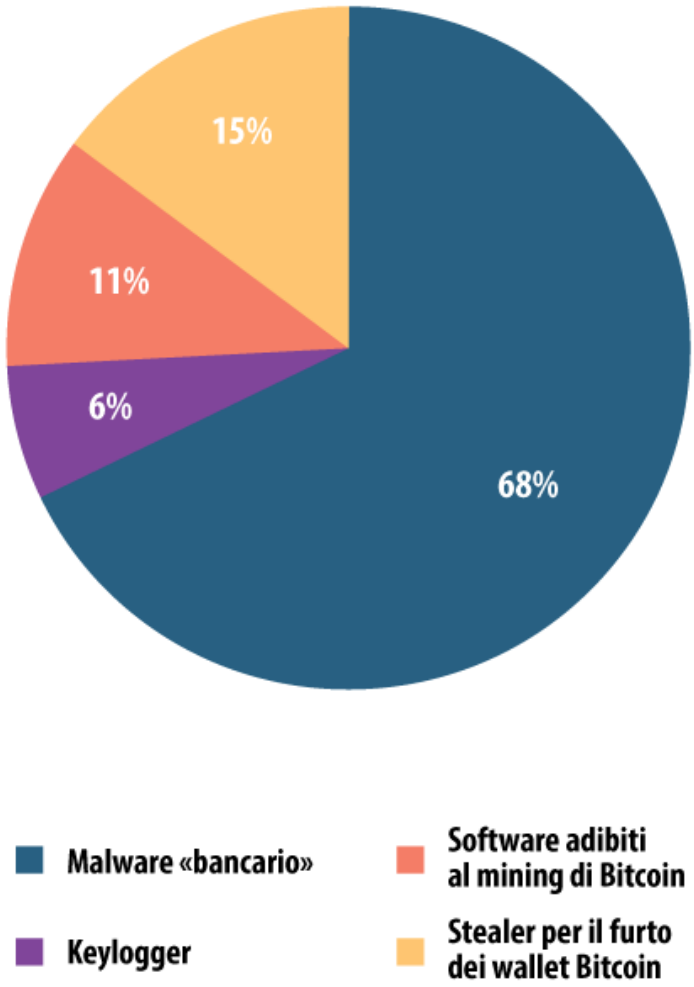
Denominazione**	**Numero di notifiche**	**Numero di utenti sottoposti ad attacco**
Trojan-Spy.Win32.Zbot	1381762	285559
Trojan-Banker.Win32.ChePro	322928	92415
Trojan-Banker.Win32.Shiotob	123150	24839
Trojan-Banker.Win32.Agent	49563	23943
Trojan-Banker.HTML.PayPal	117692	21138
Trojan-Spy.Win32.SpyEyes	73496	19113
Trojan-Banker.Win32.Lohmys	47188	16619
Trojan-Banker.Win32.Banker	39892	12673
Trojan-Banker.Win32.Banbra	20563	9646
Backdoor.Win32.Sinowal	18921	8189

Così come in precedenza, il Trojan bancario maggiormente diffuso risulta essere il famigerato software maligno denominato ZeuS (Trojan-Spy.Win32.Zbot), sebbene il numero di attacchi informatici attribuibili a tale programma malware, al pari del numero complessivo di utenti sottoposti ad attacco da parte di ZeuS, risulti in pratica dimezzato rispetto a quanto riscontrato nel trimestre precedente.

Alla terza posizione del rating elaborato dai nostri esperti è andato a collocarsi il Trojan bancario rilevato dalle soluzioni di sicurezza IT di Kaspersky Lab come Trojan-Banker.Win32.Shiotob, il quale viene prevalentemente distribuito, dai malintenzionati della Rete mediante appositi messaggi di spam nocivo. Tale insidioso software dannoso risulta altamente specializzato nel monitorare il traffico sul computer, allo scopo di intercettare i dati sensibili relativi alle operazioni di pagamento condotte dall'utente-vittima. E' di particolare interesse sottolineare come la stragrande maggioranza delle famiglie di malware (ben 9 su 10) presenti nella composizione della graduatoria da noi stilata, riportata nella tabella qui sopra inserita, si avvalgano 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 subdolamente a rimpiazzare i moduli originali.

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 degli attacchi informatici volti a carpire illecitamente il denaro degli utenti - Suddivisione realizzata sulla base delle varie tipologie di malware utilizzate dai cybercriminali (situazione relativa al terzo trimestre 2014)

La seconda tipologia di minaccia IT per grado di popolarità e diffusione - tra i vari metodi alternativi praticati dai cybercriminali per realizzare il furto del denaro elettronico - è rappresentata dagli stealer adibiti al furto dei portafogli virtuali Bitcoin, gli ambiti wallet digitali contenenti criptovaluta. La quota ascrivibile a tale metodo illecito di ricavare profitti in Rete risulta quasi raddoppiata rispetto all'analogo valore registrato nel secondo trimestre del 2014, essendo passata, in soli tre mesi, dall'8% ad un valore pari al 15%. 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. Desideriamo sottolineare, nella fattispecie, come l'utilizzo dei Bitcoin miner

malevoli (le famigerate applicazioni adibite al mining dei Bitcoin a totale insaputa dell'utente sottoposto ad attacco) rappresenti tuttora l' 11% del volume complessivo degli attacchi finanziari condotti dai criminali informatici.

TOP-20 relativa agli oggetti infetti rilevati in Internet

Come abbiamo visto, nel corso del terzo trimestre del 2014 il nostro Anti-Virus Web ha effettuato il rilevamento di ben 26.641.747 oggetti dannosi unici (script, pagine web, exploit, file eseguibili, etc.).

Fra tutti i programmi malware 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 96,2% 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	59,83%
2	AdWare.Script.Generic	14,46%
3	Trojan.Script.Generic	13,13%
4	Trojan.Script.Iframer	1,77%
5	AdWare.Win32.Agent.fflm	1,23%
6	Trojan-Downloader.Script.Generic	1,02%
7	AdWare.Win32.Agent.allm	1,02%
8	AdWare.JS.Agent.ao	0,78%
9	AdWare.JS.Agent.an	0,55%
10	AdWare.Win32.Agent.aiyc	0,32%
11	AdWare.Win32.OutBrowse.g	0,32%
12	Trojan.Win32.Generic	0,30%
13	AdWare.Win32.Amonetize.bcw	0,23%
14	AdWare.Win32.Amonetize.cmg	0,18%
15	AdWare.Win32.Yotoon.heur	0,18%
16	Trojan-Downloader.Win32.Generic	0,15%
17	AdWare.Win32.Amonetize.cmd	0,14%
18	Trojan-Dropper.Win32.Agent.lefs	0,12%
19	AdWare.Win32.Linkun.j	0,11%
20	AdWare.Win32.Amonetize.aik	0,09%

** 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.*

Così come nei precedenti trimestri oggetto della nostra analisi dedicata all'evoluzione dei malware, la TOP-20 esaminata nel presente capitolo del report annovera, per la maggior parte, la presenza di rilevamenti 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 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 59,8% del volume complessivo dei rilevamenti effettuati dal modulo Anti-Virus Web. In precedenza, tali oggetti infetti venivano da noi identificati con la denominazione generica “Blocked”. Si tratta, in sostanza, di indirizzi Internet inseriti nella nostra blacklist, relativi ad un consistente numero di siti malevoli verso i quali vengono reindirizzati gli ignari utenti-vittima; in genere, tali pagine web contengono kit di exploit, bot, trojan estorsori, etc. Nella maggior parte dei casi, gli utenti giungono sui siti web dannosi dopo aver visitato con il proprio browser risorse Internet del tutto legittime - ma violate dai cybercriminali - all'interno delle quali i malintenzionati hanno provveduto ad iniettare pericolosi codici maligni, spesso sotto forma di script nocivi (tale tipologia di attacco informatico viene definita dagli esperti di sicurezza IT con l'appellativo di “drive-by download”). Al tempo stesso, esiste in Rete un ragguardevole numero di siti web maligni creati espressamente dai criminali per lanciare pericolosi attacchi nei confronti dei computer-vittima. E’ facile quindi comprendere come risulti di fondamentale importanza poter disporre, sul proprio computer, di un’efficace soluzione anti-malware. Oltre a ciò, le infezioni informatiche possono prodursi anche quando gli utenti cliccano in maniera volontaria su collegamenti ipertestuali potenzialmente pericolosi, ad esempio nel momento in cui essi procedono alla ricerca sul web dei più svariati contenuti pirata.

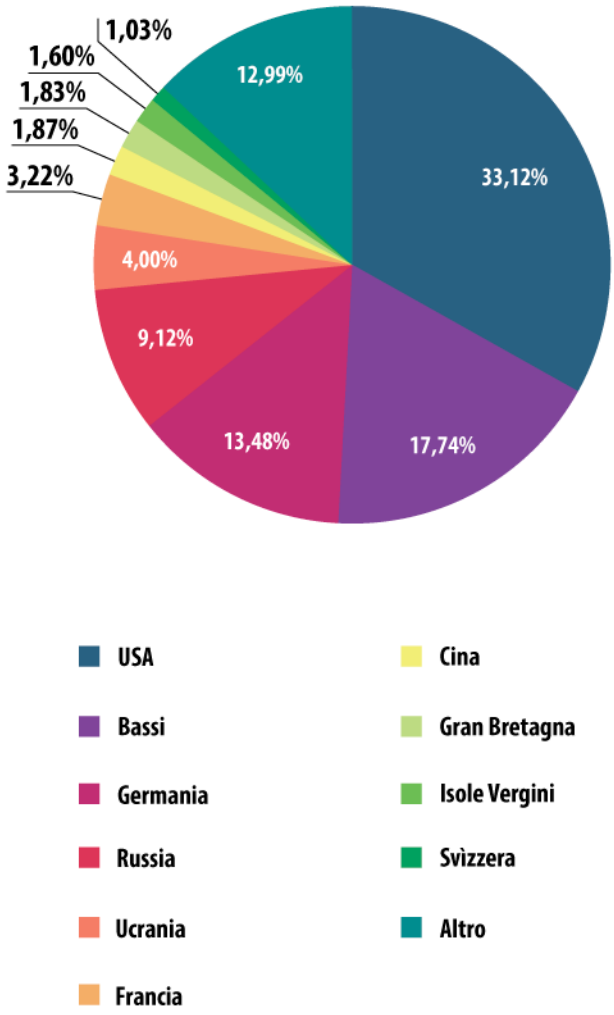
Geografia delle fonti degli attacchi web: TOP-10

Questi 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 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 condotti tramite web è stato applicato il metodo che prevede la 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 terzo trimestre del 2014 le soluzioni anti-malware di Kaspersky Lab hanno complessivamente respinto ben 367.431.148 attacchi condotti attraverso siti Internet compromessi, dislocati in vari paesi. L' 87% 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. L'indice in questione è quindi diminuito dell' 1,3% rispetto all'analoga quota percentuale rilevata nel secondo trimestre dell'anno 2014.



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

La composizione della TOP-10 da noi elaborata, riguardante i paesi che attualmente detengono le posizioni di leadership nell'ambito dell'apposita graduatoria relativa alle principali fonti degli attacchi informatici condotti via Internet, presenta importanti variazioni rispetto all'analogo rating del trimestre precedente. Osserviamo, in primo luogo, come non facciano più parte della TOP-10 né Canada (- 7 punti percentuali), né Irlanda (- 0,7 punti percentuali). La Cina, al contrario, che non compariva nelle posizioni di vertice della graduatoria "geografica" degli attacchi via web addirittura dal secondo trimestre del 2013, ha di nuovo fatto il proprio ingresso nella TOP-10 qui sopra inserita; con un indice pari all' 1,87%, la Repubblica Popolare Cinese si è direttamente collocata al 7° posto del ranking in questione. Rileviamo inoltre, per la prima volta, la presenza della Svizzera (1,03%) nell'ambito della classifica delle fonti geografiche degli attacchi via Internet, rating elaborato dagli esperti di Kaspersky Lab.

I cambiamenti più significativi prodottisi all'interno della TOP-10 in causa riguardano tuttavia gli indici relativi agli Stati Uniti (+ 11,2 punti percentuali rispetto al 2° trimestre del 2014) - gli USA si sono in tal

modo collocati al primo posto della graduatoria - ed alla Germania (- 9 punti percentuali rispetto al ranking del trimestre precedente), la quale è così scesa dal primo al terzo posto in classifica.

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

Al fine di valutare nel modo più preciso 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 pianeta - 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	Russia	46,68%
2	Kazakhstan	45,92%
3	Azerbaijan	43,50%
4	Armenia	41,64%
5	Ukraina	40,70%
6	Iran	39,91%
7	Vietnam	38,55%
8	Bielorussia	38,08%
9	Moldavia	36,64%
10	Algeria	36,05%
11	Tagikistan	36,05%
12	Kirghizistan	33,59%
13	Mongolia	33,59%
14	Qatar	30,84%
15	Uzbekistan	29,22%
16	Georgia	29,17%
17	Turchia	28,91%
18	Emirati Arabi Uniti	28,76%
19	Indonesia	28,59%
20	Germania	28,36%

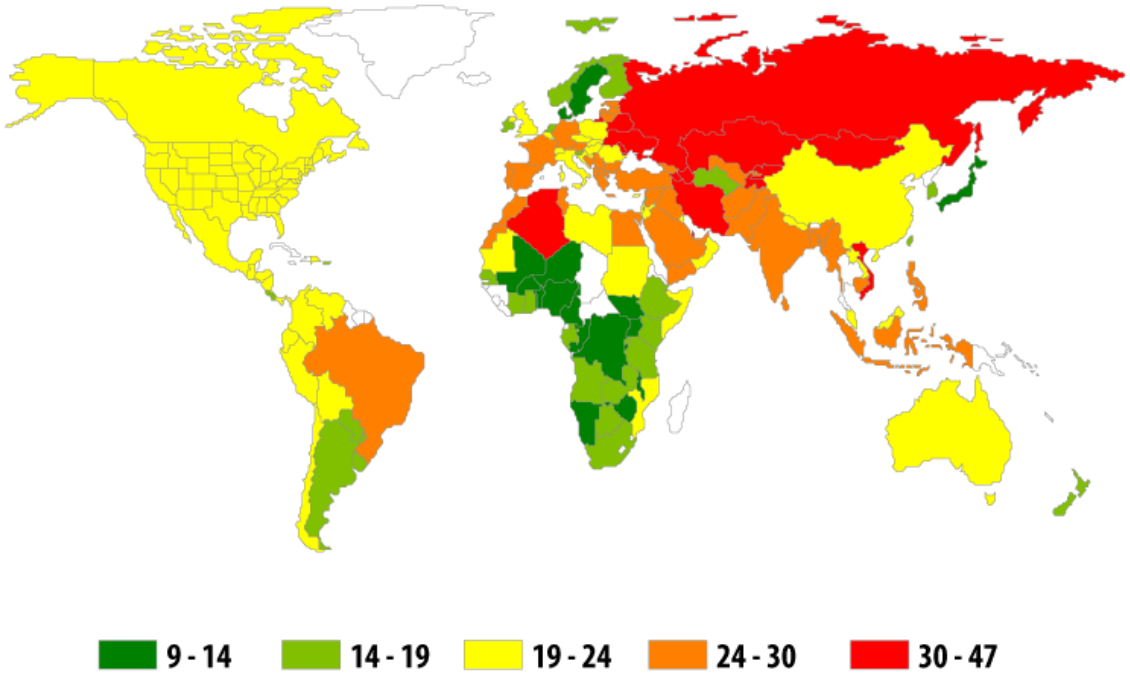
I dati statistici sopra indicati sono stati elaborati sulla base dei rilevamenti effettuati dal modulo Anti-Virus Web; essi sono stati ricevuti tramite gli utenti dei prodotti Kaspersky Lab che hanno previamente fornito l'assenso per effettuare la trasmissione di dati statistici ai nostri analisti.

**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.*

Rileviamo, innanzitutto, come nel terzo trimestre del 2014 non facciano più parte della TOP-20 qui esaminata la Croazia, la Tunisia e la Spagna. Le "new entry" del rating sono rappresentate da Emirati Arabi Uniti (28,76%), Indonesia (28,59%) e Germania (28,36%), ovvero i paesi che sono andati ad occupare, rispettivamente, le posizioni di coda della graduatoria stilata dai nostri esperti.

Tra i paesi nei quali la navigazione in Internet risulta in assoluto più sicura troviamo la Svezia (12,4%), la Danimarca (13,2%), il Giappone (13,3%), il Sudafrica (16,0%), la Finlandia (16,1%) e i Paesi Bassi (16,6%).



Complessivamente, a livello mondiale, nel corso del trimestre qui analizzato una consistente porzione degli utenti della Rete (29,5%), 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 terzo 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.
Lungo tutto l'arco del terzo trimestre dell'anno in corso, il nostro modulo Anti-Virus File ha rilevato con successo 116.710.804 oggetti maligni unici, o potenzialmente indesiderabili.

Oggetti maligni rilevati nei computer degli utenti: TOP-20

	Denominazione*	% di utenti unici sottoposti ad attacco**
1	Trojan.Win32.Generic	18,95%
2	DangerousObject.Multi.Generic	18,39%
3	AdWare.MSIL.Kranet.heur	11,61%
4	AdWare.Win32.Agent.ahbx	5,77%
5	Trojan.Win32.AutoRun.gen	4,81%
6	AdWare.Win32.Kranet.heur	4,68%
7	AdWare.NSIS.Zaitu.heur	4,51%
8	Worm.VBS.Dinihou.r	4,51%
9	Virus.Win32.Sality.gen	4,08%
10	AdWare.Win32.Yotoon.abs	4,03%
11	AdWare.Win32.IBryte.dolh	3,14%
12	AdWare.Win32.Agent.aljt	3,12%
13	AdWare.Win32.Agent.allm	3,11%
14	AdWare.Win32.Yotoon.heur	3,10%
15	Adware.Win32.Amonetize.heur	2,86%
16	AdWare.Win32.Agent.heur	2,80%
17	WebToolbar.JS.Condonit.a	2,59%
18	Worm.Win32.Debris.a	2,56%
19	AdWare.Win32.Kranet.c	2,55%
20	Trojan.Script.Generic	2,51%

**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.*

Come da tradizione ormai consolidata, la maggior parte delle posizioni di cui si compone il rating qui sopra riportato risulta occupata dai rilevamenti riconducibili ai programmi AdWare; nel terzo trimestre del 2014, tali software sono andati a collocarsi in ben 13 posizioni della TOP-20 da noi stilata riguardo agli oggetti dannosi più frequentemente rilevati sui computer degli utenti.

I worm che si diffondono attraverso i supporti di memoria rimovibili si sono a loro volta insediati in due diverse posizioni all'interno della classifica qui sopra inserita (8° e 18° posto).

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; nel terzo trimestre dell'anno corrente tale oggetto maligno è andato ad occupare il 9° posto del rating (ricordiamo che Sality.gen occupava la settima posizione nell'analogo rating relativo al secondo trimestre del 2014).

Nel concludere la nostra breve analisi della classifica qui sopra riportata, è di particolare interesse osservare come, nel trimestre oggetto del presente report, sia significativamente aumentato il numero dei programmi AdWare, e dei loro relativi componenti, via via individuati dal nostro modulo Anti-Virus File; tali componenti partecipano in maniera decisamente attiva sia alla diffusione dei suddetti programmi pubblicitari, sia all'opera di contrasto dell'azione abitualmente svolta dalle soluzioni anti-virus.

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

	Paese	% di utenti unici*
1	Vietnam	61,89%
2	Bangladesh	55,01%
3	Mongolia	54,13%
4	Nepal	53,08%
5	Algeria	51,71%
6	Cambogia	51,26%
7	Afghanistan	50,59%
8	Repubblica Popolare Democratica del Laos	50,55%
9	Yemen	50,38%
10	Pakistan	50,35%
11	Egitto	49,65%
12	India	49,44%
13	Iraq	49,33%
14	Iran	48,85%
15	Etiopia	47,87%
16	Birmania	46,71%
17	Sri Lanka	46,67%
18	Siria	46,24%
19	Qatar	46,03%
20	Tunisia	45,36%

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. 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).*

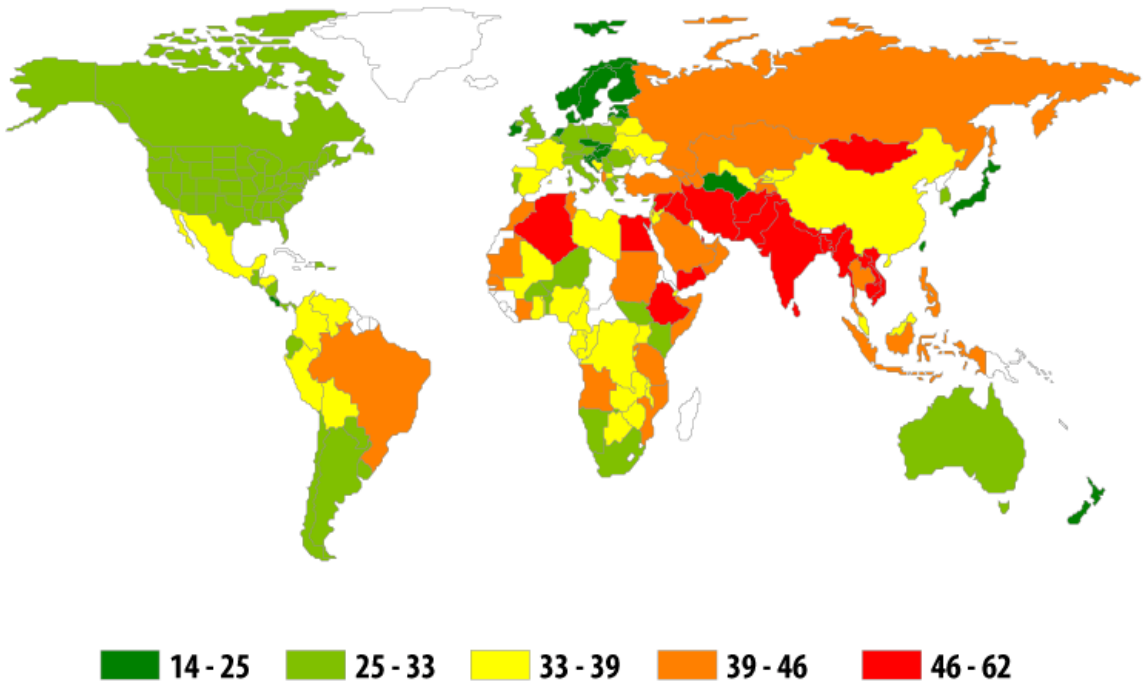
*** Quote percentuali relative al numero di utenti unici sui computer dei quali sono state bloccate e neutralizzate minacce informatiche locali, rispetto al numero complessivo di utenti unici dei prodotti Kaspersky Lab nel paese.*

Le prime venti posizioni della 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, con un indice pari al 61,89%.

Da parte sua, la Mongolia (54,13%) è scesa dal secondo al terzo gradino del podio virtuale del 3° trimestre dell'anno in corso, avendo di fatto ceduto la seconda posizione del rating al Bangladesh (55,01%).

Osserviamo, inoltre, come abbia fatto per la prima volta il suo ingresso all'interno della TOP-20 il Qatar (46,03%); il paese situato nella Penisola Arabica si è tuttavia collocato in penultima posizione. Notiamo, poi, come siano entrati nuovamente a far parte del rating Birmania (46,71%) e Sri Lanka (46,67%), mentre risultano usciti dalla composizione della TOP-20 in questione Arabia Saudita, Turchia e Gibuti.

In Russia, durante il terzo trimestre del 2014, sono state rilevate minacce IT di origine locale - perlomeno una volta - sul 44,4% 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 (15%), Svezia (16,4%), Danimarca (16,5%), Finlandia (18%) e Singapore (19,7%).

In media, nel mondo, durante il terzo trimestre del 2014, sono state rilevate minacce IT di origine locale - perlomeno una volta - sul 37,2% dei computer degli utenti; tale indice supera di ben 4,4 punti percentuali l'analoga quota rilevata riguardo al secondo trimestre dell'anno in corso.