Attacchi DDoS nel secondo trimestre del 2015

Kaspersky Lab

Sommario

La pluriennale esperienza degli specialisti di Kaspersky Lab nel contrastare gli attacchi DDoS di qualsiasi genere, complessità e potenza, unitamente alla continua e assidua osservazione delle attività condotte nell'ambito delle botnet - realizzata con l'ausilio del sistema DDoS Intelligence (parte della soluzione di sicurezza Kaspersky DDoS Protection) - consente alla nostra società di svolgere un ruolo all'avanguardia relativamente alla protezione nei confronti di tali attacchi.

I principali eventi del trimestre

Tra tutti gli avvenimenti che hanno contrassegnato il secondo trimestre del 2015 nella sfera degli attacchi DDoS e degli strumenti impiegati per la loro realizzazione, abbiamo scelto quelli che, a nostro avviso, illustrano nel modo migliore le principali tendenze che si manifestano nel costante processo di evoluzione di tale specifica minaccia IT. I malintenzionati, nella fattispecie,

- escogitano ed utilizzano nuove tecniche, volte ad incrementare la potenza e l'intensità degli attacchi condotti, senza dover necessariamente ampliare le dimensioni delle botnet di cui si avvalgono;
- creano botnet composte da dispositivi connessi ad Internet ed utilizzano poi gli stessi per effettuare gli attacchi DDoS;
- sviluppano moduli DDoS di natura complessa, mediante i quali vengono realizzati attacchi mirati.

Un modulo DDoS nell'arsenale di Animal Farm

Nello scorso mese di marzo gli esperti di Kaspersky Lab hanno pubblicato i risultati dell'indagine condotta riguardo agli attacchi informatici eseguiti dal noto gruppo APT conosciuto con l'appellativo di Animal Farm. I cybercriminali in questione hanno fatto ricorso a tutta una serie di componenti nocivi, ognuno dei quali era in grado di svolgere un determinato compito. Uno di questi componenti era rappresentato dal programma Trojan denominato NBot, utilizzato per l'allestimento e la gestione della botnet; tale software nocivo è risultato ugualmente provvisto di specifiche funzionalità atte alla conduzione di attacchi DDoS. L'elevato numero di scenari previsti per la realizzazione degli attacchi Distributed Denial of Service, scenari supportati dal malware NBot, rappresenta un indice inequivocabile del fatto che la botnet viene in pratica costruita, dai malintenzionati, allo scopo di effettuare attacchi DDoS su larga scala.

Un ulteriore metodo per incrementare la potenza dell'attacco DDoS

Gli scenari nei quali - per rafforzare la portata dell'attacco condotto - si fa ricorso ai difetti di configurazione di vari servizi di rete, hanno ulteriormente consolidato la propria posizione nell'ambito delle tecniche malevole utilizzate dai proprietari delle botnet. Nel corso del secondo trimestre del 2015, i ricercatori hanno individuato un ulteriore strumento in grado di amplificare la potenza di un attacco DDoS; esso sfrutta, in sostanza, i difetti di configurazione eventualmente presenti nei programmi che utilizzano il protocollo multicast Domain Name System (mDNS). In presenza di determinate condizioni, le dimensioni della risposta fornita dal servizio che opera in base al protocollo mDNS possono risultare sensibilmente superiori alle dimensioni della richiesta effettuata. Ciò significa, in pratica, che i proprietari delle botnet possono inviare, a simili servizi, una query appositamente confezionata, per poi reindirizzare la stessa alla vittima, con un volume notevolmente maggiore.

Il «Grande Cannone»

Il cosiddetto «Grande Cannone» è una particolare tecnologia applicata nell'ambito degli attacchi DDoS condotti nei confronti di GitHub. Lo scorso 6 marzo, i proprietari del sito web GreatFire.org rilevavano che i loro server erano divenuti bersaglio di un attacco DDoS. 10 giorni più tardi, risultava ugualmente sotto attacco la pagina ufficiale di GreatFire.org sul portale GitHub. I proprietari di GitHub, da parte loro, confermavano l'avvenuta esecuzione di un potente attacco DDoS — da parte dei server del motore di ricerca Baidu.

Gli amministratori del search engine escludevano, tuttavia, il coinvolgimento dei propri server. Questo induceva i ricercatori a presupporre il possibile scenario dell'assalto, nel corso del quale potevano essere state coinvolte attivamente le risorse del «Grande Firewall Cinese». Tale firewall, presumibilmente, era stato utilizzato in qualità di strumento preposto a realizzare un attacco del tipo MitM (man-in-the-middle), al fine di reindirizzare i visitatori cinesi verso il sito web sottoposto ad attacco.

L'incidente qui sopra descritto dimostra ancora una volta il fatto che può essere fonte di attacchi DDoS non solo una botnet, ma anche un enorme numero di utenti del tutto ignari di quanto stia realmente avvenendo.

Una botnet formata da router

Nel secondo trimestre dell'anno in corso è stata individuata l'esistenza di una botnet composta da router domestici e router in uso presso imprese di piccole dimensioni, utilizzata dai malintenzionati per compiere attacchi DDoS.

L'infezione dei router utilizzati in ambito domestico non rappresenta, di certo, una nuova tecnica nociva, visto che essa viene di frequente sfruttata dai cybercriminali. Garantire la sicurezza delle apparecchiature utilizzate per le comunicazioni dagli utenti privati - all'interno della propria abitazione - rimane, tuttora, un preciso compito a carico del produttore di tali dispositivi. Come dimostra la pratica, esiste, in effetti, un significativo numero di vulnerabilità e di difetti di configurazione, che consente ai criminali informatici di assumere agevolmente il controllo del router domestico. Nella specifica circostanza qui esaminata, i malintenzionati hanno utilizzato i router per organizzare attacchi distribuiti Denial of Service.

La creazione di botnet composte da router appare di sicuro, agli occhi dei cybercriminali, come qualcosa di piuttosto allettante. La semplicità di realizzazione di strumenti automatizzati in grado di sfruttare le vulnerabilità individuate nei suddetti dispositivi facilita considerevolmente il compito dei malfattori; inoltre, un dispositivo costantemente connesso (sono davvero in pochi coloro che scollegano il router dalla rete) garantisce, di fatto, la presenza online di un numero elevato di bot del genere.

Statistiche relative agli attacchi DDoS condotti mediante l'utilizzo di botnet

Metodologia

Nel presente resoconto vengono riportati i dati statistici raccolti attraverso il sistema DDoS Intelligence (parte della soluzione di sicurezza Kaspersky DDoS Protection) nel periodo intercorrente tra il 1° aprile ed il 30 giugno 2015 (secondo trimestre dell'anno); tali dati vengono debitamente comparati con le analoghe statistiche elaborate riguardo al trimestre precedente.

Il sistema DDoS Intelligence è preposto ad intercettare ed analizzare i comandi che giungono ai bot dai server di comando e controllo; esso non si basa quindi, né sulle eventuali infezioni generate sui dispositivi degli utenti, né sull'effettiva esecuzione dei comandi impartiti dai malintenzionati.

Nel presente report si considera come singolo attacco DDoS un attacco nel corso del quale l'intervallo tra i periodi di attività della botnet non supera le 24 ore effettive. Così, ad esempio, nel caso in cui lo stesso identico sito web venga attaccato attraverso la stessa identica botnet con un intervallo di almeno 24 ore, saranno considerati, a livello di statistica, due attacchi DDoS separati. Vengono ugualmente ritenuti singoli attacchi DDoS quelli lanciati nei confronti della medesima risorsa web, ma eseguiti mediante bot riconducibili a botnet diverse.

L'ubicazione geografica delle vittime degli attacchi DDoS e dei server dai quali vengono inviati i comandi nocivi viene determinata in base ai relativi indirizzi IP. In questo report, inoltre, il numero degli obiettivi unici degli attacchi DDoS viene calcolato in base al numero di indirizzi IP unici presenti nell'ambito dei dati statistici trimestrali.

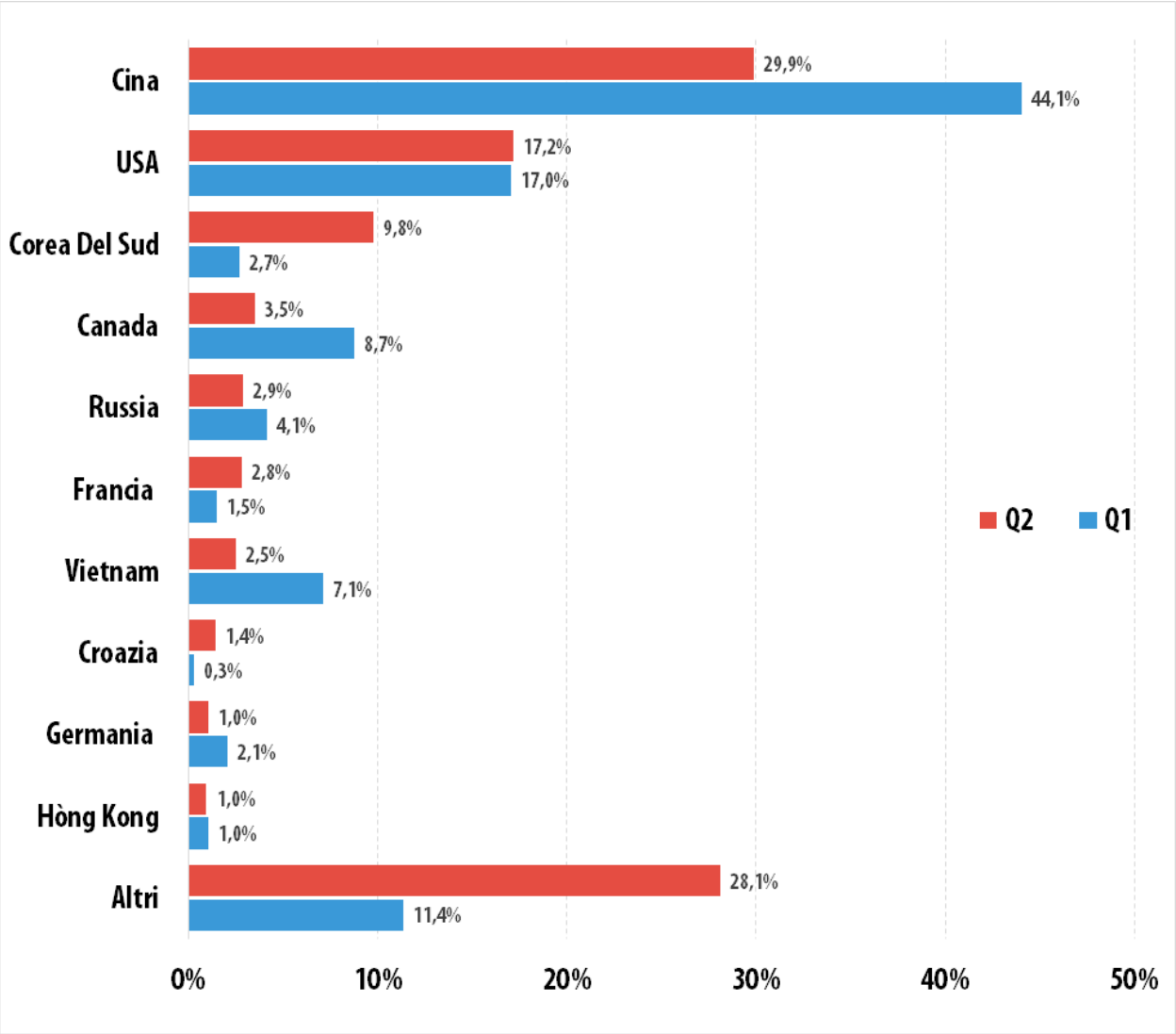
È ugualmente importante sottolineare come le statistiche ottenute grazie al sistema DDoS Intelligence si riferiscano esclusivamente alle botnet individuate ed analizzate dagli esperti di Kaspersky Lab. Occorre infine evidenziare il fatto che le botnet costituiscono soltanto uno dei possibili strumenti per mezzo dei quali possono essere realizzati gli attacchi DDoS; i dati presentati nel nostro report trimestrale non comprendono quindi, indistintamente, tutti gli attacchi DDoS compiuti nel periodo oggetto della nostra analisi.

Il trimestre in cifre

- Nel secondo trimestre del 2015 si sono registrati attacchi DDoS, condotti mediante l'utilizzo di botnet, nei confronti di "bersagli" situati in 79 diversi paesi.
- Il 77% degli attacchi eseguiti attraverso le botnet ha preso di mira risorse web ubicate in una ristretta cerchia di 10 paesi.
- Il maggior numero di assalti DDoS è risultato essere rivolto ad obiettivi situati sul territorio di Cina e Stati Uniti; rileviamo, inoltre, come al terzo posto della speciale graduatoria sia salita la Corea del Sud.
- Nel periodo oggetto del presente report, l'attacco DDoS più esteso in termini temporali si è protratto per ben 205 ore (8,5 giorni).
- SYN-DDoS e TCP-DDoS sono divenuti gli scenari più frequenti nel quadro degli attacchi DDoS eseguiti tramite botnet, mentre la tipologia HTTP-DDoS è andata ad occupare la terza posizione dell'apposito rating da noi stilato.

Geografia degli attacchi

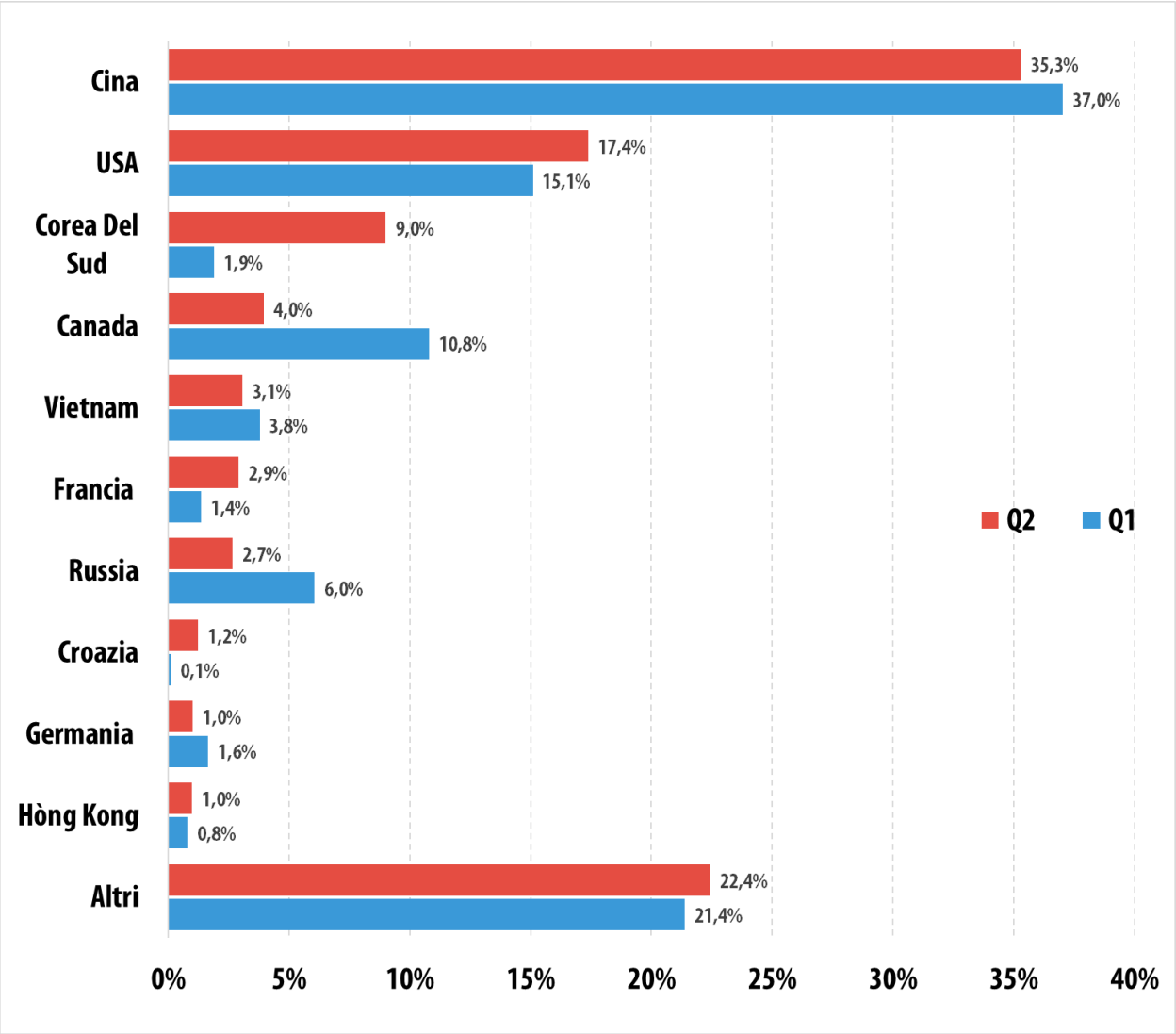
Nel secondo trimestre dell'anno in corso, la geografia "territoriale" inerente agli obiettivi sottoposti ad attacco si è leggermente "ampliata", rispetto a quanto rilevato in relazione al trimestre precedente: sono stati in effetti registrati attacchi DDoS nei confronti di "bersagli" situati in 79 diversi paesi (76 paesi nel primo trimestre del 2015). Il 71,9% delle risorse web prese di mira è risultato ubicato sul territorio di soli 10 paesi.



Ripartizione per paesi degli obiettivi unici bersagliati dagli attacchi DDoS - 1° e 2° trimestre del 2015 a confronto

La composizione della TOP-10 risulta pressoché invariata (è entrata a far parte della speciale graduatoria la Croazia, mentre hanno abbandonato le prime dieci posizioni del rating i Paesi Bassi). Le prime due posizioni della classifica continuano ad essere occupate da Cina (29,9%) e Stati Uniti (17,2%), mentre il Canada è stato scalzato dal terzo posto del ranking dalla Corea del Sud (9,8%), salita dalla sesta alla terza piazza della graduatoria.

Se si considera il numero complessivo di attacchi DDoS individuati, si osserva come il 77,6% degli stessi sia stato condotto verso il territorio dei medesimi 10 paesi:



Ripartizione per paesi degli attacchi DDoS - 1° e 2° trimestre del 2015 a confronto

Anche in questo caso la leadership del rating è detenuta da Cina (35,3%) e Stati Uniti (17,4%).

I due grafici qui sopra riportati evidenziano come in entrambe le graduatorie, rispetto al trimestre precedente, per ciò che riguarda le prime tre posizioni delle stesse, risulti diminuita la quota percentuale ascrivibile alla Cina, mentre gli indici relativi ad USA e Corea del Sud hanno invece fatto registrare un significativo incremento.

Proprio in virtù dei prezzi particolarmente contenuti che si registrano sia negli USA che in Cina riguardo all'hosting web, la maggior parte delle risorse Internet mondiali viene di fatto collocata sul territorio di questi due paesi; tale specifica circostanza fornisce quindi una logica spiegazione al fatto che Cina e Stati Uniti continuino a detenere in maniera permanente la leadership in entrambi i rating, sia nell'ambito della graduatoria riguardante il numero degli attacchi complessivamente condotti, sia all'interno della classifica che tiene invece in considerazione il numero di bersagli unici.

Nel secondo trimestre del 2015 è stato da noi osservato un repentino aumento delle attività malevole svolte da alcune famiglie di bot, attraverso le quali sono stati attaccati, in particolar modo, obiettivi

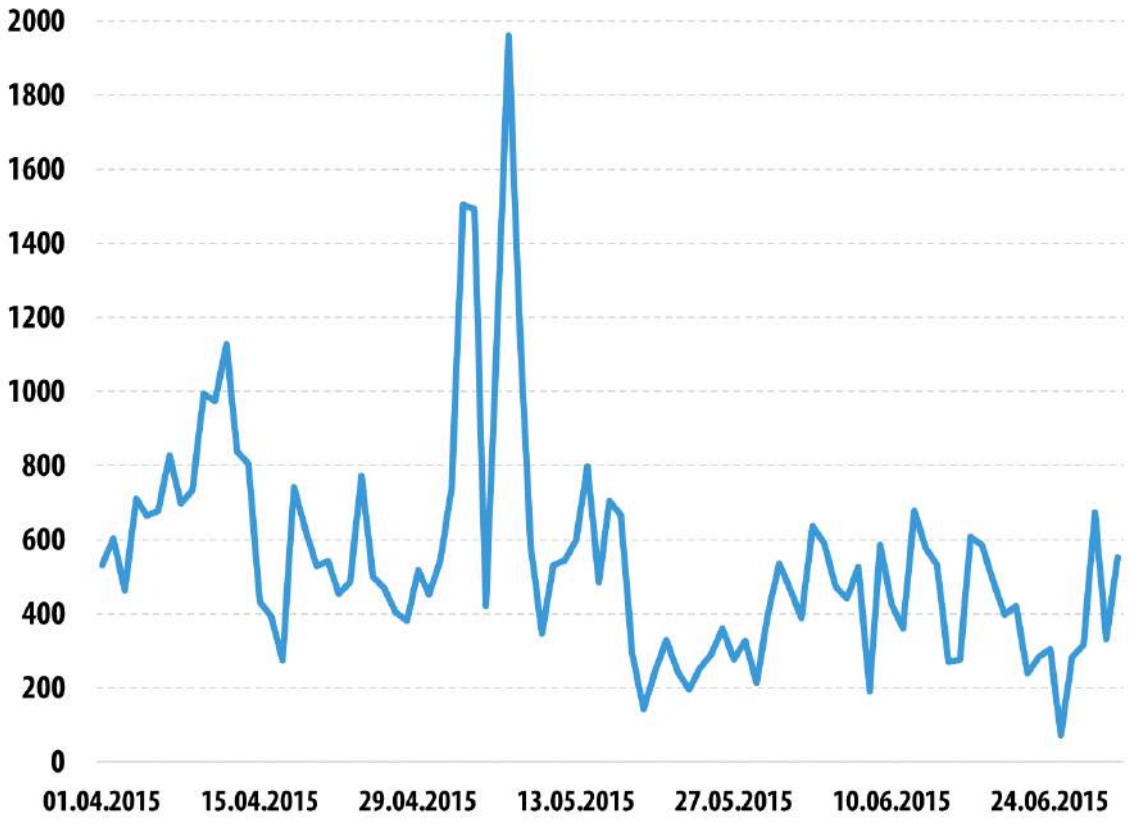
situati nella Corea del Sud. Il risultato di tutto ciò è che il paese dell'Estremo Oriente è andato ad occupare, in entrambe le graduatorie, il terzo gradino del "podio" virtuale.

Desideriamo ugualmente porre in evidenza la diminuzione degli indici percentuali relativi a Russia e Canada, particolarmente marcata soprattutto nel rating che tiene in considerazione il numero di attacchi portati verso il territorio di questi paesi.

Dinamiche relative al numero di attacchi DDoS individuati

È stato osservato un repentino aumento del numero degli attacchi DDoS nella prima settimana di maggio; il minor livello di attività è stato invece registrato alla fine del mese di giugno.

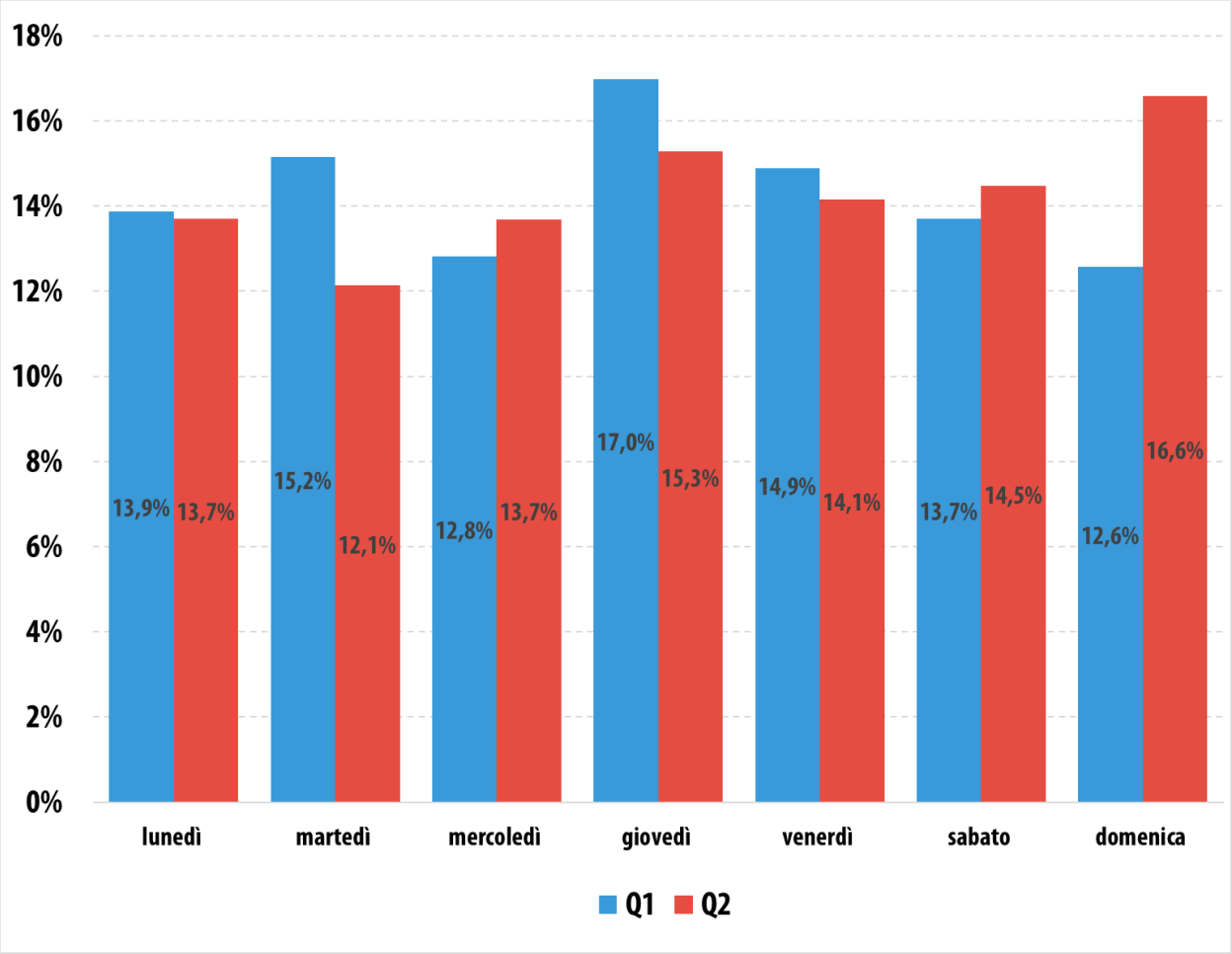
Il picco del numero di attacchi condotti nell'arco delle 24 ore si è avuto il 7 maggio scorso (1960 attacchi); la giornata in assoluto più "calma" si è invece rivelata essere il 25 giugno, quando sono stati complessivamente rilevati 73 attacchi DDoS.



Dinamiche relative al numero di attacchi DDoS - 2° trimestre 2015

**Visto che gli attacchi DDoS possono protrarsi ininterrottamente per alcuni giorni, nella relativa timeline un attacco può essere considerato varie volte (in pratica una volta per ogni singolo giorno).*

Nel secondo trimestre dell'anno, il giorno della settimana in cui è stato riscontrato il livello di attività più elevato in termini di quantità di attacchi DDoS condotti, è risultato essere la domenica (16,6% del numero complessivo di attacchi). Il minor numero di attacchi è stato invece osservato il martedì.



Ripartizione degli attacchi DDoS in base ai giorni della settimana

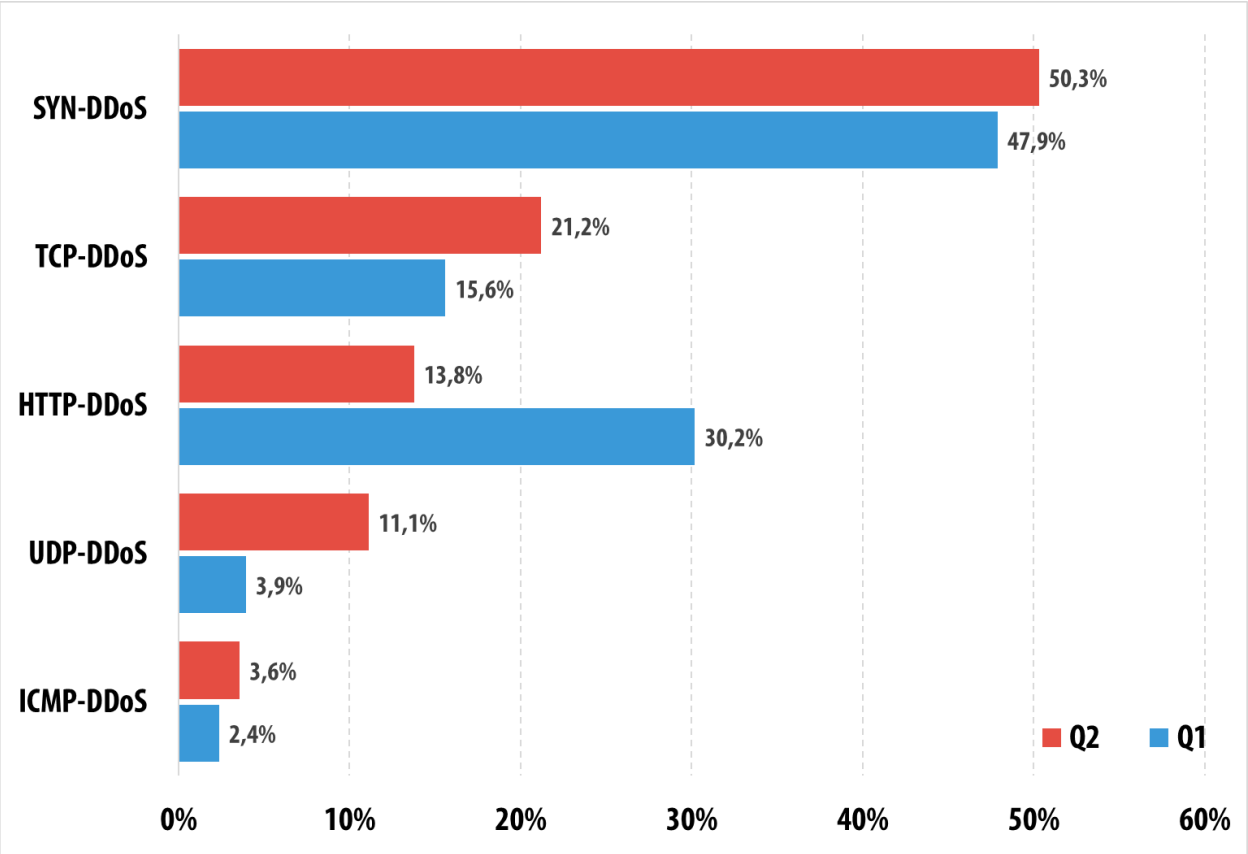
È stato da noi rilevato un forte aumento dell'attività di una delle botnet nella giornata di domenica 3 maggio. È possibile che, trattandosi di un giorno festivo, i malintenzionati abbiano provveduto a testare il funzionamento della propria botnet.

Tipologie e durata degli attacchi DDoS

L'efficacia di un attacco Distributed Denial of Service si basa essenzialmente sulla durata dello stesso e sul relativo scenario in cui esso si svolge; sono, in effetti, proprio questi elementi a determinare l'entità del danno inflitto alla vittima.

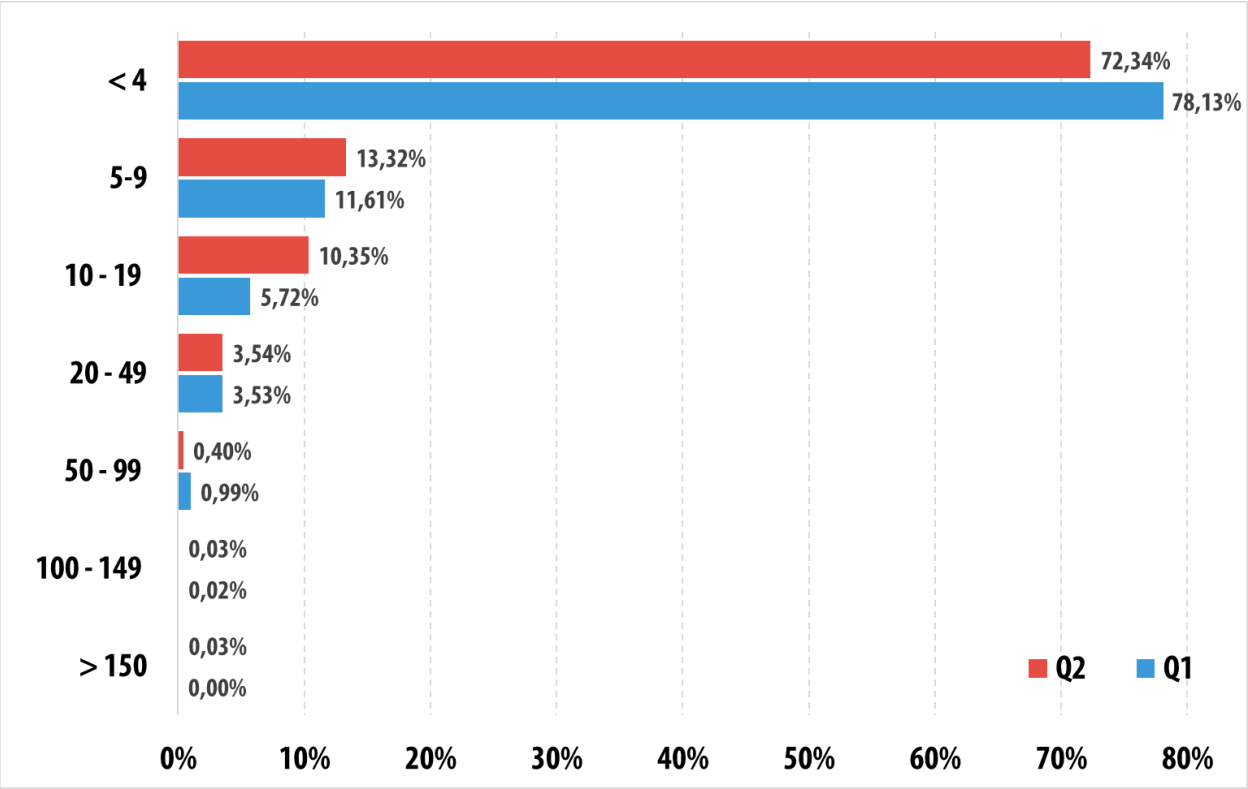
Nel secondo trimestre del 2015 il 98,2% (93,2% nel primo trimestre dell'anno) degli obiettivi è stato attaccato da bot riconducibili ad un'unica famiglia. Solo nell' 1,7% dei casi i malfattori hanno utilizzato, per condurre i loro attacchi, bot appartenenti a due diverse famiglie (oppure, nella circostanza, i committenti si sono rivolti a più esecutori); nello 0,1% dei casi, poi, si è fatto ricorso all'utilizzo di tre o più bot (nel primo trimestre, rispettivamente, 6,2% e 0,6%).

Nel secondo trimestre dell'anno in corso SYN-DDoS (50,3%) si è confermato come metodo di attacco in assoluto più diffuso; gli attacchi di tipo TCP-DDoS (21,2%), poi, sono nuovamente saliti al secondo posto della graduatoria, mentre la tipologia HTTP-DDoS (13,8%) è scesa alla terza posizione della stessa.



Ripartizione degli attacchi DDoS in base alle varie tipologie esistenti

Nel secondo trimestre del 2015 la stragrande maggioranza degli attacchi si è protratta per meno di 24 ore; ci siamo tuttavia imbattuti in attacchi DDoS che sono continuati per un'intera settimana, e anche oltre.

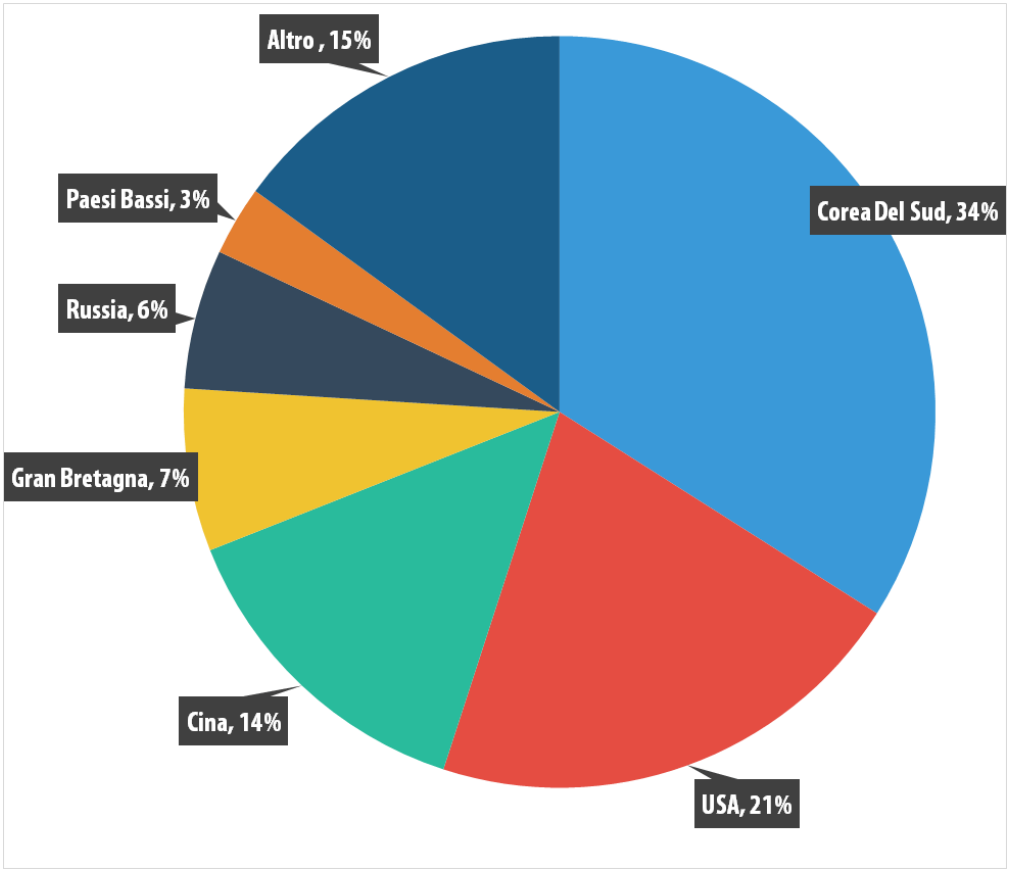


Ripartizione degli attacchi DDoS in base alla loro durata

Nel periodo oggetto del presente report, l'attacco DDoS più esteso in termini temporali si è protratto per ben 205 ore (8,5 giorni).

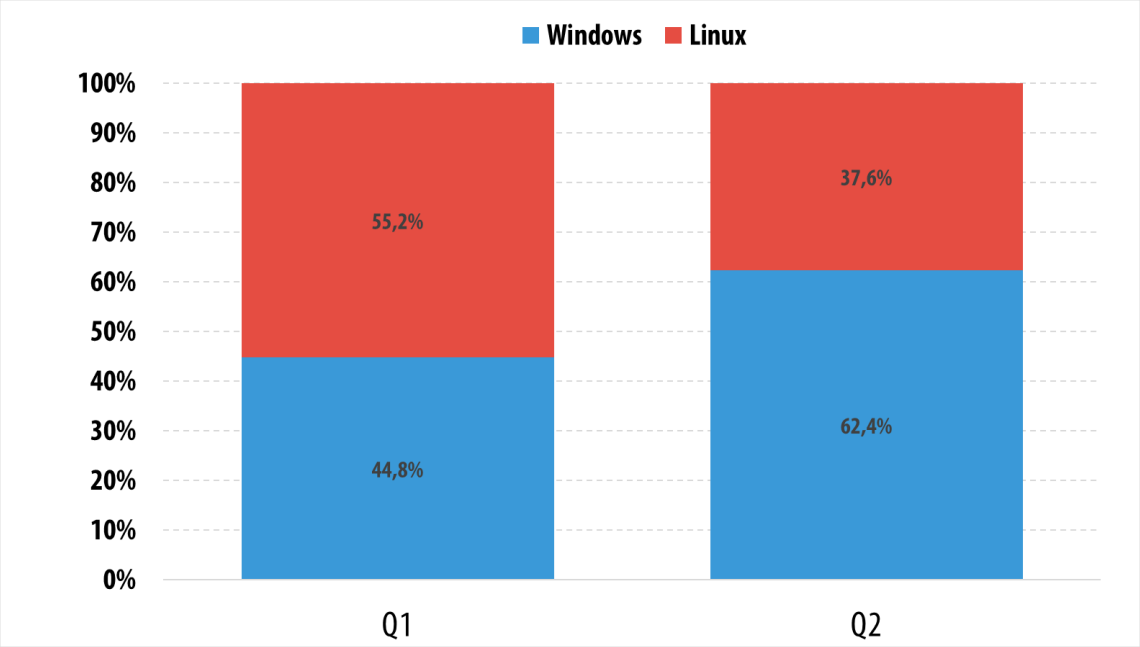
Server di comando e controllo; tipologie di botnet

Nel trimestre qui preso in esame, la leadership della graduatoria relativa al numero di server di comando e controllo dislocati sul territorio dei vari paesi - è andata ad appannaggio della Corea del Sud, con una quota pari al 34%; le posizioni di rincalzo, nell'ambito di tale classifica, risultano occupate, rispettivamente, da Stati Uniti (21%), Cina (14%) e Gran Bretagna (7%). Tale situazione è stata accompagnata, di pari passo, dal considerevole aumento del numero di attacchi DDoS e del numero di relativi bersagli individuati sul territorio della Corea del Sud.



Ripartizione per paesi dei server di comando e controllo - Situazione relativa al 2° trimestre del 2015

Nel secondo trimestre del 2015 è sensibilmente aumentato il numero degli attacchi DDoS provenienti da bot per i sistemi operativi Windows; di conseguenza, il livello di attività dei bot per l'OS Windows è risultato significativamente superiore a quello fatto registrare dai bot destinati a Linux.



Correlazione tra gli attacchi lanciati mediante botnet basate sull'OS Windows e gli attacchi eseguiti ricorrendo a botnet operanti con Linux

Vengono da noi costantemente monitorati i cambiamenti che intervengono, nel tempo, a livello di correlazione esistente tra le attività condotte attraverso le botnet basate su Linux e le botnet che invece operano con l'OS Windows; di fatto, ogni tipologia di botnet presenta, allo stesso tempo - per i cybercriminali che ne fanno uso - sia vantaggi che specifici inconvenienti.

Le botnet basate sull'OS Linux forniscono ai malintenzionati la possibilità di manipolare i protocolli di rete, mentre i server infetti sono provvisti di elevata velocità a livello di canale Internet (ciò significa che gli attacchi realizzati attraverso tali botnet risulteranno più potenti rispetto a quelli organizzati mediante botnet basate su Windows). Tuttavia, il processo di creazione e di gestione delle botnet Linux richiede non solo una buona conoscenza di tale sistema operativo, ma anche la disponibilità di un bot che si riveli adatto all'uso, reperibile sul mercato della cybercriminalità o liberamente accessibile.

I bot per l'OS Windows, da parte loro, risultano largamente disponibili sia sul mercato nero, sia a livello di libero accesso agli stessi; per la loro distribuzione vengono in effetti utilizzati meccanismi ampiamente collaudati. Sui personal computer, tuttavia, la protezione nei confronti del malware rappresenta un elemento ormai ben collaudato ed efficace (a differenza dei server Linux infetti, i quali, di solito, non presentano alcun tipo di protezione IT), per cui, su tali macchine, i bot sono destinati a non sopravvivere a lungo.

L'utilizzo di bot destinati a Windows, quindi, risulta più semplice ed economico, ma le botnet costruite grazie ad essi, in genere, hanno vita piuttosto breve. Ad ogni caso, la presenza di un elevato numero di botnet basate su Windows consente di ottenere, complessivamente, un livello di attività che supera, di fatto, quello che si può raggiungere attraverso l'utilizzo di potenti server Linux contaminati dal malware.

Attacchi complessi

Coloro che commissionano la conduzione di attacchi DDoS nei confronti di importanti società, enti ed organizzazioni, sono in genere ben disposti a spendere cifre ragguardevoli, pur di raggiungere il proprio obiettivo; tali attacchi risultano quindi ben organizzati e si distinguono per la loro particolare complessità dal punto di vista tecnico.

Nel corso del processo di neutralizzazione e respingimento di uno di tali attacchi per mezzo della soluzione di sicurezza Kaspersky DDoS Protection, gli esperti di Kaspersky Lab hanno individuato ben quattro diversi metodi utilizzati dai cybercriminali:

1. una potente "NTP amplification";
2. la "SSDP amplification", il cui uso è relativamente recente; tale metodo sta tuttavia acquistando una popolarità sempre maggiore;
3. SYN-flood;
4. HTTP Flood.

Tutti i metodi qui sopra elencati sono stati impiegati contemporaneamente, e sono risultati diretti ad alcuni componenti dell'infrastruttura presa di mira:

- Gli attacchi di tipo NTP amplification e SSDP amplification producono l'intasamento, mediante traffico parassita, dei canali riservati alla trasmissione dei dati.
- SYN-flood è un attacco rivolto all'infrastruttura, in grado di generare un elevato carico sui firewall e di provocare l'esaurimento delle risorse del sistema operativo.

- Il metodo HTTP Flood produce l'impatto di maggior efficacia sul server web, mediante la creazione di una vera e propria ondata di richieste; rispondendo a queste ultime, il server web è costretto a far uso di molte risorse hardware.

Il raggiungimento dell'obiettivo attraverso uno qualsiasi dei componenti previsti per realizzare l'attacco avrebbe significato, per i criminali, il pieno successo dell'operazione. In tal caso, l'organizzazione-vittima avrebbe sostenuto significative perdite sia dal punto di vista finanziario, sia dal punto di vista della propria reputazione. Sono occorsi ben 20 minuti, ai malintenzionati, per convincersi della solidità della protezione di cui disponeva l'organizzazione presa di mira; trascorso questo intervallo di tempo, i malfattori hanno interrotto l'attacco.

Si è trattato, nella fattispecie, dell'attacco in assoluto più potente tra quelli in cui, nel corso del secondo trimestre dell'anno, si sono imbattuti gli esperti di KDP; la potenza massima dispiegata nel corso di tale attacco ha in effetti raggiunto i 92 Gbit/sec. Attacchi di simile portata costituiscono una seria minaccia non solo per le specifiche risorse che essi prendono di mira, ma anche per i data center nell'ambito dei quali agiscono, così come per le infrastrutture dei provider Internet, visto che, ancor prima dello stesso canale Internet della risorsa sottoposta ad attacco, possono divenire angusti colli di bottiglia i canali di cui dispongono i relativi provider e i data center.

Conclusioni

Nel secondo trimestre del 2015, oltre il 77% degli attacchi eseguiti mediante botnet ha preso di mira risorse web ubicate in una ristretta cerchia di 10 paesi. Le posizioni di vertice della speciale graduatoria da noi stilata sono rimaste invariate; Cina e Stati Uniti, in effetti, continuano ad occupare il primo ed il secondo posto del rating in questione. L'apposito sistema di monitoraggio ha rilevato un repentino aumento delle attività condotte da alcune famiglie di bot; gli obiettivi di tali attività dannose sono risultati principalmente ubicati nella Corea del Sud. Ciò costituisce una logica spiegazione riguardo al terzo posto occupato dal paese dell'Estremo Oriente nell'ambito della suddetta classifica.

Se si considerano le tecnologie utilizzate per la conduzione degli attacchi, osserviamo come i criminali specializzati nella creazione di botnet DDoS - oltre a sviluppare botnet di tipo standard, composte da personal computer e server - stiano attualmente investendo nella creazione di botnet formate da dispositivi di rete; si tratta, nella maggior parte dei casi, di router e modem DSL. Evidentemente, la crescente diffusione dei dispositivi IoT e l'attuale situazione riguardo al loro livello di protezione IT fornisce un ulteriore impulso allo sviluppo di botnet del genere.

Continua nel frattempo ad accrescersi il livello di persistenza applicato dai cybercriminali agli attacchi DDoS da essi realizzati. Nel periodo oggetto del presente report sono stati in effetti rilevati attacchi la cui durata si è addirittura protratta sino a 8,5 giorni. Desideriamo sottolineare, tuttavia, come anche un "semplice" attacco di breve durata possa seriamente danneggiare una società o un'organizzazione, sia causando perdite dirette dal punto di vista finanziario, sia generando elevati rischi riguardo alla reputazione dell'azienda presa di mira.

Gli attacchi DDoS, inoltre, servono spesso come utile copertura per la conduzione di attacchi informatici mirati, volti a produrre consistenti perdite di dati sensibili di particolare importanza, oppure a realizzare il furto di cospicue somme di denaro. Il modulo DDoS scoperto dagli esperti di Kaspersky Lab, che rappresenta una parte del ricco arsenale di cui dispone il noto gruppo APT Animal Farm, conferma

ancora una volta il fatto che, per i cybercriminali, gli attacchi DDoS costituiscono uno strumento di particolare efficacia.

Al momento attuale, stanno divenendo bersaglio di attacchi DDoS le organizzazioni più diverse. Tra coloro che vengono protetti dagli esperti di Kaspersky DDoS Protection, incontriamo enti governativi, società finanziarie ed istituti bancari di primaria importanza, mass media, piccole e medie imprese, persino istituzioni didattiche.

Per difendersi in maniera efficace nei confronti di tale genere di minaccia IT è necessario elaborare per tempo sia una valida tattica che un'adeguata strategia di difesa, così come adottare tutte le opportune misure di sicurezza, quali, ad esempio, connettersi all'apposito servizio preposto al filtraggio del traffico "spazzatura"; una volta iniziato l'attacco vero e proprio, infatti, risulterà di sicuro ben più complesso cercare di evitare sostanziose perdite.