



WebBook

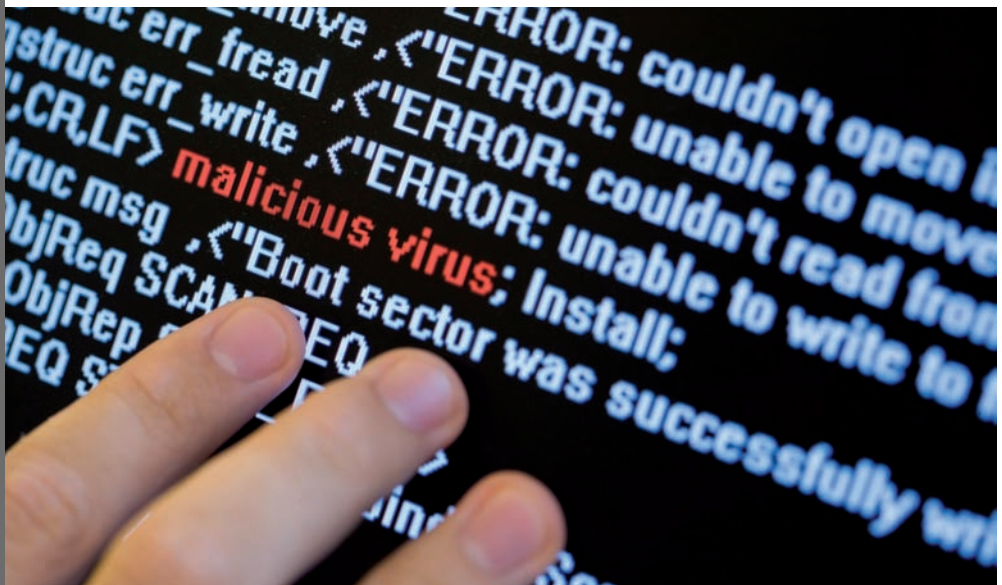
Analisi di un attacco web

Il Fenomeno di DDoS Distributed Denial of Services attack

Massimo Penco

Vice presidente Gruppo Comodo,

Presidente Associazione Cittadini di Internet



Analisi di un attacco web

Il Fenomeno di DDoS

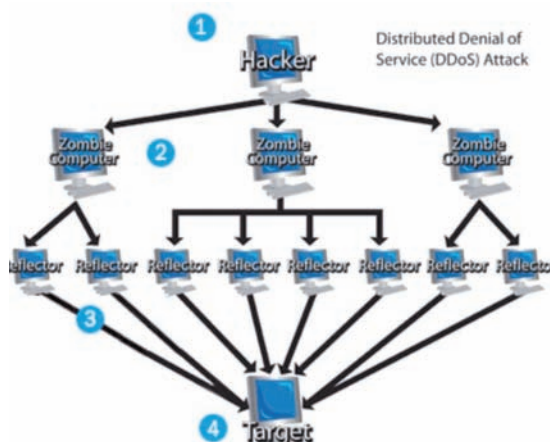
Distributed Denial of Services attack

Massimo Penco

Vice presidente Gruppo Comodo, Presidente Associazione Cittadini di Internet

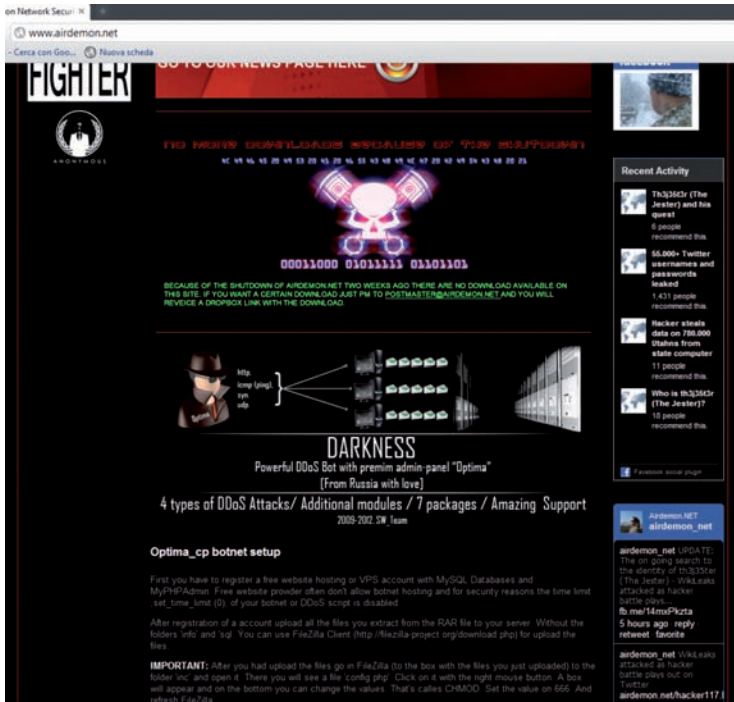
Il Fenomeno di DDoS Distributed Denial of Services attack

Si chiama *Distributed denial-of-service attacks* (Gli attacchi basati sul blocco diffuso di un servizio) e si tratta di un attacco informatico che cerca di mettere in sovraccarico di richieste un sistema e/o un sito web, fino a rendere impossibile l'erogazione dei servizi. Questi attacchi vengono messi in atto attraverso un numero estremamente elevato di pacchetti di richieste, generate da più macchine che puntano verso lo stesso server, saturandone le risorse e rendendolo instabile. In Italia, purtroppo, e in parte anche in Europa, non siamo in possesso di dati certi su questi tipi di attacchi e, come al solito, dobbiamo riferirci agli Stati Uniti.



Analisi di un attacco web

hanno scarsa esperienza tecnologica, di aggredire qualsiasi sito web on-line. Questo tipo di attacchi, ormai, non possono più considerarsi casi isolati poiché vengono compiuti da diversi tipi di organizzazioni, anche governative. Gli scopi sono di diversa natura e, sovente, sono strettamente collegati a motivi di concorrenza di mercato oppure a movimenti politici che ricorrono all'attacco informatico come forma eversiva di protesta. Una delle caratteristiche di LOIC's è "HIVE MIND," una sorta di coscienza collettiva che permette ad un singolo LOIC di controllare un intero network, distribuendo globalmente l'attacco. Di seguito l'inquietante Home di uno dei gruppi.



LOIC viene installato tramite un malware e dà la possibilità, a coloro che partecipano all'azione criminale di DDoS, di osservarne tutte le fasi. Alcuni attivisti, ad esempio quelli di "Anonymous", molto spesso usano chat on-line e Twit-

ter per dare e ricevere istruzioni sul da farsi.

I danni indiretti



Chi è convinto che il danno provocato da un qualsiasi attacco DDoS colpisca solo l'obiettivo dell'attacco si sbaglia. Siamo sempre più dipendenti dalle nuove tecnologie e dai computer, pertanto DDoS può provocare assalti che possono arrivare a bloccare un'intera nazione se non, addirittura, il mondo intero. Se, per esempio, si bloccassero improvvisamente tutti i Bancomat, si metterebbe fuori uso un intero paese e qualsiasi sistema andrebbe in tilt con enormi conseguenze sul piano economico.



Non tutti gli attacchi DDoS, però, sono perpetrati per ottenere un profitto.

I cybercriminali stanno bersagliando sempre di più le risorse governative o i siti delle grandi compagnie per dare prova della loro abilità, per dimostrare il loro potere e, in alcuni casi, ricorrono agli attacchi come forma di protesta, proprio quella alla quale i media danno più risonanza e pubblicità. I gruppi di hacker più attivi nel

secondo trimestre del 2011 sono stati [LulzSec](#) e [Anonymous](#) e, in Italia, quest'ultimo ha [un proprio blog ufficiale](#) dove dirama i suoi proclami.



Manifestazione di Anonymus contro Scientology a Los Angeles.

Analisi di un attacco web

Hanno organizzato attacchi DDos sui siti governativi degli Stati Uniti, del Regno Unito, della Spagna, della Turchia, dell'Iran, dell'Italia e di tanti altri paesi e sono riusciti a mettere temporaneamente fuori uso siti come <http://www.cia.gov/> (la *Central Intelligence Agency* americana) e www.soca.gov.uk (la Soca, *British Serious Organized Crime Agency*). Ciò dimostra come anche i siti governativi controllati e tutelati da agenzie specializzate, non sono immuni dagli attacchi DDoS.

Assaltare i siti governativi è un'attività rischiosa per gli hacker poiché attira immediatamente l'attenzione e la reazione delle autorità competenti. Nel secondo trimestre del 2011, ad esempio, più di 30 membri di *Anonymous* sono stati arrestati perché sospettati di aver lanciato attacchi DDoS sui siti governativi. In ogni caso non tutti coloro che sono coinvolti rischiano l'arresto, poiché in molti paesi la semplice partecipazione ad organizzazioni che effettuano attacchi DDoS non è ancora considerata illegale.

Una delle grandi multinazionali che hanno subito grandi assalti informatici è la Sony. Alla fine di marzo, la compagnia ha avviato un procedimento legale contro un gruppo di hacker accusandoli di aver violato il firmware della popolare console PlayStation3 ma, come accade molto spesso, oltre all'attacco DDos si è verificato anche il furto di milioni di dati sensibili, come i numeri di carta di credito degli utenti.

In risposta all'azione legale della Sony, *Anonymous* ha lanciato un attacco DDoS che ha praticamente paralizzato, per un certo periodo di tempo, tutti i siti della compagnia www.Playstationnetwork.com. Ma ciò è solo la punta dell'iceberg: secondo la Sony, infatti, durante l'attacco DDoS sono stati presi di mira i server del servizio PSN e rubati i dati sensibili di 77 milioni di utenti. Che sia stato fatto intenzionalmente o meno, l'attacco DDoS ha comunque funzionato come tattica alternativa e fuorviante al fine realizzare il furto di innumerevoli dati; un evento che ha colpito la reputazione della Sony che ha subito ripercussioni in Borsa sul proprio titolo. In questo particolare caso si può parlare di una vera e propria "guerra" da parte di *Anonymous* contro Sony, una guerra che è ancora in corso, non ultimo l'intervento di *Anonymous* attraverso la pubblicazione di tutta la [discografia di Sony video](#).

Attacchi DDoS sui social media

Il secondo trimestre del 2011 verrà probabilmente ricordato per la serie di attacchi ai danni del *social network* [Live Journal](#), attraverso l'uso massivo di reti infette botnet. Si tratta di una piattaforma molto sofisticata che vanta una grande varietà di iscritti, dalle casalinghe ai fotografi, dai piloti ai politici, che creano i loro blog personali sul sito. L'attacco è iniziato prendendo di mira giornali di natura politica, in particolare quello dell'attivista anti-corruzione [Alexey Navalny](#), il blogger che ha osato sfidare Putin.

In seguito ad analisi sofisticate si è trovata la rete botnet chiamata Optima che gli haker hanno reso pubblica diffondendola su Youtube. <http://www.youtube.com/watch?v=qhzu3gDylu8> la stessa è normalmente utilizzata negli attacchi DDoS, ultimamente perpetrati ai danni di LiveJournal.

Nel periodo tra il 23 Marzo e il 1 Aprile Optima riceve l'ordine di attacco contemporaneo contro i siti anticorruzione <http://rospil.info>, <http://www.rutoplivo.ru> e <http://navalny.livejournal.com> così come il sito della fabbrica di arredi <http://www.kredo-m.ru> e, dopo alcuni giorni, è stato attaccato anche il sito <http://navalny.livejournal.com>

Una volta impossessatesi della rete *Live Journal*, è stato facile completare l'opera e, all'inizio di aprile, il botnet Optima ha ricevuto il comando di attaccare una lunga lista di indirizzi presenti su *LiveJournal*, gran parte dei quali appartenenti a famosi blogger che trattano una vasta gamma di argomenti.

Il botnet Optima è noto sul mercato già dalla fine del 2010 e, dal tipo di codice usato, possiamo dire con certezza che i bots Optima sono sviluppati da *malware writers* di lingua russa e vengono usati soprattutto sui forum in lingua russa anche se è difficile determinare la dimensione del botnet, poiché è molto segmentato. Il botnet è una rete formata da computer collegati ad Internet e infettati da malware, controllata da un'unica entità: il botmaster. A causa di falle nella sicurezza o per la mancanza di attenzione da parte di un qualsiasi utente della rete (per esempio, non aver installato nessun antivirus nel proprio PC) o dell'amministratore di sistema di un'intera rete, i computer vengono infettati da virus informatici, o trojan, che consentono ai loro creatori di controllare il sistema da remoto. I controllori della botnet possono, in questo modo, sfruttare i sistemi compromessi all'insaputa dei rispettivi proprietari, per scagliare attacchi del tipo DDoS contro qualsiasi altro sistema in rete oppure compiere altre operazioni

Analisi di un attacco web

illecite. In alcuni casi agiscono persino su commissione di organizzazioni criminali e/o governative se non, addirittura, concorrenti. I computer che compongono la botnet sono chiamati *bot* (derivante RO-BOT) o *zombie*.

Il sistema è semplice: i *malware* creati per far parte di una botnet, non appena assunto il controllo del sistema, devono poter fornire al proprio autore i dati relativi al sistema infettato. Per fare ciò spesso sfruttano i canali IRC (*Internet Relay Chat*) e si connettono ad un dato canale, situato su un dato server, il quale spesso è protetto da una password che garantisce accesso esclusivo all'autore. Tramite il canale di chat, l'autore è in grado di controllare contemporaneamente tutti i sistemi infetti collegati al canale (i quali possono essere anche decine di migliaia) e di impartire loro degli ordini. Per esempio, con un solo comando potrebbe far partire un attacco DDoS verso un sistema a sua scelta.

Un altro sistema utilizzato dai botmaster per controllare i bot sono le reti *peer-to-peer* (tra queste è compresa la rete di Skype). In questo caso la rete p2p viene usata come veicolo per le informazioni che il botmaster invia ai bot.

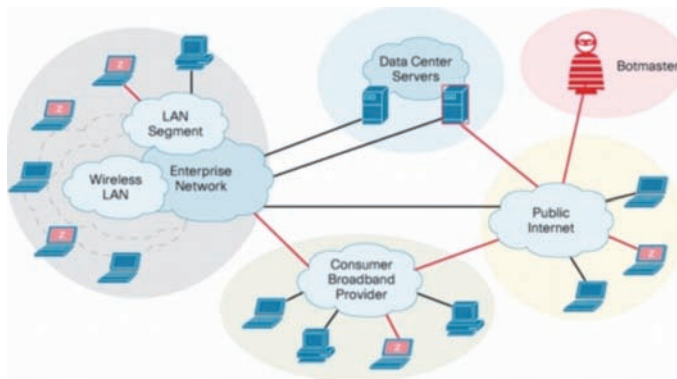
Le botnet vengono spesso utilizzate anche per altri scopi oltre al DDoS; questi virus sono spesso programmati in modo da spiare il sistema infetto e intercettare password ed altre informazioni utili. Possono, inoltre, offrire accesso alle macchine infette tramite *backdoor* oppure servizi *proxy*, che garantiscono l'anonimato in rete.

Infine, un altro uso delle botnet è come proxy verso un sistema compromesso. I bot, infatti, spesso vengono "ripuliti" e, di fatto, non fanno parte più della botnet. Se un pirata installa un server su una di queste macchine e ne perde il controllo il danno è grave. Una tecnica usata recentemente è quella del *fastflux* [1] in cui una macchina fuori dalla botnet fa girare un finto server (per esempio per fare *spoofing*) e le macchine della botnet fungono solo da proxy verso questa macchina.

Si sono notati casi di bots Optima, che è ormai venduto on-line dai propri sviluppatori, in cui è evidente una fase continua di implementazione del malware; basti vedere la relativa "pubblicità" qui di seguito.



Il gruppo cha ha attaccato *Live Journal* con questa tecnica ha ricevuto comandi per scaricare altri programmi dannosi in quantità rilevante. Ciò indica che il [bot-net Optima](#) include decine di migliaia di macchine infette, poiché questi *downloads* sono considerati inutilizzabili per [botnets](#) di piccole dimensioni.



Nell'immagine tipica rete di Botnet

Le ragioni degli attacchi a *LiveJournal* restano inspiegabili dal momento che ancora nessuno li ha rivendicati. Fino a quando i cyber-criminali responsabili non verranno identificati, sarà difficile stabilire se gli attacchi fossero comandati da un'organizzazione precisa o si sia trattato di semplici azioni intimidatorie in modalità random.

Analisi di un attacco web

Gli attacchi DDoS ai social media stanno diventando più frequenti, poiché tali servizi consentono l'immediato scambio di informazioni tra decine di migliaia di utenti. Bloccare questo processo, anche se solo per breve tempo, è possibile solo con l'aiuto di attacchi DDoS.

Un sistema botnet recentemente alla ribalta delle cronache è un sistema che si credeva immune da questo tipo di attacchi: il MAC della Apple. Almeno 600.000 Mac sono stati infettati dal [trojan Flashback](#) che li ha trasformati in altrettanti membri di un'inedita botnet della Mela. Questo malware è noto almeno dall'anno scorso, ma solo di recente la sua viralità è esplosa, a causa di una versione che può installarsi senza che l'utente debba inserire le proprie credenziali.

Apple è intervenuta relativamente in fretta per risolvere il problema, pubblicando un aggiornamento di sicurezza anche se, a quanto pare, il malware ha avuto il tempo di diffondersi su un buon numero di computer.

Il nostro pc può divenire il nostro peggior nemico

Non auguro a nessuno di divenire, seppur inconsapevolmente, parte di un attacco DDoS! Che la nostra macchina venga infettata e vada a fare parte, nostro malgrado, di quelle centinaia di migliaia di altri PC che attaccano, magari, un ente governativo è assolutamente possibile. Divenire parte inconscia di una Botnet, infatti, non è certo un gioco. Il proprio PC diviene, così, il peggior nemico che osserva, copia e trasmette ogni singola operazione dell'utente. Ma cosa vuol dire, realmente, divenire parte inconscia di un Botnet? E, soprattutto, cosa si può fare per risolvere il problema? Purtroppo fino a quando non ci si accorge di tale problema rischiamo di divenire complici inconsci di un crimine informatico, con tutte le conseguenze del caso e le relative implicazioni di carattere penale.

Come si fa a determinare se il proprio PC sia divenuto parte di una botnet? E, in tal caso, come comportarsi? Qualora non si abbia sufficiente esperienza in merito, l'unica cosa da fare per dimostrare la propria estraneità ai fatti è sporgere una denuncia presso la Polizia postale.

Intervenire, infatti, sul proprio PC, quando lo stesso è nella botnet, vuol dire compromettere eventuali prove; un po' come alterare la scena di un crimine. Prendere provvedimenti a posteriori è piuttosto difficile e lanciare degli antimalware

in un PC già compromesso non fa che peggiorare le cose. Esiste un numero piuttosto vasto di prodotti che vengono pubblicizzati come risolutori di problemi come questo ma, di fatto, non sono così efficaci poiché nessuno potrà dirci quanti dei nostri dati siano finiti nella botnet, dati che potrebbero anche essere usati per fini estorsivi.

On demand DDoS business model

Le organizzazioni criminali che si occupano di DDoS si evolvono divenendo “for-profit”: ecco un bel software per calcolare il prezzo per le estorsioni.



Direi che le richieste di denaro per attacchi DDoS stanno diminuendo. Ciò ha provocato, da parte dei gruppi interessati, una sorta di standardizzazione di questo losco mercato attraverso delle vere e proprie applicazioni software verticali, in special modo per i nuovi adepti. Si tratta di una vera e propria industrializzazione di questo crimine informatico dal quale scaturisce un vero guadagno. Ecco un esempio, in lingua originale, di una richiesta di denaro ai fini dell'estorsione:

“Hello. If you want to continue having your site operational, you must pay us 10 000 rubles monthly. Attention! Starting as of DATE your site will be a subject to a DDoS attack. Your site will remain unavailable until you pay us.

The first attack will involve 2,000 bots. If you contact the companies involved in the protection of DDoS-attacks and they begin to block our bots, we will in-

Analisi di un attacco web

crease the number of bots to 50 000, and the protection of 50 000 bots is very, very expensive.

1-st payment (10 000 rubles) Must be made no later than DATE. All subsequent payments (10 000 rubles) Must be committed no later than 31 (30) day of each month starting from August 31. Late payment penalties will be charged 100% for each day of delay.

For example, if you do not have time to make payment on the last day of the month, then 1 day of you will have to pay a fine 100%, for instance 20 000 rubles. If you pay only the 2 nd date of the month, it will be for 30 000 rubles etc. Please pay on time, and then the initial 10 000 rubles offer will not change.

Penalty fees apply to your first payment - no later than DATE”

You will also receive several bonuses.

1. 30% discount if you request DDoS attack on your competitors/enemies. Fair market value ddos attacks a simple site is about \$ 100 per night, for you it will cost only 70 \$ per day.

2. If we turn to your competitors / enemies, to make an attack on your site, then we deny them.

Payment must be done on our purse Yandex-money number 41001474323733. Every month the number will be a new purse, be careful. About how to use Yandex-money read on www.money.yandex.ru. If you want to apply to law enforcement agencies, we will not discourage you. We even give you their contacts: www.fsb.ru, www.mvd.ru”

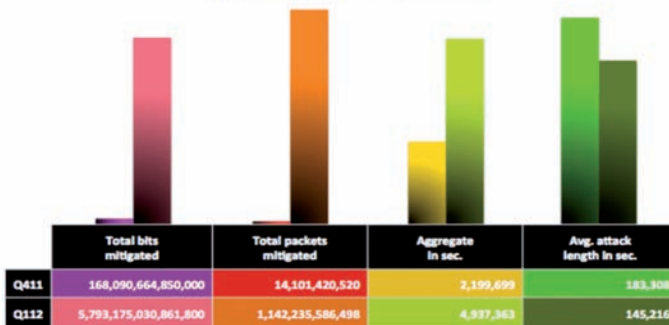
Il futuro degli attacchi DDoS si sta espandendo su larga scala. L'ultima invenzione si chiama [Ransomware](#), ed è un attacco con richiesta di denaro diretta ad un numero illimitato di utenti ai quali si presentano schermate come quella di seguito riportata. Si tratta di un sistema estorsivo molto efficiente focalizzato sui grandi numeri e, in pratica, funziona con la semplice “regola” del “se vuoi essere lasciato in pace, pagami!”.



Attacchi a Istituzioni Finanziarie

Le Istituzioni finanziarie hanno subito un incremento di attacchi di *denial of service* (DDoS) su grande scala del 25 % durante il primo trimestre 2012, in comparazione con un analogo periodo del 2011. Il mese di gennaio ha visto un incremento degli attacchi del 41% per l'intero trimestre 2012. Il numero è poi diminuito fino a marzo che è stato il mese con il minor numero di assalti. Durante il primo trimestre 2012 se ne è registrato, invece, un significativo incremento, finalizzato ad attaccare qualsiasi tipo di istituzioni finanziarie. Infatti, il numero totale di attacchi contro queste ultime, negli Stati Uniti, è aumentato di tre volte se confrontato con il primo trimestre del 2011. La misurazione del traffico malevolo nei confronti di questo tipo di istituzioni ha raggiunto il picco di 65TB di dati e 1.1 trilioni di pacchetti di dati che sono stati individuati e “sedati”.

Key Metrics Q1 2012: Financial Services



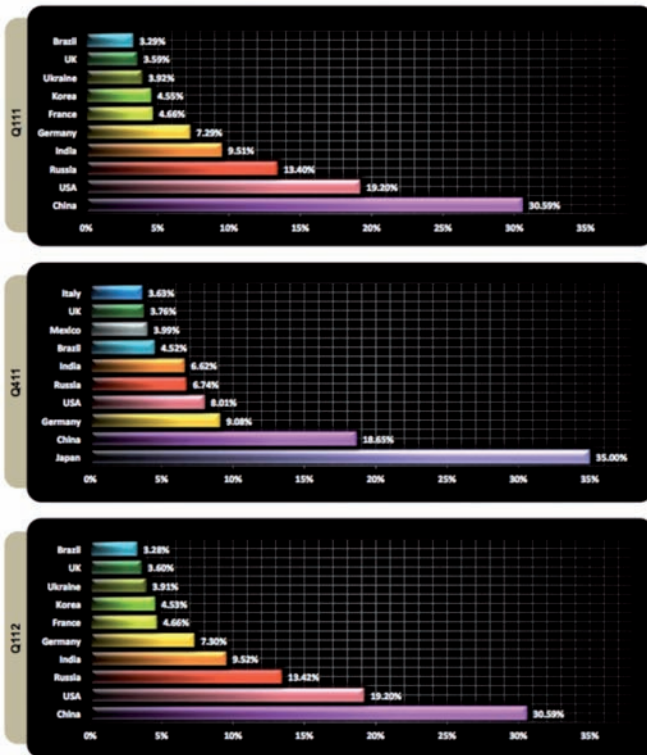
Comparazione degli attacchi ultimo trimestre 2011 e primo trimestre 2012.

Una delle domande che si pone è: da dove vengono questo tipo di attacchi e da dove, geograficamente, sono generati? E' molto difficile stabilire quale sia la provenienza di un attacco e, in base ad approfondite analisi forensi, nei primi

Analisi di un attacco web

tre mesi del 2012 il traffico malevolo generato e verificato ammonta alla cifra spaventosa di 2.9 milioni di indirizzi IP coinvolti.

Solo la Cina rappresenta circa un terzo di tutti i luoghi d'origine di attacchi *denial-of-service*, nel primo trimestre del 2012, seguita dagli Stati Uniti e dalla Russia che, insieme al paese del Sol Levante, sono le tre principali fonti di provenienza degli attacchi con un aumento sostanziale di IP coinvolti. Nell'ultimo trimestre del 2011 il Giappone aveva superato tutti con il 35% di indirizzi IP coinvolti in attacchi DDoS, da ottobre a dicembre.



I paesi dove sono stati rilevati computer compromessi da attacchi DDoS nel 2011 e nel primo trimestre del 2012.

Attacchi DDoS commerciali

Anche i criminali ordinari continuano a compiere attivamente attacchi DDoS. Comunque, le informazioni sugli attacchi che mirano ad estorcere o a ricattare le organizzazioni, raramente sono rese pubbliche e, quando lo sono, lo scopo è, generalmente, quello di favorire le necessarie indagini.

Ad aprile scorso, un tribunale di Düsseldorf ha emesso una sentenza nei confronti di un cyber-criminale che ha tentato di ricattare sei *bookmakers* tedeschi durante la Coppa del Mondo del 2012. Il colpevole ha utilizzato e messo in atto la solita “procedura” in casi come questi: intimidazione, tentato attacco sul sito della vittima e un messaggio contenente una richiesta di riscatto. Tre dei sei uffici hanno acconsentito al pagamento del riscatto. Secondo le dichiarazioni dei *bookmakers*, poche ore di *crash* del sito hanno provocato una perdita di 25/40,000 euro per gli uffici maggiori e 5/6,000 euro per quelli minori. A sorpresa, il truffatore ha chiesto solo 2,000 euro e ha ricevuto il denaro in *U-cash vouchers* (un metodo già utilizzato dall'autore del noto programma [GpCode Trojan](#)) e, attraverso i medesimi mezzi, si è riusciti ad individuare il colpevole e ad arrestarlo. Il tribunale ha inflitto all'imputato una pena di quasi tre anni di carcere (il primo caso nella storia legale tedesca di carcerazione per attacchi DDoS) e tali assalti sono ora classificati dal sistema giudiziario tedesco come “sabotaggi informatici” e sono punibili anche con 10 anni di reclusione.

A giugno, anche il sistema giudiziario russo ha affrontato la questione degli attacchi DDoS. Il 24 giugno, un tribunale moscovita ha stabilito la carcerazione di [Pavel Vrublevsky](#), noto multimilionario proprietario di [ChronoPay](#), il più grande provider di servizi di pagamento in Russia. Vrublevsky era accusato di avere organizzato un attacco DDoS contro l'impresa concorrente, la [Assist](#), allo scopo di penalizzarla nel contesto di una gara d'appalto per un contratto vantaggioso avente come oggetto il sistema dei pagamenti di [Aeroflot](#), la maggiore compagnia aerea russa. Fonti vicine agli investigatori hanno dichiarato che Vrublevsky era anche considerato il proprietario della rete affiliata *Rx-Promotion*, specializzata nello *spamming* di prodotti farmaceutici. Questo è un tipico esempio di uso di attacchi informatici per battere la concorrenza e ce ne sono molti esempi in tutto il mondo anche perché, come ho già ribadito, questo tipo di attacco, in alcuni paesi, spesso non è perseguibile per legge.

Analisi di un attacco web

Attacchi DDoS a Compagnie aeree e centri prenotazioni per il trasporto

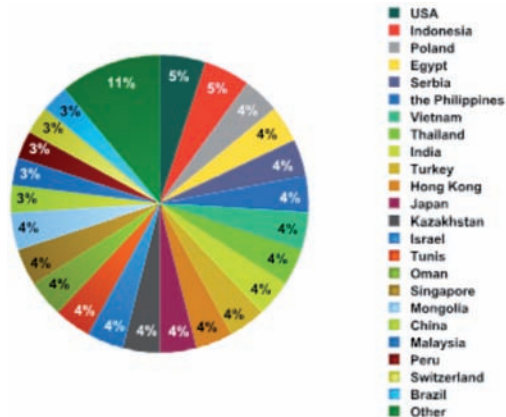
Molti anni fa mi occupai di quello che può essere considerato uno dei primi attacchi DDoS ai danni di un centro-prenotazione di una nota compagnia aerea. Fu molto semplice realizzarlo anche perché il numero di accessi on-line era piuttosto limitato. In pratica si trattò di saturare le prenotazioni su più aerei in modo da farli partire semivuoti. All'epoca fu un evento che fece scalpore e la IATA, l'associazione che riunisce le compagnie aeree di tutto il mondo, allertò tutte le associate che capirono la gravità di una minaccia come questa. All'epoca, infatti, stavano lavorando per far sì che il sistema di prenotazione on-line sostituisse la classica prenotazione presso l'Agenzia di viaggio, risparmiando sulle commissioni. Oggi questa pratica è una realtà consolidata, visto che difficilmente ci si rivolge ad un'agenzia di viaggi per l'acquisto di un biglietto aereo o ferroviario, ma anche le altre aziende di trasporto, che investono con cifre ragguardevoli, hanno cercato in tutti i modi di realizzare sistemi a prova di DDoS che rappresenta il loro tallone d'Achille.

Particolare menzione merita l'attacco ad [un'istituzione come il Vaticano](#); un tipo di assalto che non credo abbia scopi truffaldini, tantomeno religiosi. ma è l'ennesima dimostrazione che nessuno è immune da questo tipo di pericoli.

Risultati statistici

Distribuzione degli attacchi DDoS nei singoli paesi

In base alle statistiche relative al secondo trimestre del 2011, l'89% del traffico DDoS è stato generato in 23 paesi.



Distribuzione degli attacchi DDoS nei singoli paesi nel secondo trimestre del 2011. (Come si nota manca l'Italia, non perché non abbia subito gli attacchi, ma perché manca la fonte d'informazione).

La maggior parte degli attacchi, come si vede, ha interessato gli Stati Uniti e l'Indonesia, che rappresentano, ognuno, il 5% dell'intero traffico DDoS.

La posizione leader degli USA è dovuta anche alla presenza di un gran numero di computer nel paese. Le autorità di polizia americane hanno promosso una vittoriosa campagna anti-botnet che ha portato alla chiusura di un certo numero di botnet. È possibile, tuttavia, che i cybercriminali proveranno a ripristinare le capacità del botnet andate perdute e che il numero degli attacchi DDoS aumenti.

Nel frattempo, il grande numero di computer infetti in Indonesia indica che anche questo paese si trova in alto nella classifica dei paesi più interessati dal traffico DDoS. Nel secondo trimestre del 2011, quasi tutti i PC monitorati in rete in Indonesia (il 48%), sono stati oggetto di tentativi di infezione da parte di malware locali. Una percentuale così alta di manovre bloccate è il risultato della mancata protezione di un gran numero di computer utilizzati da coloro che difendono malware.

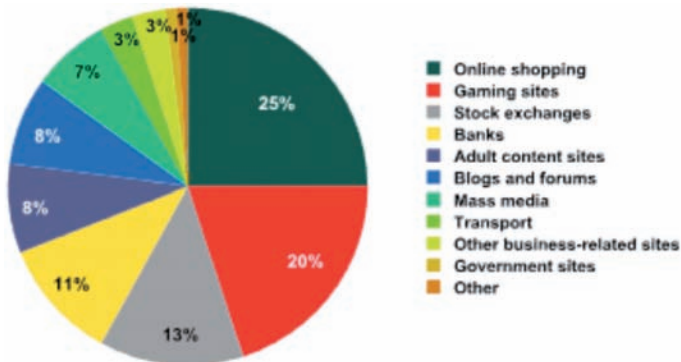
Tra i paesi responsabili per meno del 3% di tutto il traffico DDoS sono inclusi quelli dotati di alti livelli di computerizzazione e sicurezza informatica (Giappone,

Analisi di un attacco web

Hong Kong, Singapore), così come quelli in cui il numero di computer per ogni persona è significativamente più basso e la protezione antivurs è tutt'altro che perfetta (India, Vietnam, Oman, Egitto, Filippine, etc.).

Distribuzione degli attacchi ai danni di siti web attraverso attività on line

Sempre nel secondo trimestre del 2011, siti commerciali, compresi negozi on-line, aste, annunci di vendita e di acquisto, sono stati progressivamente bersagliati da cybercriminali. I siti web di questa categoria rappresentano un quarto di tutti gli attacchi. Un dato poco sorprendente: il commercio *on line* dipende ampiamente dalla fruibilità del sito e ogni ora di guasto corrisponde ad una perdita di clientela e, dunque, di profitto. Ciò spiega perché questo tipo di siti viene attaccato più spesso e, di solito, dietro questi attacchi si celano aziende concorrenti oppure azioni studiate per compiere estorsioni dirette.



*Danni relativi a siti attaccati in base alle aree di attività.
Secondo trimestre del 2011.*

I siti per il gioco *on line* rappresentano invece il secondo target. La maggior parte degli attacchi ha colpito [Eve online](#) (che ha una nutrita schiera di seguaci anche in Italia) e il suo sito web. [The MMORPG space-themed game](#) contava 357.000 giocatori attivi alla fine del 2010. Un sito in particolare, che pubblica

news di *EVE Online*, ha subito uno dei più prolungati attacchi da parte dei bots DDoS, durato ben 35 giorni. Anche [WoW](#) e [Lineage](#) hanno subito la stessa indesiderata attenzione da parte dei cybercriminali e ad avere la peggio sono stati i vari server di giochi pirata che clonavano i rispettivi legittimi proprietari; una sorta di ritorsione, che ritengo non volontaria, da parte delle *software house* produttrici.

I siti web di ricambi elettronici e delle banche occupano, rispettivamente, il terzo e il quarto posto. I cybercriminali attaccano le piattaforme standard di mercato ormai comuni a tutte le industrie e distributori di *automotive* per disperdere le tracce dopo aver effettuato transazioni fraudolente, molto spesso anche per estorcere denaro.

Le organizzazioni finanziarie, così come i loro clienti, subiscono non solo notevoli perdite di denaro, dovute all'interruzione del servizio, ma anche di credibilità e, molto spesso, anche di utenti che scelgono di rivolgersi altrove per essere più sicuri. Per questo, la protezione di un servizio contro gli attacchi DDoS è un elemento che condiziona fortemente la fiducia dei clienti e la reputazione dell'istituzione finanziaria.

È interessante il dato che una sostanziale parte degli attacchi DDoS sia stata rivolta contro siti di mass-media (7%), blog e forum (8%), che rappresentano, essenzialmente, una forma di "social mass-media". C'è sempre qualcuno che contrasta la libertà di espressione e sembra che gli attacchi DDoS siano usati anche come mezzo di censura e/o blocco contro i canali di informazione, a volte utilizzati anche da regimi repressivi.

I siti governativi costituiscono l' 1% di tutti gli attacchi, anche se questa statistica non comprende quelli compiuti dal gruppo *Anonymous*, attraverso il "voluntary botnet", basati su LOIC¹, un programma utilizzato per organizzare gli attacchi DDoS. Tali assalti vengono sempre di più utilizzati per avanzare proteste contro gli enti di governativi in molti paesi, e ci si aspetta che, in futuro, aumentino ulteriormente, specialmente nelle fasi cruciali dei processi politici in

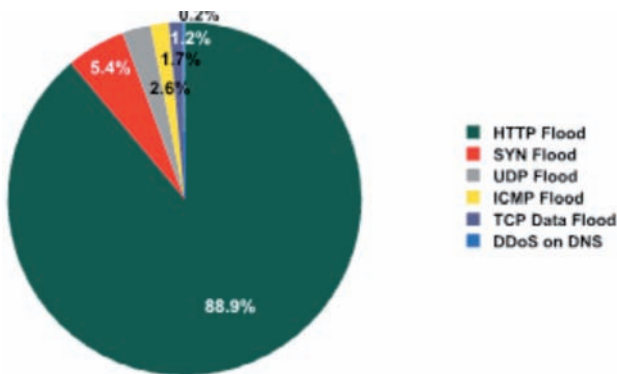
¹ **LOIC** (un acronimo per **Low Orbit Ion Cannon**, in italiano: cannone ionico di *orbita inferiore*) è un software open source per generare grandi quantità di traffico di rete (richieste) verso un sistema target e testare la sua risposta sotto carico, scritto in C#. LOIC è stato sviluppato inizialmente da Praetox Technologies.

Analisi di un attacco web

alcuni paesi, come già è avvenuto nel Nord Africa poco tempo fa.

Tipi di attacchi DDoS

Sempre nello stesso periodo esaminato, i sistemi di monitoraggio di botnet hanno fermato oltre 20.000 comandi *web-borne*, prima che portassero a termine attacchi ai danni di vari siti.



Tipo di attacchi DDoS nel secondo trimestre del 2011.

Il [Flood HTTP](#)² è il metodo più popolare (88.9%) di attacchi ai siti web: un vastissimo numero di richieste HTTP viene inviato al sito preso di mira per un breve periodo. Nella maggior parte dei casi appaiono come richieste di utenti regolari e risulta così più difficile filtrarle. Ciò rende questo tipo di attacco più comune degli altri tra i cybercriminali.

Gli attacchi Flood SYN³ rappresentano il secondo tipo di attacchi più comune (5.4%). Nel corso di queste azioni, i botnets inviano pacchetti di dati multipli al

² Nella terminologia informatica, con *flood* si indica l'invio a grande velocità di una serie di messaggi o pacchetti oppure il continuo abuso di messaggi non inerenti ad un determinato argomento prestabilito. Il termine inglese *flood* significa, letteralmente, alluvione, inondazione.

³ Il *SYN flood* è un attacco di tipo *denial of service* nel quale un utente malevolo invia una serie di richieste SYN verso il sistema oggetto dell'attacco. Quando un client cerca di iniziare una con-

server per stabilire una connessione TCP. I cybercriminali manipolano questi pacchetti in modo tale che le connessioni al server restino aperte a metà anziché essere stabilite completamente. Siccome un server può mantenere aperto solo un limitato numero di connessioni nello stesso tempo e i botnets possono generare moltissime richieste in periodi di tempo brevi, il server preso di mira sarà presto incapace di accettare connessioni da qualsiasi altro tipo di utenti.

Gli attacchi DDoS ai server DNS (0.2%) sono gli ultimi tra le tipologie più comuni. In seguito a questo tipo di azione i server DNS diventano incapaci di convertire i nomi dei siti in indirizzi IP, in modo che il sito servito dal server preso di mira diventi non disponibile per gli utenti. Questo tipo di attacco risulta particolarmente dannoso perché un singolo attacco può mettere fuori suo centinaia e, addirittura, migliaia di siti contemporaneamente.

Durante un attacco DDoS ad una fonte web, i bots ricevono il comando di inviare una richiesta ad una media di due pagine web sul sito preso di mira. Se confrontiamo il numero di attacchi indirizzati ai nomi dei siti con quelli indirizzati ad indirizzi IP, risulta che ad essere attaccati sono maggiormente gli indirizzi IP: oltre il 72% di tutti gli attacchi.

nessione TCP verso un server, il client e il server scambiano una serie di messaggi che di norma è così articolata:

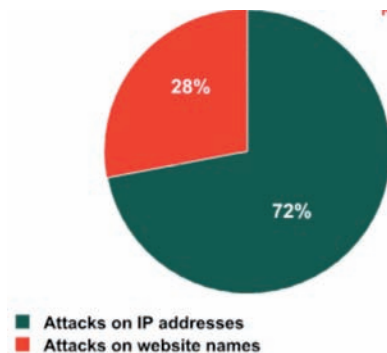
Il client richiede una connessione inviando un messaggio SYN (synchronize) al server.

Il server acknowledges, cioè risponde a tale richiesta inviando un messaggio SYN-ACK indietro al client, che infine,

Risponde con un ACK e la connessione è stabilita.

Tale processo è chiamato TCP three-way handshake e costituisce il fondamento per ogni connessione stabilita utilizzando i protocolli TCP/IP.

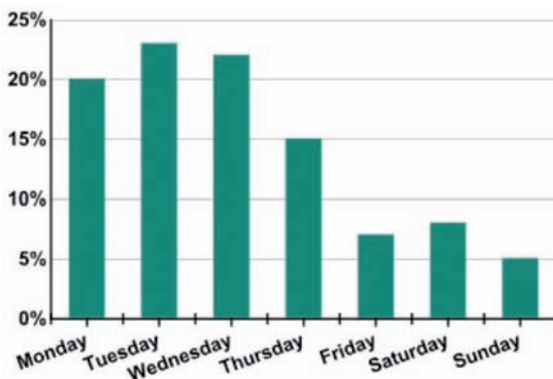
Analisi di un attacco web



Danni dovuti ad attacchi DDoS in base all'obiettivo nel II trimestre del 2011: nomi dei siti verso indirizzi IP.

Attività dei botnets nel tempo

Dopo aver analizzato tutti i dati disponibili, si può stabilire in quali giorni della settimana i cybercriminali preferiscono compiere i loro attacchi contro i siti web.



Danni ai siti in seguito ad attacchi DDoS in base al giorno della settimana. Il trimestre del 2011.

I giorni feriali sono quelli caratterizzati da un uso più intenso di internet. Ed è

proprio in questi giorni che la probabilità che gli attacchi DDoS arrechino il maggior numero di danni ai siti web si fa più alta. Un altro importante fattore è che il maggior numero di computer viene acceso nei giorni infrasettimanali, per cui ci sono più bots attivi. Di conseguenza, l'attività dei cybercriminali raggiunge il picco massimo dal lunedì al giovedì, che sono proprio i giorni in cui si verifica l' 80% di tutti gli attacchi DDoS

Conclusioni

Gli attacchi DDoS sono stati a lungo usati per scopi criminali ma, recentemente, sono sempre di più utilizzati come forma di protesta contro le attività sia dei governi, sia delle grandi aziende multinazionali. Questi attacchi ottengono moltissima pubblicità dai mass media e sono oggetto d'investigazioni da parte delle autorità. Ci si aspetta di assistere ad un progressivo aumento della popolarità dei siti governativi che subiranno attacchi di protesta DDoS. Ciò non significa, tuttavia, che gli attacchi DDoS non siano più utilizzati per scopi estorsivi o ricattatori. Le vittime, comunque, raramente riconoscono pubblicamente tali incidenti, sovente per difendere la propria reputazione. I cybercriminali, inoltre, usano sempre di più questi attacchi come tattica di distrazione mentre, nel frattempo, lanciano altri assalti più sofisticati, come quelli ai danni di sistemi bancari *on line* che possono comportare significative perdite per le istituzioni finanziarie, così come per i loro clienti. La maggior parte dei siti web in cui ci si è imbattuti in conseguenza agli attacchi DDoS ha bisogno di una protezione molto più forte. Specialmente in considerazione dell'approssimarsi dell'estate e, a breve, verrà messo in funzione nuovamente un gran numero di computer, soprattutto macchine *zombie* controllate da botmasters che effettueranno solo attacchi DDoS più potenti e dannosi. E proprio di questi giorni la notizia di uno dei più organizzati sistemi di botnet in Russia con oltre 6 milioni di computer interessati, c'è quindi da considerare con serietà questo fenomeno che può potenzialmente fermare un'intera nazione o interi sistemi che sono sempre più globalizzati, con conseguenze inimmaginabili.

Una iniziativa

Edisef srl
Via G. B. Falda, 3
00152 Roma
T. 06.5895104
F. 06.58179316

info@edisef.it