

Le tensioni politiche tra Georgia e Russia scatenano un attacco DDoS

Recentemente il sito internet della Presidenza della Georgia è stato vittima di un attacco DDoS (Distributed Denial of Service), sferrato presumibilmente per motivazioni politiche.

Lexington, Mass, 23 Luglio 2008 – Durante lo scorso weekend, il sito ufficiale della Presidenza - www.president.gov.ge – è stato reso inaccessibile per circa 24 ore. Un'analisi dell'attacco condotta da Arbor Networks, azienda leader nella fornitura di soluzioni di controllo dei servizi per le reti globali, indica che l'attacco è molto probabilmente di origine russa ed è la conseguenza delle recenti tensioni politiche tra Georgia e Russia.

Jose Nazario, Chief Analyst di Arbor Networks, commenta: "Questo attacco sembra chiaramente avere una matrice politica. Uno dei messaggi apparsi nei flood (HTTP, SYN, ICMP) riporta infatti la scritta "win+love+in+Russia". Le tensioni esistenti tra i due Paesi stanno ultimamente crescendo";

Nelle ultime settimane la Georgia si è scontrata nuovamente con le autorità russe relativamente al modo di gestire le dispute nelle regioni dell'Abkhazia e nell'Ossetia del Sud, e i recenti colloqui tra la Georgia e la Nato sono stati considerati dalla Russia come una minaccia.

Non è la prima volta che degli hackers russi vengono accusati di essere coinvolti in attacchi informatici mossi da motivazioni politiche: lo scorso anno, il Presidente Ucraino Viktor Yushchenko è stato vittima di attacchi DDoS, considerati di origine russa. Allo stesso modo, anche il sito di Gary Kasparov, famoso Gran Maestro scacchista russo e attualmente impegnato contro l'establishment politico del proprio Paese, è stato colpito.

Dichiara Marco Gioanola, Consulting Engineer Arbor Networks, EMEA - Italia: "Ciò che colpisce di questi attacchi è la relativa facilità con cui vengono attivati e portati a termine con successo. Eventi di questo tipo mostrano che le botnet, attualmente usate in gran parte per l'invio di SPAM, continuano a essere a disposizione per attacchi DDoS: le nostre ricerche, e non solo, hanno mostrato come sia possibile "affittare" queste infrastrutture per attacchi "una tantum" o per attività continuate. La nostra rete di monitoraggio ATLAS registra una continua attività legata alle botnet e una costante sofisticazione nei metodi di gestione; già oggi, tra le principali sorgenti di attacchi osserviamo paesi dove la penetrazione di Internet è ancora bassa: cosa accadrà quando la Cina avrà la stessa percentuale di utenti Internet dei paesi europei?"

Jose Nazario, membro del team di ricerca Arbor, terrà un intervento sull'incremento di attacchi DDoS motivati politicamente alla prossima conferenza USENIX in California, il 30 Luglio.

Sul blog di José Nazario sono disponibili ulteriori informazioni sull'ultimo attacco DDoS:
<http://asert.arbornetworks.com/2008/07/georgia-on-my-mind-political-ddos/>

Approfondimenti sui precedenti attacchi, sono invece disponibili al seguente link:
<http://asert.arbornetworks.com/2007/12/political-ddos-ukraine-kasparov/>

About Arbor Networks

Arbor Networks(R) fornisce servizi per la sicurezza di rete core-to-core e le prestazioni operative per le reti aziendali globali. Le soluzioni NBA (Network Behavioral Analysis) di Arbor sono costruite sulla piattaforma Arbor Peakflow(R), per garantire visualizzazioni in tempo reale delle attività di rete che consentono alle organizzazioni di proteggersi immediatamente da worm, attacchi DDoS, abuso interno, instabilità di traffico e routing, nonché di suddividere in segmenti e rafforzare le reti in vista di future minacce. Oggi, i clienti di Arbor Networks comprendono una vasta gamma di provider di servizi e clienti aziendali, appartenenti a diversi settori in tutto il mondo, a dimostrazione della profondità e dell'ampiezza dell'esperienza di Arbor Networks in fatto di sicurezza. La tecnologia si serve della piattaforma Arbor Peakflow per impedire costosi tempi di inattività, consentire la pulizia della rete e aumentare la fiducia dei clienti. Per ulteriori informazioni su Arbor Networks, visitare <http://www.arbornetworks.com>.

Per ulteriori informazioni su ASERT(Arbor Security Engineering & Response Team), il ramo della società che si occupa di ricerche nel campo della sicurezza, visitare il blog di ASERT all'indirizzo <http://asert.arbornetworks.com>.

Nota per i redattori: Arbor Networks, Peakflow, ATLAS e il logo Arbor Networks sono marchi commerciali di Arbor Networks, Inc. Ellacoya Networks è un marchio di Ellacoya Networks Inc. Tutti gli altri marchi possono essere marchi commerciali dei rispettivi proprietari.