RAPPORTO NICP OTTOBRE 2001 SUL TERRORISMO INFORMATICO

SOMMARIO

Gli eventi politici e le emergenti situazioni internazionali porteranno ad un aumento delle "proteste informatiche" (*cyber protests*). Le proteste che ci sono state finora hanno avuto un impatto modesto sulle infrastrutture degli Stati Uniti. Mentre la tecnologia informatica migliora e diventa più veloce e quella degli hackers più avanzata e facile da usare, le proteste informatiche e l'attivismo degli hacker (*hactivism*) assumono un rilievo maggiore per gli interessi nazionali degli Stati Uniti. I manifestanti informatici *(cyber protesters)* cominciano ad aumentare e ad essere più organizzati; le loro tecniche più sofisticate anche se, molto probabilmente, continueranno a danneggiare i siti Web a compiere attacchi DOS. Ci sarà anche un aumento del numero della partecipazione di gruppi hacker apparentemente non correlati con le proteste informatiche. I confini nazionali non saranno sempre ben delineati negli attacchi contro le organizzazioni. Le attività internazionali tenderanno a diffondersi in tutti gli Stati Uniti e, poiché gli Stati Uniti sono una nazione guida multiculturale, in futuro soffrirà per attacchi a strutture e a siti stabiliti secondo un criterio culturale.
In genere, i siti più colpiti sono quelli che appartengono al governo ed alle istituzioni educative, commerciali e culturali. Comunque, ogni sito che sia potenzialmente vulnerabile sarà suscettibile di attacchi. Le infrastrutture hanno costituito gli obiettivi di attacchi in altri paesi ed, probabilmente, sarà così anche negli Stati Uniti. Certamente i manifestanti informatici avranno più spesso come bersaglio le infrastrutture e sfrutteranno le opportunità di distruggerle o danneggiarle.
I siti Web che rimarranno aperti agli attacchi degli hacker attraverso i sistemi conosciuti, avranno maggiori possibilità di essere attaccati. Gli amministratori dei network devono essere sempre istruiti e le difese devono evolversi, così come si evolvono le capacità di minaccia ed offensiva. Benché le proteste viste sino ad ora abbiano causato dei danni limitati, in futuro gli attacchi potrebbero portare a grosse perdite economiche, a gravi danni alle infrastrutture nazionali, così come colpire i mercati mondiali o la sicurezza pubblica.

INTRODUZIONE

Nell'ultima decade, con l'esplosione di Internet, le proteste e l'attivismo politico hanno trovato un nuovo regno. L'attivismo politico in Internet ha già generato una grande catena di attività, dall'uso delle e-mail e dei siti Web per organizzarsi, al danneggiamento delle pagine Web e agli attacchi che paralizzano i servizi. Questi attacchi, politicamente motivati e basati sull'informatica, vengono generalmente descritti come *hactivism*, un'unione di attività politica ed hackeraggio.
In aggiunta a consistenti attività di gruppi, dedicate a cause specifiche e a lungo termine, Internet ha visto anche brevi periodi di intensa attività politica che possono essere ricondotti alle *cyber protests*.
Le *cyber protests* hanno cominciato ad assumere le vesta di un fenomeno mondiale, accessibile a chiunque abbia un computer. Non limitati da confini geografici, le proteste informatiche hanno un forum enorme dove possono essere sentite. I manifestanti informatici hanno una gran varietà di mete ed obiettivi. Alcuni hackers vogliono rendere pubblica la corruzione del governo e la violazione fondamentale dei diritti umani; altri vogliono fare danni per il puro divertimento. E' solo dal 1998 che le proteste informatiche hanno raggiunto una popolarità smisurata e sono diventate luogo comune nel mondo computerizzato di oggi. Il tipo più comune di protesta informatica è il danneggiamento della *Web page*. In uno scenario come questo, un sito Web è compromesso a causa di alcune mancanze del sistema di

sicurezza e l'hacker è in grado di alterarlo, facendo spesso propaganda, profanandolo o mettendoci immagini pornografiche. Le conseguenze possono consistere in un fastidio ed imbarazzo oppure in una perdita economica per *l'e-commerce business*.
Le proteste e i disturbi non rappresentano nulla di nuovo. La gente infelice per cause proprie ha sempre trovato una valvola di sfogo per lanciare i suoi messaggi, fosse un sit-in di pace, una catena di S.Antonio, una marcia o un combattimento violento tra opposte fazioni. Ora, con l'avvento di Internet e la crescita del numero di persone *online*, organizzare proteste è diventato più facile. Questo non vuol dire che ogni attacco al Web è un evento progettato da qualche organizzazione politica. Molti danneggiamenti sono perpetrati da hacker solitari che non hanno una motivazione politica oltre a quella di creare caos. Gli stati-nazione e i loro cittadini sono stati coinvolti nelle proteste informatiche. Molti paesi hanno condotto delle battaglie reciproche attraverso gli hacker e i loro attacchi. Bombardare di e-mail è una forma comune di attacco DOS.
Deve essere rilevato, comunque, che alcune delle parti coinvolte in queste proteste informatiche, non sono necessariamente cittadini dei rispettivi paesi. Essi potrebbero avere idee simili oppure essere coinvolte solo per fare hackeraggio. per alcuni di questi gruppi le alleanze possono essere sottili.

GLI HACKER CINESI

Un incidente molto grave è avvenuto nel maggio 1999 dopo che gli Stati Uniti hanno bombardato accidentalmente l'ambasciata cinese a Belgrado, in Yugoslavia, durante la campagna aerea della NATO. I siti Web degli Stati Uniti sono stati danneggiati in nome della Cina e una massiccia campagna di e-mail è stata effettuata per solidarietà alla causa cinese. I primi obiettivi sono stati i siti del Governo, *l' U.S. Departments of Energy and the Interior e il National Park Service* hanno subito danni a i loro siti. Inoltre, il sito della Casa Bianca è stato messo fuori uso per tre giorni a causa dell'enorme quantità di e-mail ricevute. Quell'azione fu relativamente disorganizzata nel modo, nella durata, breve, e colpì un numero limitato di siti.
Hackers a favore della Cina colpirono anche Taiwan durante le elezioni presidenziali Taiwanesi nell'agosto e settembre 1999. Le proteste e azioni di hackeraggio compromisero 165 siti Web Taiwanesi, danneggiandoli gravemente in un periodo di due mesi. Il loro obiettivo finale era di colpire le infrastrutture di Taiwan e metterle fuori uso. Tra i bersagli, istituzioni per l'energia elettrica, economiche, delle telecomunicazioni e del controllo del traffico aereo. Sebbene le reazioni avvennero verso la fine degli attacchi, i danni furono relativamente leggeri.
Il modo strategico di colpire ed alcune unioni di forze divennero strategie consolidate per le successive azioni di hackeraggio o protesta e renderanno gli hacker più forti ed organizzati per il futuro. Alla fine di aprile, inizio di maggio 2001, gli *hactivists* per la Cina e i manifestanti informatici cominciarono un attacco ai siti degli Stati Uniti dovuto alla caduta di un jet da combattimento cinese dopo la collisione con un ricognitore americano. Il fatto coincise anche con il secondo anniversario del bombardamento all'ambasciata cinese di Belgrado e con il tradizionale May Day e Youth Day in Cina. L'attacco fu ad opera degli HUC (Honkers Union of China), gli hackers per la Cina danneggiarono o distrussero oltre 100 siti Web apparentemente scelti a caso, principalmente .gov o .com, attraverso attacchi DOS o simili exploit.
Malgrado molti dei sistemi fossero sofisticati, essi furono velocemente disponibili per entrambe le parti su Internet.
Molti danneggiamenti dei siti degli Stati Uniti comprendevano l'inserimento delle fotografie del pilota cinese Wang Wei e messaggi che incitavano alla caduta

dell'America. Gli hackers pro Stati Uniti risposero con azioni simili, messaggi e danneggiarono oltre 300 siti cinesi.
E' interessante il fatto che alcuni hackers cinesi violarono la loro etiquette, distruggendo alcuni servers compromessi. Bisogna danneggiare o distruggere il sito ma lasciare l'informazione intatta, altrimenti è una *bad form*.

HACKERS ISRAELIANI E PALESTINESI

Nell'ottobre 2000 gli hackers israeliani e palestinesi ingaggiarono una guerra di hackeraggio quando si interruppe la lunga tregua tra i due popoli. Durante questo periodo difficile, gli hacker valutarono l'opportunità di attaccare i siti avversari. Dal 6 ottobre 2000, 40 siti Web israeliani e almeno 15 palestinesi subirono danneggiamenti. Naturalmente, ciò coincise con la violenza nelle regioni. Ci furono dei problemi anche per siti americani che spesso si trovano coinvolti negli eventi. Per esempio, molti siti americani vennero attaccati, tra i quali il sito di una lobby. Gli hackers registrarono anche le informazioni personali dei membri del gruppo ed i numeri delle loro carte di credito. Il livello di sofisticazione spaziava dai piccoli danneggiamenti ad attacchi relativamente sofisticati che penetravano nelle radici del sistema.
Alcuni sistemi vennero elaborati apposta per quell'azione, dove venne usato ogni mezzo: virus, bombardamenti di e-mail ed attacchi amplificati. I siti Web contenenti questi sistemi furono prontamente disponibili per il *download* da parte di chiunque volesse prendere parte all'azione. Gli hackers palestinesi colpirono ogni tipo di sito israeliano che fossero capaci di compromettere, spesso distruggendoli con messaggi come "*Free Palestine*" o *Free Kashmir".* Il *software Floodnet* era uno dei più usati da Israele. Il manifestante informatico visitava semplicemente un sito e *Floodnet* mandava ripetutamente richieste al server bersaglio. Questo tipo di sit-in virtuale è una forma comune di attacco DOS. Molti di questi attacchi ebbero successo e i *server* bombardati furono messi fuori uso ripetutamente. Gli obiettivi consistevano nel distruggere le infrastrutture dei siti Web delle istituzioni economiche. I siti *e-commerce* vennero distrutti con un impatto economico sul mercato di Israele. L'accesso alla memoria dei sistemi fu, però, il pericolo maggiore. Un hacker che riesce ad accedervi ha la libertà illimitata di fare ciò che vuole. Questo è il livello di penetrazione più alto che esista ma non si conosce nessun tipo di attacco di questo tipo che abbia avuto successo.
Questi eventi attirarono un'ampia schiera di hackers desiderosi di partecipare alla battaglia. Entrambe le parti erano ben organizzate ed usavano tecniche di accesso e di riconoscimento intelligenti per massimizzare la loro efficacia. Anche gruppi di hacker esterni, come il G-Force Pakistan, si unì ai palestinesi per dare loro una mano, un fatto sempre più comune. Altri gruppi esterni diedero il loro appoggio per motivazioni politiche simili. Altri ancora, parteciparono agli attacchi per il semplice desiderio di hackeraggio o per pubblicità. Ci si può aspettare che gli hacker palestinesi e quelli israeliani si attiveranno ogni volta che apparirà un ostacolo sulla loro strada per la pace. D'altra parte, invece, l'incremento degli attacchi degli hacker può avvenire quando Israele e la Palestina siano vicino ad un accordo di pace. I *system administrator* devono rimanere vigili e provvedere all'efficacia della sicurezza dei network.

GLI HACKERS INDIANI E PAKISTANI

Un altro esempio è fornito dall'India e dal Pakistan, impegnati in una guerra informatica a causa delle differenze etniche e nazionali. Dopo la tregua in Kashmir, gli hacker hanno deciso di continuare le ostilità. I pro pakistani hanno distrutto nel 2000 oltre 500 siti Web indiani; al contrario, si sa che solo un sito pakistano è stato attaccato dagli indiani. Questo ci mostra la grande differenza di tecnica, di capacità

e la prontezza di usare gli esperti per sconfiggere un avversario. In questo caso, però, il livello apparente di sofisticazione è relativamente basso da entrambe le parti. Il danneggiamento dei siti Web è la forma maggiore di questa protesta. Il gruppo G-Force è stato il più attivo in quegli eventi.

GLI INCIDENTI GIAPPONESI

Recentemente il Giappone è stato doppiamente bersagliato da proteste online. Durante la prima settimana di aprile del 2001, gli hacker pro Corea hanno attaccato le organizzazioni giapponesi responsabili dell'approvazione di un nuovo testo di storia che ha omesso le atrocità commesse dal Giappone durante la seconda guerra mondiale e nell'occupazione della Cina e della Corea del Sud e la persistente riluttanza del Giappone ad accettare la responsabilità delle sue azioni ha provocato questi attacchi. I principali partecipanti a questi incidenti sono stati gli studenti universitari che hanno usato il bombardamento e-mail in un attacco DOS. Gli studenti hanno distrutto molti siti, compreso quello del Ministero dell'educazione, del *Liberal Democratic Party* e le case editrici responsabili del libro di testo. Ai primi di agosto del 2001 gli hacker pro Cina hanno bersagliato i siti giapponesi dopo la visita del primo Ministro giapponese ad un controverso memoriale di guerra, lo *Yasukuni Shrine*. In un breve periodo di tempo gli hacker hanno danneggiato molti siti di compagnie giapponesi e di istituti di ricerca. Questo indica la continua volontà degli hacker pro Cina ad usare il cyber spazio ed i sistemi di hackeraggio come piattaforma per le proteste e la disobbedienza civile informatica, così come la dimostrazione di un forte senso di nazionalismo patriottico.

CONCLUSIONI

Mentre sin ora il danno informatico è stato contenuto, le infrastrutture saranno certamente l'obiettivo del futuro da parte dei manifestanti informatici e degli *hactivists,* con il potenziale obiettivo di una distruzione intenzionale piuttosto che creare un imbarazzo pubblico o un discorso puramente politico. La difesa pro-attiva dei network e la gestione della sicurezza sono d'obbligo per la prevenzione di gravi danni alle infrastrutture. La cooperazione internazionale e quella tra privato e pubblico con gli Stati Uniti è necessaria per assicurare la funzione crescente delle infrastrutture critiche.