

Investigazioni digitali e business

L'investigazione su sistemi digitali non è riservata agli hacker o alle spystory. Potrebbe avere a che fare con il business di tutti i giorni.



Andrea Ghirardini, Senior Storage & Virtualization Expert di Tc Systems

Hollywood è da sempre, oltre che il posto dove si produce l'entertainment, anche la più grande fabbrica al mondo di luoghi comuni e leggende metropolitane. Tutti noi abbiamo visto qualche scena relativa all'hacking di sistemi informatici. Purtroppo i film dove le cose sono rappresentate nella maniera più realistica (su tutti 'War Games, giochi di guerra' o 'S.y.n.a.p.s.e') sono sconosciuti ai più mentre, nel contempo, gli esempi più irrealistici (vengono in mente 'Hackers!' o 'Codice Swordfish') sono quelli che maggiormente hanno fatto presa nella mente del grande pubblico.

Si pensa quindi non solo all'hacker come un individuo in grado di aprire qualunque sistema con proprietà quasi magiche, ma anche al fatto che costoro puntino esclusivamente, per notorietà o al soldo di qualche compagnia di intelligence o alla malavita, a sistemi supersegreti contenenti chissà quali informazioni atte a sconvolgere il mondo.

Nella vita reale le cose ovviamente non funzionano in questo modo. Innanzitutto nessun sistema informatico viene aperto in maniera magica. Servono conoscenze e studio per trovare le vulnerabilità esposte e sfruttarle nella maniera opportuna. Ma è anche vero che i tool per verificare i sistemi (e abusare di essi) e le conoscenze necessarie per sfruttarli sono alla portata di chiunque, grazie alla rete Internet.

Ovviamente questo non significa che chiunque possa trasformarsi dall'oggi al domani in un soldato di cyberwar, però chiunque può accumulare sufficienti informazioni per abusare di un sistema mal protetto.

Tenendo questo in mente è bene capire perché un sistema debba essere scel-

to come target per un attacco informatico. Le ragioni sono molteplici e dipendono da una serie di fattori legati al sistema stesso e ai motivi dell'attaccante. Potrebbe essere un dipendente che voglia aggirare i vincoli di un proxy aziendale ("Perché mai non posso raggiungere Facebook?"), oppure che voglia vendicarsi per una mancata promozione, una vessazione (vera o presunta che sia), un licenziamento.

Potrebbe essere un concorrente interessato a qualche informazione (un brevetto, l'offerta per una gara, una campagna marketing). Oppure uno spammer interessato a nuovi Pc da cui spedire nuove offerte, un criminale informatico in cerca di computer per espandere una botnet, qualche ragazzino in cerca di numeri di carte credito, un paparazzo in cerca di foto scottanti nello smartphone della starlette di turno, un gruppo di attivisti che bersaglia la multinazionale di turno.

Tirando le fila si può tranquillamente affermare che un computer che possiede un indirizzo Ip, potenza computazionale e delle informazioni può essere il target di un attacco informatico. Come chiunque può facilmente capire questa descrizione include qualche ogni sistema informatico della Terra.

È bene tenere in considerazione questo perché quando il fattaccio accade spesso è semplicemente troppo tardi. Chi si ritrova a dover ricostruire cosa sia realmente accaduto si trova a non disporre delle informazioni necessarie per proseguire l'indagine.

I log file sono incompleti (quando vi sono), le politiche di sicurezza inesistenti o disattese, i sistemi di test promossi in produzione senza che vi sia stato alcun controllo di sicurezza, le regole di firewall

troppo lasche o errate. Non sempre si tratta di problemi facilmente risolvibili. Si pensi ad una ditta che debba garantire ai clienti un servizio protetto da un accordo di Sla stringente, ad un sistema critico come quello di controllo della produzione o della distribuzione di corrente, ad un server di e-commerce a cui siano sottratti dati di clienti, o banalmente ad un dipendente che aggirando un proxy aziendale abbia visitato un sito pedopornografico dal lavoro.

Taluni di questi problemi possono dar luogo a contenziosi in sede civile e penale e quindi poter organizzare una difesa opportuna può diventare vitale.

Quando quindi si verifica la sicurezza degli apparati della propria azienda è bene non solo pensare alle difese perimetrali (leggi firewall o vpn), ma considerare che certi asset (file, account, accesso ad internet) dovrebbero essere opportunamente controllati,

Le informazioni generate, i famosi file di log, dovrebbero essere salvati in un luogo sicuro e con le necessarie garanzie atte a garantire che non possano essere alterati dopo la loro generazione. In questo modo si può facilitare la ricostruzione dell'accaduto agli investigatori digitali e nel contempo usare tali file come prove legittime in tribunale, qualora si rendesse necessario arrivare a tali mezzi.

La sicurezza informatica, in tutte le forme, non dovrebbe seguire l'iter dei backup: di solito, chi li adotta, lo fa perché ha già perso dei dati in passato.