PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 18 - numero 3723 di lunedì 22 febbraio 2016

DDoS cambia aspetto

Questa diffusa tipologia di attacco via Internet è in costante evoluzione, grazie alla inventiva dei malviventi. Esaminiamo insieme le più recenti tecniche di attacco e quelle di difesa.

La gran parte degli attacchi, chiamati distributed denial of service (DDoS), non sembra essere più diretta al blocco dei sistemi informativi, quanto a distrarre l'attenzione degli esperti di sicurezza, permettendo quindi ai malviventi di penetrare per altre vie nei sistemi informativi.
Alcuni analisti hanno recentemente rilevato che questo tipo di attacchi non tende più a bloccare i siti Web di determinate aziende, ma tendono invece a **installare del malware** o a rubare dei dati, approfittando dello scompiglio che si crea nell'azienda, a fronte di questi attacchi.

Durante questi attacchi, infatti, il sistema attaccato continua ad essere funzionante, seppure con capacità limitate, e quindi è possibile inserire dei programmi o estrarre dei dati.
Con questo approccio, attacchi di piccole dimensioni possono essere perfino più pericolosi di attacchi su larga scala, perché se il sistema aziendale viene interamente bloccato, esso diventa più resistente alla estrazione di dati o all'immissione di programmi.

Questa è la ragione per la quale un recente studio ha messo in evidenza che la tendenza attuale è quella di aumentare il numero degli attacchi, anche se su scale inferiori.
Solo il due % degli attacchi ha carattere catastrofico e il 18 % ha un valore intermedio.
Proprio per questa ragione più di un terzo delle aziende interpellate ha rivelato di avere scoperto del malware installato nei propri sistemi, a seguito di un attacco **DDoS**, mentre altre aziende hanno rilevato che erano stati sottratti dei dati, soprattutto nel settore del commercio al minuto e dei servizi finanziari.

In particolare, nel settore dei servizi finanziari, il 50 % di questi attacchi ha avuto dimensioni assai limitato, ma nel 43 % dei casi è stata successivamente rilevata la installazione di malware.
Anche la durata di questi attacchi tende ad aumentare ed il 40 % di essi è durato per più di un giorno, il 10 % addirittura per una settimana.
Appare evidente che questi attacchi di durata prolungata offrono una maggiore finestra di opportunità per installare del malware o sottrarre dei dati.
Per quanto riguarda il costo di questi attacchi, uno studio pubblicato nel marzo 2015 parla di una perdita media di 100.000 sterline o più per un attacco della durata di un'ora. A questo costo occorre aggiungere il costo del fermo del sistema, nonché l sovraccarico di lavoro dei call center, contattati dai clienti che non riescono a ottenere tramite Internet le informazioni desiderate.
Occorre poi tener conto anche del costo di una campagna che tende a ripristinare l'immagine di un'azienda, danneggiata da questi attacchi.

Per questa ragione molte aziende stanno potenziando le difese contro questo tipo di attacco, anche se, almeno ad oggi, non sembra che sia possibile trovare soluzioni radicali.
Un certo numero delle aziende interpellate ha dichiarato di avere sei o più addetti alla gestione di questi attacchi, mentre altre aziende hanno dichiarato che nel 73 % dei casi esse investiranno una somma maggiore nella prevenzione di questi attacchi.

L'utilizzo di un sistema di elaborazione combinato con una parte delle elaborazioni svolte in casa ed una parte svolte nel cloud può contribuire alla mitigazione dei danni.
In questo modo, le soluzioni ibride permettono di attivare più rapidamente le contromisure.
Come sempre, occorre tenere sotto controllo le reti e svolgere indagini su picchi di traffico in uscita o sul traffico indirizzato agli indirizzi IP sconosciuti. Da notare che questi attacchi vengono anche utilizzati per attività estorsive, chiedendo denaro per bloccare gli attacchi in corso. Una prestigiosa rivista settimanale recentemente ha riferito che una banda utilizzava questi attacchi per estorcere denaro, pagabile in bitcoins. Questa banda, che si chiama DD4BC (DDoS for Bitcoin), ha attaccato agenzie di scommesse, istituzioni finanziarie e casinò on-line.

Non v'è dubbio che questo tipo di attacco abbia un basso costo, un basso rischio e possa portare ad incassare denaro, difficilmente tracciabile; per questa ragione le forze dell'ordine raccomandano di essere molto prudenti nel rispondere a queste domande estorsive, perché è possibile che esse vengano ripetute, almeno finché la azienda non ha messo a punto delle difese efficaci.

Adalberto Biasiotti
