Attacchi Denial of Service

L'obiettivo di un attacco Denial of Service è quello di impedire l'accesso a un server o a un sito Internet. Gli utenti dell'e-banking possono trovarsi a essere colpiti da questo genere di attacchi, ma anche esservi coinvolti senza saperlo. Proteggetevi!

Proteggetevi dagli attacchi Denial of Service (DoS) così:

- Utilizzate un programma antivirus aggiornato.
- Monitorate le connessioni per mezzo di un firewall.
- Installate regolarmente gli aggiornamenti del vostro sistema operativo e di tutti i programmi installati.
- Prestate attenzione e agite con cautela.

Esistono diverse tipologie di attacchi DoS. La più frequente consiste nell'invio contemporaneo di enormi quantità di dati a un servizio disponibile su un server, in modo da sovraccaricare quest'ultimo e impedirgli di rispondere a ulteriori richieste (p. es., il sito Internet non è più visualizzato nel browser). Solitamente non vengono sottratti o danneggiati dati.

In generale queste grandi quantità di dati vengono inviate attraverso una botnet. Si tratta allora di un attacco DDoS (Distributed Denial of Service) (vedi sotto).

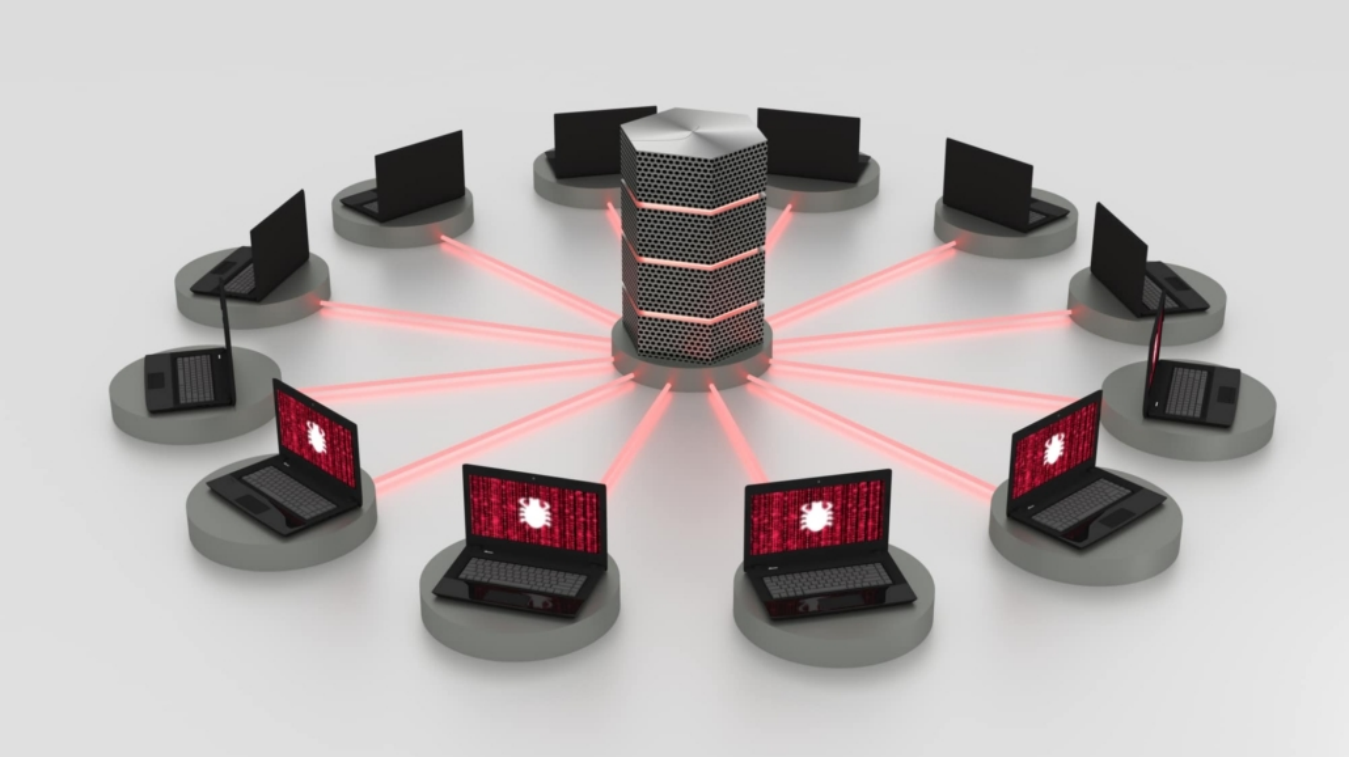
È importantissimo attenersi alle «5 operazioni per la vostra sicurezza digitale»(https://www.ebas.ch/it/5-operazioni-per-la-vostra-sicurezza-digitale/) per evitare che il vostro dispositivo entri a far parte di una botnet e quindi sia «coinvolto suo malgrado» in un attacco DDoS.

Attacchi coordinati provenienti da diversi dispositivi (DDoS – Distributed Denial of Service)

La forma più comune di attacco DoS è il cosiddetto attacco Distributed Denial of Service (DDoS), che viene sferrato in modo coordinato da un numero elevato di dispositivi.

L'attacco DDoS si suddivide in due fasi. In un primo momento l'hacker acquisisce il controllo di diversi dispositivi collegati a Internet per mezzo di cavalli di Troia o altre forme di malware, sviluppando una cosiddetta botnet. Successivamente l'hacker guida il comportamento dei dispositivi infettati (labotnet) portandoli ad attaccare contemporaneamente il bersaglio (p. es. un sito Internet).

L'attacco DDoS risulta molto efficace perché è sferrato contemporaneamente da numerosi dispositivi e quindi è semplicissimo produrre la grande quantità di dati necessaria. Questa tipologia viene sfruttata prevalentemente per paralizzare server e siti Internet. Negli attacchi DDoS solitamente è complicato individuare il vero autore dell'attacco, dato che il dispositivo dell'hacker stesso non esegue alcuna operazione diretta nei confronti del bersaglio.



Quando lancia un attacco Denial of Service (attacco DoS), un hacker sovraccarica o mette fuori uso un server o un sito Internet eseguendo un gran numero di richieste mirate. Lo scopo è bloccare l'accesso a tutti gli utenti.

L'attacco è rivolto per lo più contro un sito Internet, solitamente non vengono sottratti o danneggiati dati. L'hacker punta soltanto a impedire che gli utenti legittimi possano accedere al sito Internet (p. es. il sistema di e-banking).