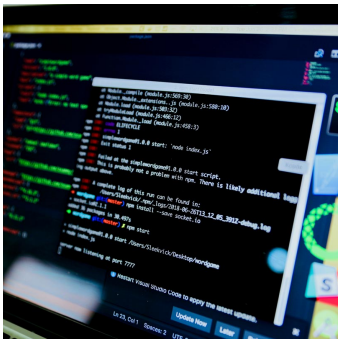
Valle Sabbia non solo News

INFO – TECNOLOGIA

Attacchi DDoS in aumento, Italia ancora bersaglio: come difendersi

Di Redazione

*I primi giorni del 2025 sono stati segnati da numerosi e preoccupanti **attacchi hacker verso importanti siti istituzionali e aziendali**. Si tratta di una minaccia denominata DDoS, che può interessare anche gli utenti privati, soprattutto chi utilizza siti per il gioco online*



DDos: una subdola categoria di attacchi informatici
Nella prima metà di gennaio 2025, l'Italia è stata bersagliata da numerosi attacchi informatici, diretti principalmente verso importanti siti istituzionali, istituti bancari e aziende.
Tali attacchi sono stati messi in atto con una particolare tecnica, denominata **DDoS (Denial of Service)**. Questa consiste nell'invio di un enorme numero di **false richieste a un server**, che diviene perciò inaccessibile, con gravi problemi nella funzionalità del sito.

I disagi sono di solito temporanei, e non compromettono l'integrità dei dati, ma **i danni potenziali** per quanto riguarda i siti più importanti costituiscono una grave minaccia per il Paese. Questi attacchi sono stati rivendicati da gruppi filorussi e filopalestinesi. Con questo tipo di strategia queste organizzazioni intendono comunicare il loro dissenso verso la politica estera italiana, come ad esempio il sostegno all'Ucraina. I social vengono poi sfruttati come mezzo di propaganda per esibire i risultati degli attacchi messi in atto.

Come si manifesta un attacco e come difendersi
Un attacco DDoS (Distributed Denial of Service) si manifesta generalmente con un sovraccarico di richieste inviate simultaneamente a un server o a una rete da una serie di dispositivi distribuiti.
Questo tipo di attacco ha l'obiettivo di interrompere l'accesso a un servizio, rendendo i siti web o le applicazioni inaccessibili agli utenti legittimi.

Le sue manifestazioni più comuni includono **rallentamenti significativi**, **inaccessibilità totale delle risorse online**, eccessivo tempo di risposta o errori di timeout. Il traffico di rete diventa anomalo, con un **numero molto elevato di richieste provenienti da più indirizzi IP**, spesso geograficamente distribuiti, che appaiono legittimi ma che, in realtà, provengono da botnet, ovvero reti di dispositivi compromessi, ad oggi venduti peraltro anche online. Questo può causare il blocco o il malfunzionamento del sistema colpito, compromettendo l'esperienza utente e l'affidabilità dei servizi online.

Questo tipo di attacco può colpire non solo le aziende e i governi, ma anche i privati cittadini.
Sebbene i grandi enti siano i bersagli più comuni, **anche un utente domestico può diventare vittima di attacchi DDoS**, specialmente se dispone di dispositivi IoT vulnerabili o se la sua rete domestica viene utilizzata come parte di una botnet per lanciare l'attacco.

Per difendersi, le aziende generalmente ricorrono a soluzioni avanzate come firewall configurati per filtrare il traffico, bilanciamento del carico e servizi di protezione DDoS basati su cloud. Tuttavia, anche i singoli cittadini possono adottare misure preventive per ridurre i rischi.

Un primo passo è proteggere i dispositivi personali, come computer e router, con **password robuste** e **aggiornamenti di sicurezza regolari**, per evitare che vengano compromessi e utilizzati per lanciare attacchi. È consigliabile utilizzare una **rete privata virtuale** (VPN) per mascherare il proprio indirizzo IP e ridurre il rischio di essere individuati come bersaglio di un attacco.

I migliori servizi VPN mettono a disposizione anche app dedicate, che semplificano l'utilizzo della VPN su vari dispositivi, offrendo una protezione aggiuntiva contro gli attacchi. Inoltre, è utile monitorare il traffico di rete, se possibile, e **disabilitare i dispositivi IoT non necessari**, che possono rappresentare un punto di accesso vulnerabile.

Infine, in caso di un attacco, disattivare temporaneamente i dispositivi o limitare l'accesso alla rete può ridurre l'impatto, mentre **contattare il proprio provider di servizi internet** per richiedere assistenza specifica può aiutare a mitigare l'effetto dell'attacco.
Anche se la protezione completa non è sempre garantita, questi accorgimenti possono ridurre il rischio di essere coinvolti in un attacco DDoS.

DATA DI PUBBLICAZIONE: 22/01/2025 – AGGIORNATO IL 27/03/2025 ALLE 02:00