

# Shodan: “Il motore di ricerca più terrificante del mondo”

Viviamo ormai in un mondo in cui i dispositivi fisici e sistemi elettronici sono sempre più connessi tra loro a causa dell'espansione dell'Internet delle cose (IOT), una rete complessa che consente lo scambio di dati. Questi sconvolgenti progressi tecnologici stanno permeando ogni aspetto della nostra vita, facilitando e monitorando numerosi compiti quotidiani relativi a trasporti, salute, casa, benessere o industria.

Oltre alle molteplici applicazioni che l'IOT ha per tutti i settori della vita in generale, ci sono anche alcuni problemi di sicurezza legati al suo aspetto. Il contesto del *deep web* (la parte “invisibile” di Internet) è un terreno pericoloso in cui è possibile individuare qualsiasi dispositivo.

All'interno di questo deep web, Shodan è un motore di ricerca per gli indirizzi HTTP collegati a Internet, molti dei quali non compaiono nelle ricerche di Google o simili. Può essere definito come un motore di ricerca dell'Internet delle cose, poiché è in grado di localizzare frigoriferi, allarmi, videocamere di sicurezza, webcam, dispositivi indossabili e qualsiasi altro dispositivo collegato.

Shodan è un motore di ricerca creato nel 2009 dall'esperto di sicurezza John Matherly, che lo ha definito “*il motore di ricerca più terrificante del mondo*” (il suo nome deriva dal tipo di malvagia intelligenza artificiale del leggendario videogioco *System Shock*). Il funzionamento di Shodan è simile a Google, anche se le somiglianze finiscono qui. Invece di indicizzare i contenuti Web tramite le porte 80 (HTTP) o 443 (HTTPS) come fa Google, Shodan esegue la scansione del Web alla ricerca di dispositivi che rispondano a un'altra serie di porte.

Shodan è quindi in grado di scoprire e indicizzare praticamente qualsiasi dispositivo, da una vasta gamma di webcam, segnaletica stradale, router, firewall, sistemi TVCC, sistemi di controllo industriale per centrali nucleari, reti elettriche, elettrodomestici e molto altro.

La parte più pericolosa e negativa di questo rilevamento è che tutti questi dispositivi sono connessi a Internet senza che i loro proprietari siano consapevoli dei pericoli e dei rischi a livello di sicurezza, e quindi, senza avere l'applicazione di misure di protezione di base come nome utente o password forti e affidabili. La sicurezza degli utenti è particolarmente instabile con le webcam, in quanto possono catturare immagini di ogni tipo in casa, informazioni personali o volti di minori.

Nel 2012, il ricercatore Dan Tentler ha dimostrato come sia stato in grado di utilizzare Shodan per trovare sistemi di controllo per macchine, scaldabagni a pressione e persino porte da garage. È stato anche in grado di trovare una centrale idroelettrica in Francia, un autolavaggio che poteva essere acceso e spento da remoto e una pista di hockey in Danimarca che avrebbe potuto essere sbrinata al clic di un pulsante! Ha persino trovato l'intero sistema di controllo del traffico di una città collegata alla rete, che avrebbe potuto essere interrotto con l'uso di alcuni comandi.

L'esistenza di progetti come Shodan ci porta a riflettere con urgenza sull'implementazione di nuovi meccanismi e misure di sicurezza sui nostri dispositivi indossabili, gadget e altri prodotti e dispositivi intelligenti.