Comprendere come Umbrella previene gli attacchi DDoS

Sommario

Introduzione

In questo documento viene descritto come Umbrella fornisce protezione contro un attacco distribuito di negazione del servizio.

Premesse

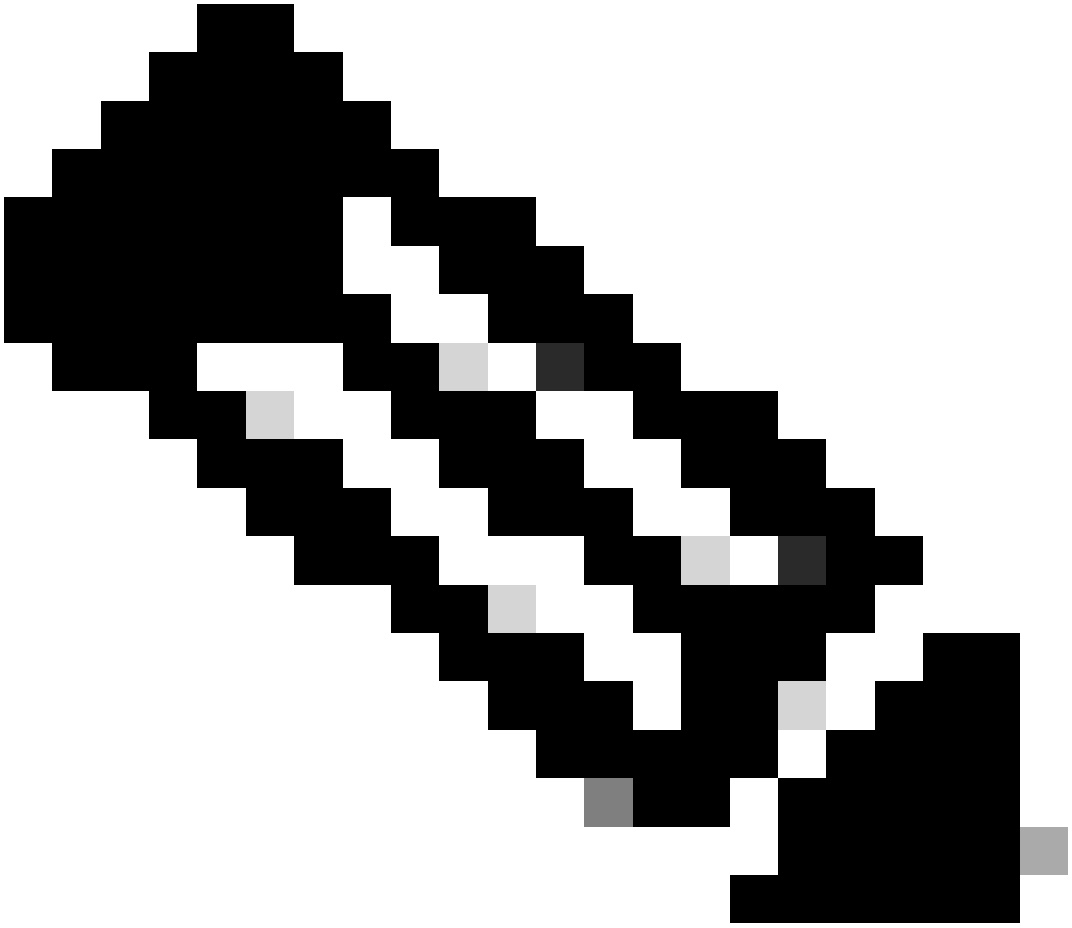
Un attacco DDoS (Distributed Denial-of-Service Attack) è un metodo con il quale gli aggressori malintenzionati, utilizzando reti di computer infetti, possono saturare il traffico diretto a un sito o servizio online per rendere la destinazione non disponibile.

I servizi forniti da Umbrella includono la protezione contro Command and Control Callback e malware nella categoria di sicurezza per la prevenzione. In questo modo è possibile evitare che l'infrastruttura venga utilizzata come piattaforma di lancio per attacchi DDoS ad altre società impedendo malware e, soprattutto, contenente Richiamate di comando e controllo tramite risoluzione DNS ricorsiva.

Come funziona Umbrella

Quando un computer con un malware tenta di attaccare un altro sito con un attacco DDOS, Umbrella gli impedisce di raggiungere quel sito. Impedendo ai computer della rete estesa, inclusi i computer in roaming, di partecipare a un attacco Command and Control Callback, l'organizzazione può evitare di essere vista come una possibile fonte di questo tipo di attacco.

Alcuni tipi di attacchi possono essere mitigati da Umbrella, come l'attacco contro DynDNS a causa della nostra tecnologia SmartCache che memorizza nella cache l'IP "buono" più recente conosciuto quando i record DNS di un sito web diventano non disponibili.



Nota: Per maggiori informazioni sull'attacco contro DynDNS, si veda: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

A causa della struttura del servizio, i servizi DNS di Umbrella non sono in grado di proteggere dagli attacchi DDoS che colpiscono i server DNS autorevoli o i server Web dall'esterno.

Per attacchi di questo tipo, è consigliabile un servizio che fornisca o gestisca un firewall dell'applicazione Web e il DNS autorevole. Un esempio di questo servizio complementare è CloudFlare.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).