So verhindert Umbrella DDoS-Angriffe

Inhalt

Einleitung

Dieses Dokument beschreibt, wie Umbrella Schutz vor einem verteilten Denial-of-Service-Angriff bietet.

Hintergrundinformationen

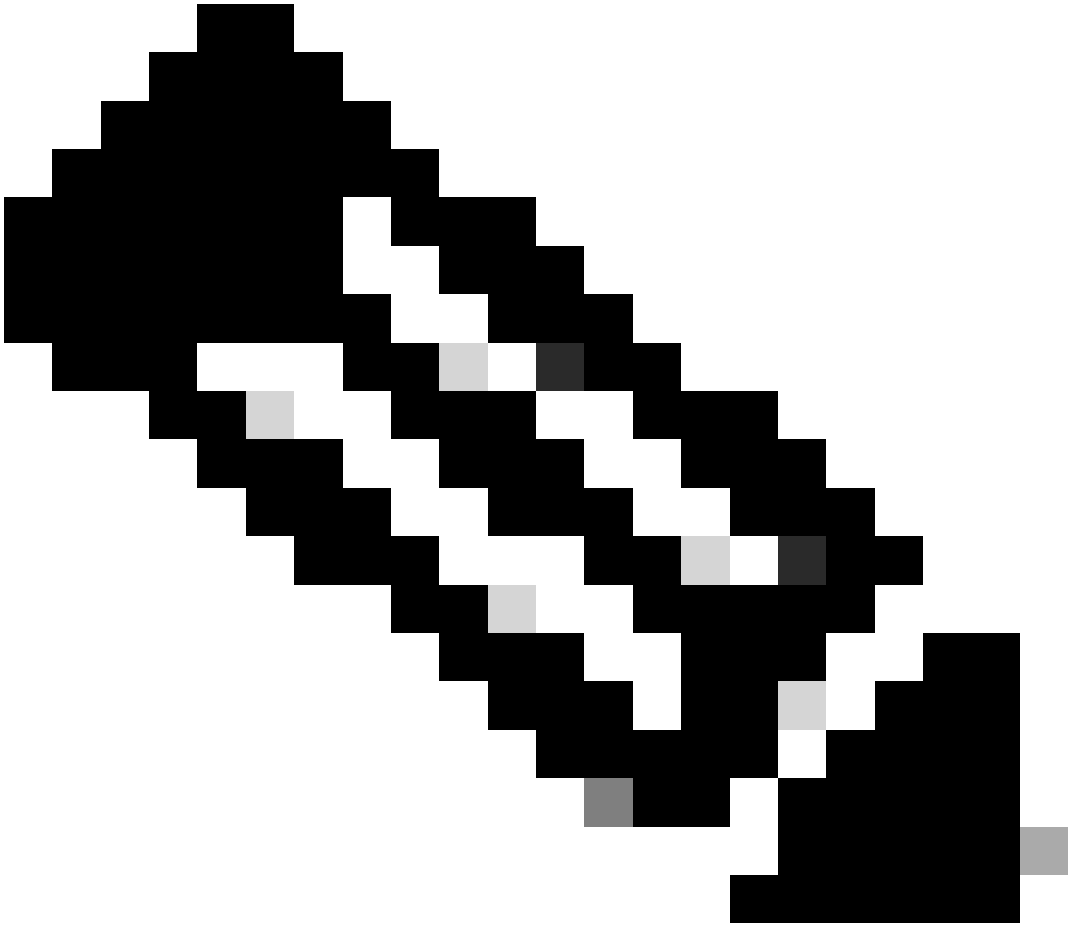
Ein DDoS- oder Distributed-Denial-of-Service-Angriff (DDoS-Angriff) ist eine Methode, mit der böswillige Angreifer mithilfe von Netzwerken infizierter Computer den Datenverkehr zu einer Online-Site oder einem Online-Dienst sättigen können, um das Ziel nicht verfügbar zu machen.

Die von Umbrella angebotenen Services beinhalten den Schutz vor Command-and-Control-Rückruf und Malware unter der Sicherheitskategorie für Prävention. Dies hilft zu verhindern, dass Ihre Infrastruktur als Startrampe für DDoS-Angriffe auf andere Unternehmen verwendet wird, indem Malware verhindert wird und vor allem Command-and-Control-Callback durch rekursive DNS-Auflösung eingedämmt wird.

Funktionsweise von Umbrella

Wenn ein Computer mit Malware versucht, einen anderen Standort mit einem DDoS-Angriff anzugreifen, verhindert Umbrella, dass dieser Standort erreicht wird. Wenn Sie Computer im erweiterten Netzwerk, einschließlich Roaming-Computer, von der Teilnahme an einem Command-and-Control-Rückruf-Angriff abhalten, kann Ihr Unternehmen verhindern, als mögliche Quelle für diese Art von Angriff angesehen zu werden.

Bestimmte Arten von Angriffen können durch Umbrella abgewehrt werden, wie z. B. der Angriff auf DynDNS aufgrund unserer SmartCache-Technologie, die die zuletzt bekannte "gute" IP zwischenspeichert, wenn die DNS-Einträge einer Website nicht mehr verfügbar sind.



Anmerkung: Weitere Informationen zum Angriff auf DynDNS finden Sie unter: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

Aufgrund der Struktur unseres Dienstes können die DNS-Dienste von Umbrella keinen Schutz vor DDoS-Angriffen bieten, die autoritative DNS-Server oder Webserver von außen angreifen.

Für solche Angriffe empfehlen wir einen Service, der eine Webanwendungs-Firewall und autoritative DNS bereitstellt oder verwaltet. Ein Beispiel für einen solchen ergänzenden Service ist CloudFlare.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.