Begrijp hoe paraplu DDoS-aanvallen voorkomt

Inhoud

Inleiding

In dit document wordt beschreven hoe Umbrella bescherming biedt tegen een gedistribueerde denial-of-service-aanval.

Achtergrondinformatie

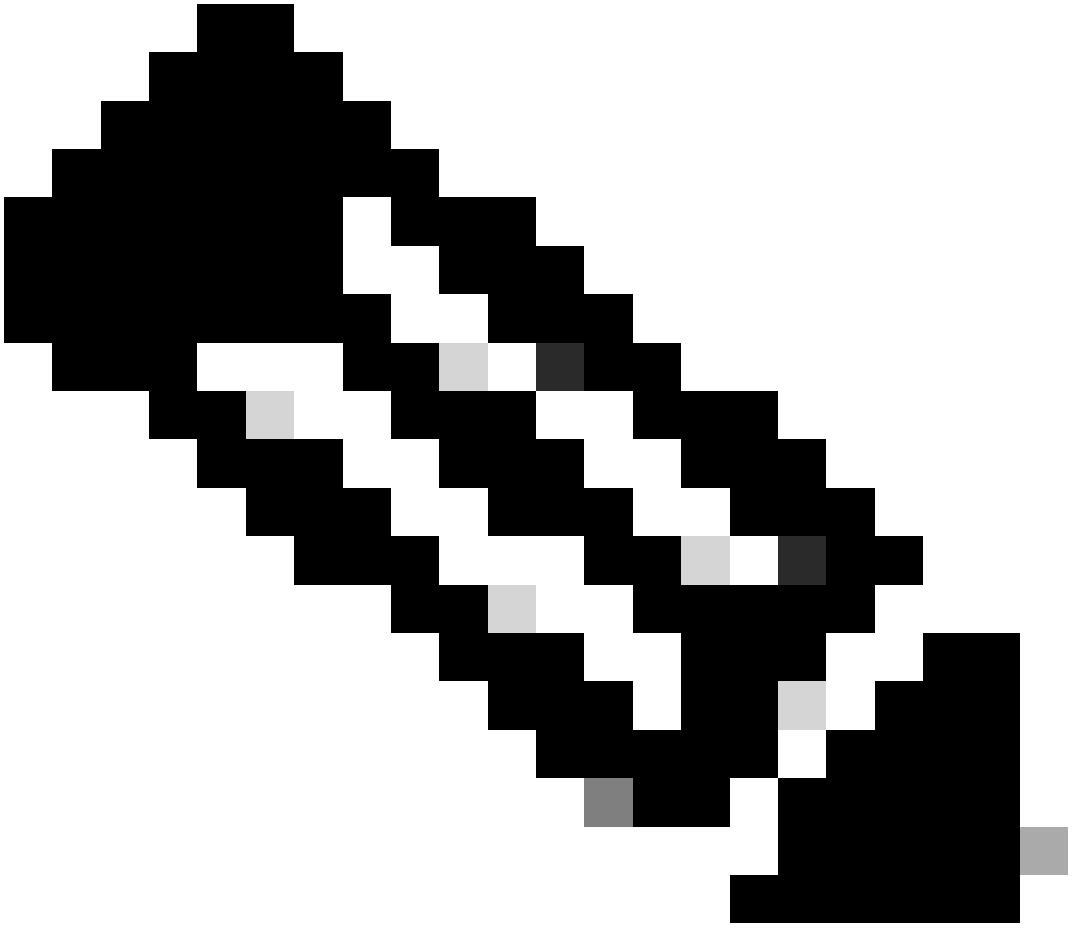
Een DDoS- of Distributed Denial-of-Service-aanval (DDoS-aanval) is een methode waarmee kwaadwillende aanvallers, met behulp van netwerken van geïnfecteerde computers, het verkeer naar een online site of service kunnen verzadigen om het doel niet beschikbaar te maken.

De diensten van Umbrella omvatten bescherming tegen Command and Control Callback en malware onder de beveiligingscategorie voor preventie. Dit helpt voorkomen dat uw infrastructuur wordt gebruikt als een lanceerplatform voor DDoS-aanvallen op andere bedrijven door malware te voorkomen en, nog belangrijker, Command and Control Callback te bevatten via recursieve DNS-resolutie.

Hoe werkt een paraplu

Wanneer een computer met malware probeert een andere site aan te vallen met een DDOS-aanval, voorkomt Umbrella dat deze die site bereikt. Door te voorkomen dat computers binnen uw uitgebreide netwerk, inclusief roamingcomputers, deelnemen aan een Command and Control Callback-aanval, kan uw organisatie voorkomen dat ze worden gezien als een mogelijke bron van dit soort aanvallen.

Bepaalde soorten aanvallen kunnen worden beperkt door Umbrella, zoals de aanval op DynDNS vanwege onze SmartCache-technologie die het meest recent bekende 'goede' IP-adres in cache opslaat wanneer de DNS-records van een website niet beschikbaar zijn.



Opmerking: voor meer informatie over de aanval op DynDNS, zie: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

Vanwege de manier waarop onze service is gestructureerd, kunnen de DNS-services van Umbrella niet beschermen tegen DDoS-aanvallen die van buitenaf op gezaghebbende DNS-servers of webservers zijn gericht.

Voor dergelijke aanvallen raden we een service aan die een webtoepassingsfirewall en een gezaghebbende DNS biedt of beheert. Een voorbeeld van zo'n complementaire dienst is CloudFlare.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.