Entenda como o Umbrella evita ataques de DDoS

Contents

Introdução

Este documento descreve como o Umbrella oferece proteção contra um ataque de negação de serviço distribuído.

Informações de Apoio

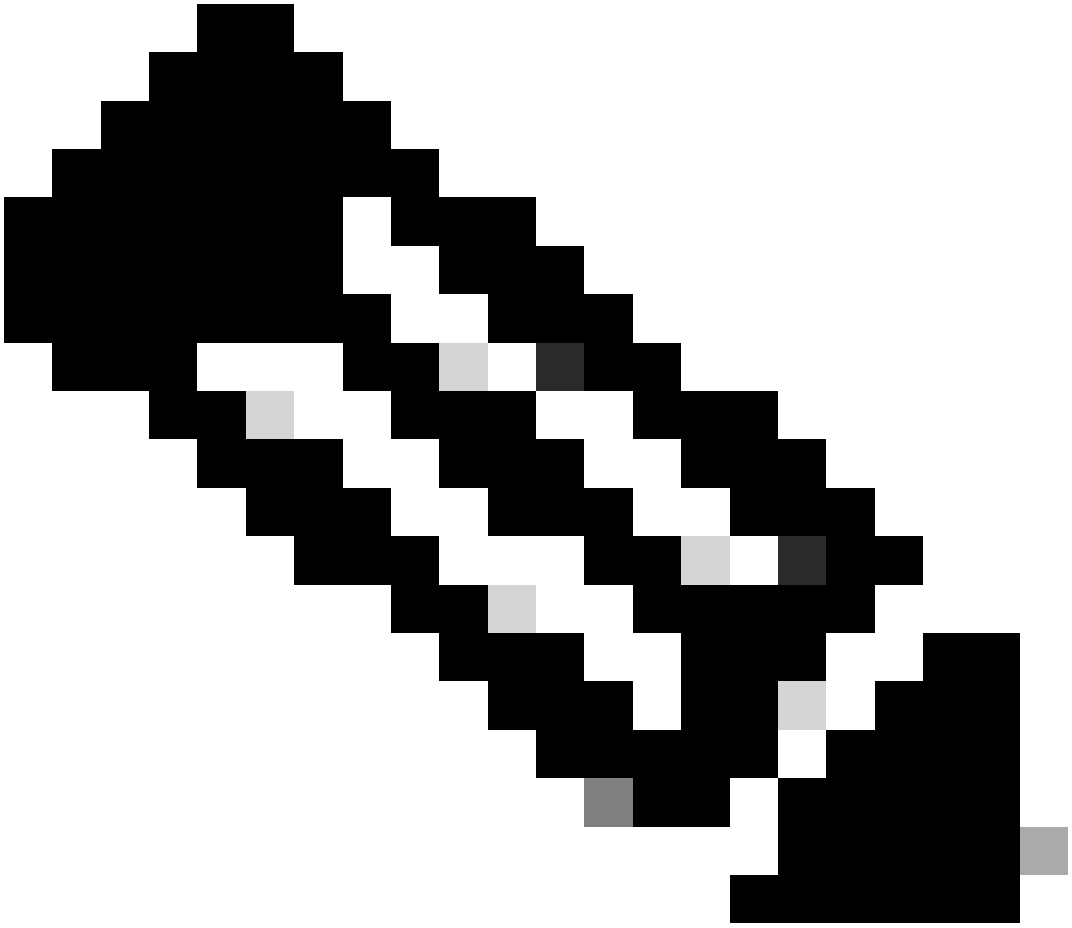
Um ataque DDoS ou de negação de serviço distribuído (ataque DDoS) é um método pelo qual invasores mal-intencionados, usando redes de computadores infectados, podem saturar o tráfego para um site ou serviço on-line para tornar o destino indisponível.

Os serviços fornecidos pela Umbrella incluem proteção contra Command and Control Callback e malware sob a Categoria de Segurança para Prevenção. Isso ajuda a evitar que sua infraestrutura seja usada como uma plataforma de lançamento para ataques DDoS em outras empresas, evitando malware e, mais importante, contendo o retorno de chamada de comando e controle por meio da resolução DNS recursiva.

Como o Umbrella funciona

Quando um computador com malware tenta atacar outro site com um ataque de DDOS, o Umbrella impede que ele acesse esse site. Impedindo que computadores em sua rede estendida, incluindo computadores em roaming, participem de um ataque de retorno de chamada de comando e controle, sua organização pode evitar ser vista como uma possível fonte desse tipo de ataque.

Certos tipos de ataques podem ser mitigados pelo Umbrella, como o ataque contra o DynDNS por causa de nossa tecnologia SmartCache que armazena em cache o IP "bom" conhecido mais recentemente quando os registros DNS de um site ficam indisponíveis.



Note: Para obter mais informações sobre o ataque ao DynDNS, consulte: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

Devido à forma como nosso serviço é estruturado, os serviços DNS da Umbrella não podem proteger contra ataques DDoS que têm como alvo servidores DNS ou servidores Web autorizados de fora.

Para ataques como o, recomendamos um serviço que forneça ou gerencie um firewall de aplicativo da Web e DNS autoritativo. Um exemplo desse serviço complementar é o CloudFlare.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.