Comprender cómo Umbrella previene los ataques DDoS

Contenido

Introducción

Este documento describe cómo Umbrella proporciona protección contra un ataque de denegación de servicio distribuido.

Antecedentes

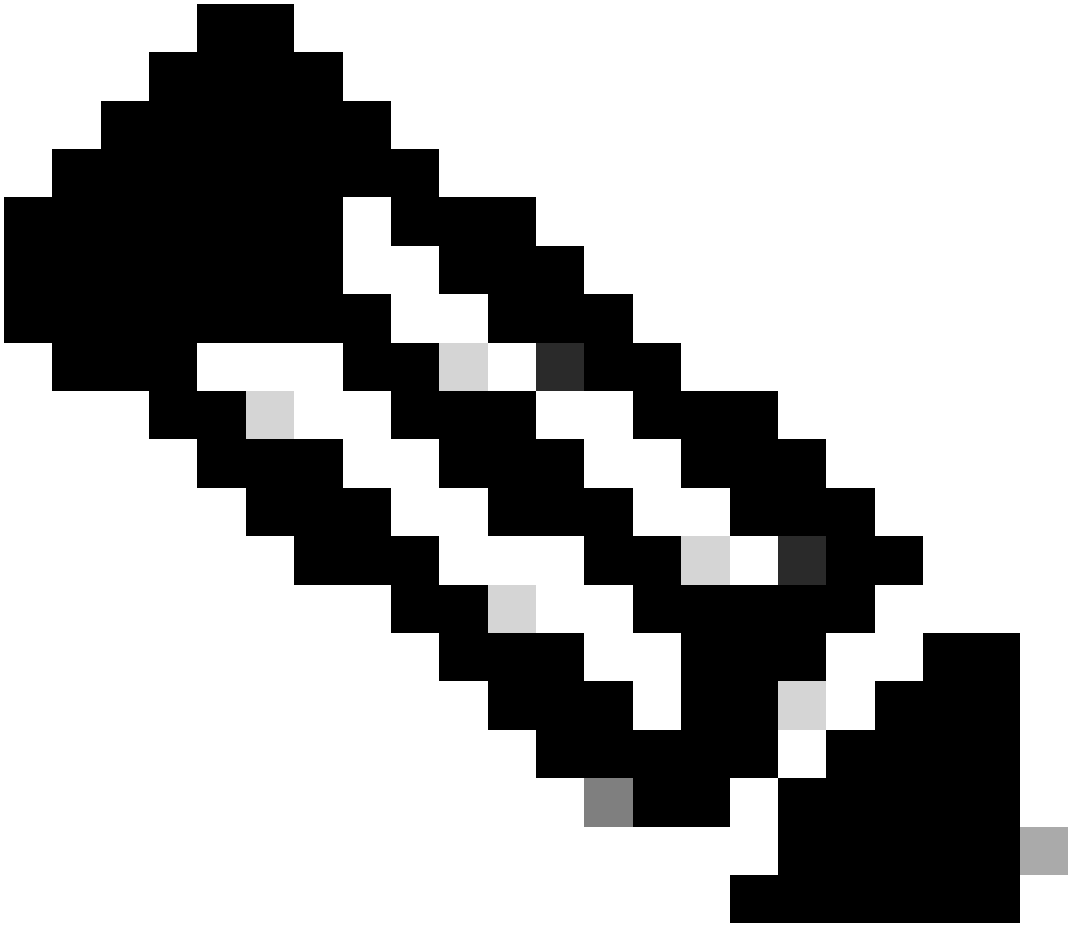
Un ataque DDoS o de denegación de servicio distribuida (ataque DDoS) es un método mediante el cual los atacantes malintencionados, que utilizan redes de ordenadores infectados, pueden saturar el tráfico de un sitio o servicio en línea para que el objetivo no esté disponible.

Los servicios proporcionados por Umbrella incluyen protección contra devolución de llamada de comando y control y malware en la categoría de seguridad para la prevención. Esto ayuda a evitar que su infraestructura se utilice como plataforma de lanzamiento de ataques DDoS a otras empresas mediante la prevención de malware y, lo que es más importante, la contención de la devolución de llamada de comando y control a través de la resolución de DNS recursiva.

Cómo funciona Umbrella

Cuando un equipo con malware intenta atacar otro sitio con un ataque DDOS, Umbrella impide que llegue a ese sitio. Al impedir que los equipos de la red extendida, incluidos los equipos móviles, participen en un ataque de devolución de llamada de comando y control, su organización puede evitar ser vista como una posible fuente de este tipo de ataque.

Umbrella puede mitigar ciertos tipos de ataques, como el ataque contra DynDNS debido a nuestra tecnología SmartCache que almacena en caché la IP "buena" conocida más recientemente cuando los registros DNS de un sitio web dejan de estar disponibles.



Nota: Para obtener más información sobre el ataque contra DynDNS, consulte: http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

Debido a la forma en que está estructurado nuestro servicio, los servicios DNS de Umbrella no pueden protegerse contra ataques DDoS dirigidos a servidores DNS autorizados o servidores web desde el exterior.

Para ataques como este, recomendamos un servicio que proporcione o administre un firewall de aplicaciones web y DNS autorizado. Un ejemplo de este tipo de servicio complementario es CloudFlare.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).