Umbrella가 DDoS 공격을 방지하는 방법 이해

목차

소개

이 문서에서는 Umbrella가 DDoS(Distributed Denial-of-Service) 공격을 차단하는 방법을 설명합니다.

배경 정보

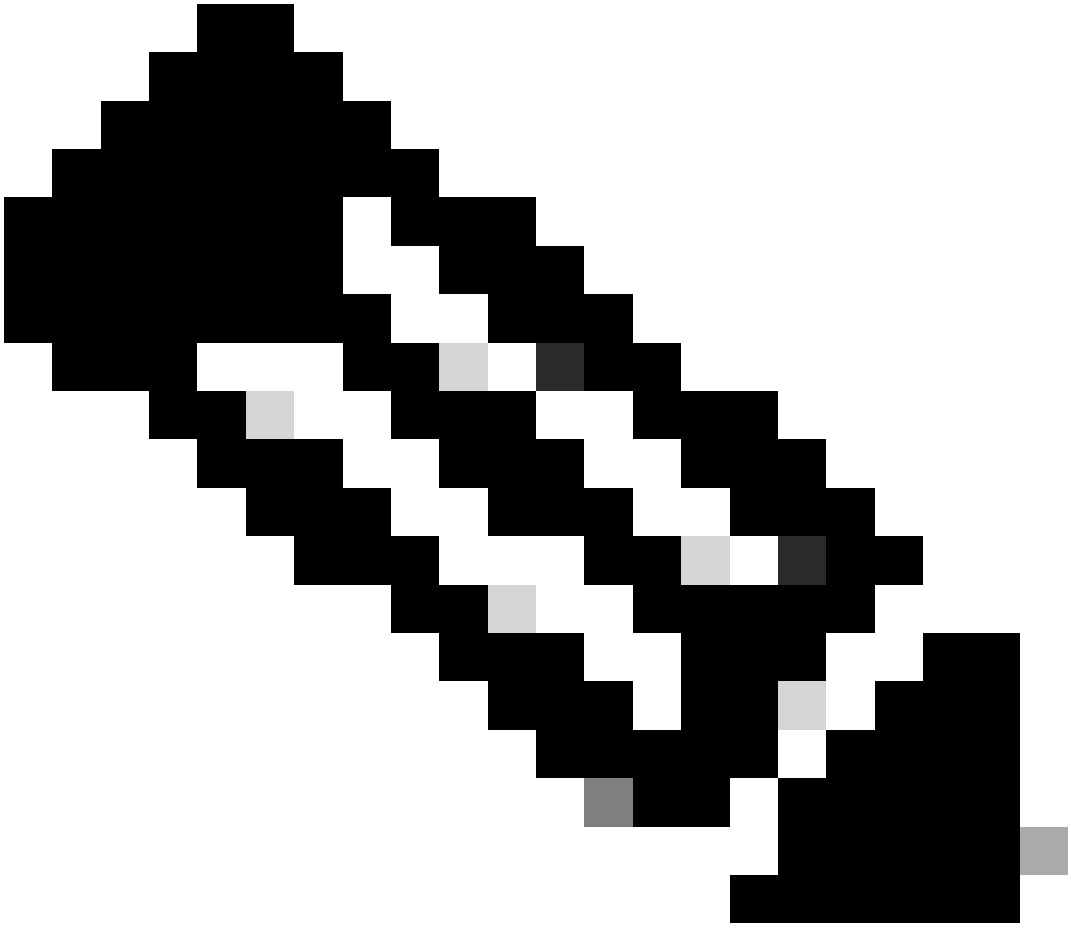
DDoS 또는 DDoS 공격(Distributed Denial-of-Service Attack, DDoS 공격)은 악의적인 공격자가 감염된 컴퓨터의 네트워크를 사용하여 온라인 사이트 또는 서비스에 트래픽을 포화시켜 대상을 사용할 수 없게 만드는 방법입니다.

Umbrella에서 제공하는 서비스에는 Security Category for Prevention(차단 보안 카테고리) 아래의 Command and Control Callback(명령 및 제어 콜백) 및 악성코드에 대한 보호가 포함됩니다. 이를 통해 재귀적 DNS 확인을 통한 악성코드, 특히 Command and Control Callback을 억제하여 인프라가 다른 회사에 대한 DDoS 공격의 실행 기지로 사용되는 것을 방지할 수 있습니다.

Umbrella 작동 방식

악성코드가 있는 컴퓨터가 DDOS 공격으로 다른 사이트를 공격하려고 하면 Umbrella는 해당 사이트에 도달하지 못하도록 차단합니다. 로밍 컴퓨터를 비롯한 확장 네트워크 내의 컴퓨터가 Command and Control 콜백 공격에 참여하는 것을 중지하면 조직이 이러한 유형의 공격의 가능한 소스로 간주되지 않을 수 있습니다.

Umbrella는 웹 사이트의 DNS 레코드를 사용할 수 없게 되면 가장 최근에 알려진 '정상' IP를 캐시하는 SmartCache 기술을 통해 DynDNS에 대한 공격과 같은 특정 유형의 공격을 완화할 수 있습니다.



참고: DynDNS 공격에 대한 자세한 내용은 다음을 참조하십시오.
http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta

---

Umbrella의 DNS 서비스는 서비스 구조 때문에 외부에서 신뢰할 수 있는 DNS 서버 또는 웹 서버를 대상으로 하는 DDoS 공격으로부터 보호할 수 없습니다.

이러한 공격의 경우 웹 애플리케이션 방화벽과 권한 있는 DNS를 제공하거나 관리하는 서비스를 권장합니다. 이러한 보완 서비스의 예로 CloudFlare가 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.