瞭解Umbrella如何防止DDoS攻擊

目錄

簡介

本檔案將說明Umbrella如何提供針對分散式拒絕服務攻擊的保護。

背景資訊

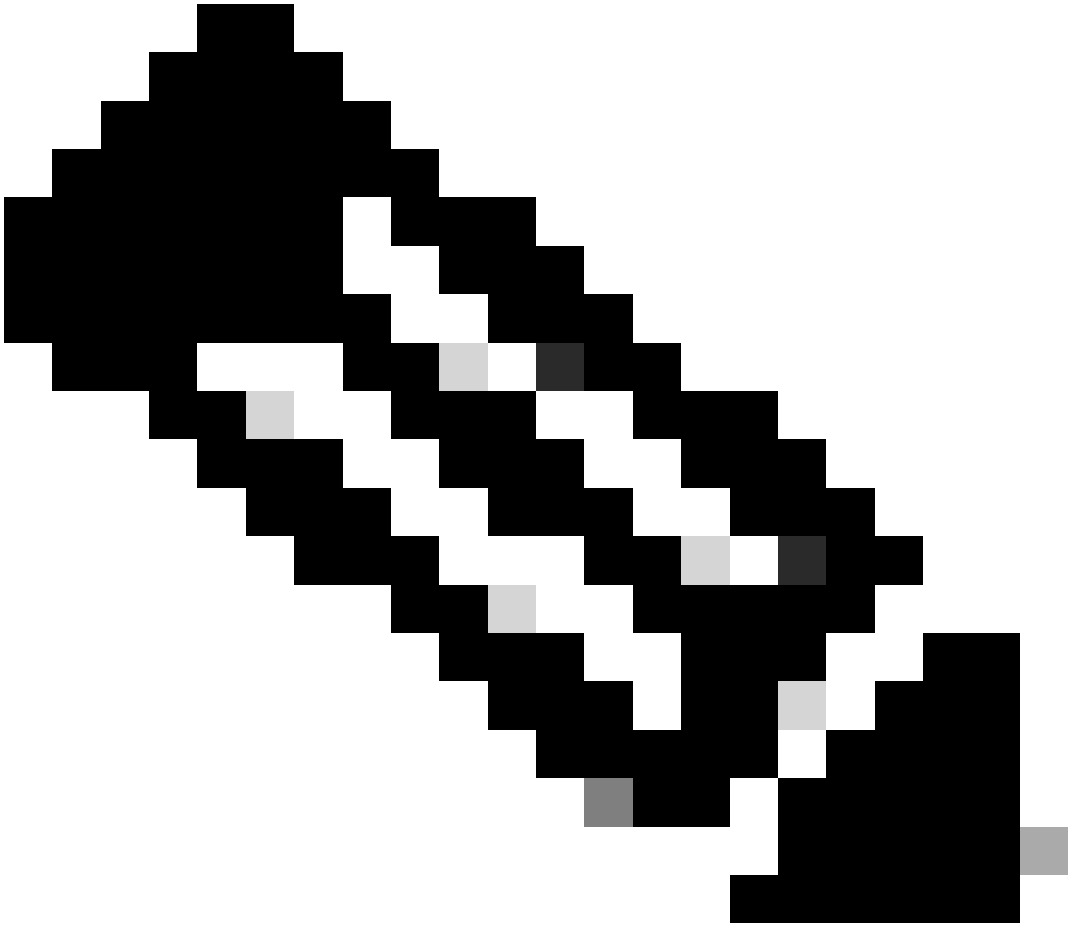
DDoS攻擊或分散式拒絕服務攻擊（DDoS attack，DDoS攻擊）是一種方法，惡意攻擊者利用受感染的電腦網路，可以飽和流向線上站點或服務的流量，使目標不可用。

Umbrella提供的服務包括針對命令和控制回叫以及針對防禦安全類別下的惡意軟體的防護。通過防止惡意軟體，更重要的是通過遞迴DNS解析包含命令和控制回撥，這有助於防止您的基礎設施被用作其他公司的DDoS攻擊啟動平台。

Umbrella的工作原理

當帶有惡意軟體的電腦嘗試使用DDOS攻擊其他站點時，Umbrella會阻止其訪問該站點。通過阻止擴展網路中的電腦（包括漫遊電腦）參與命令和控制回叫攻擊，您的組織可以避免被視為此類攻擊的可能來源。

Umbrella可以緩解某些型別的攻擊，例如針對DynDNS的攻擊，因為我們的SmartCache技術可以在網站的DNS記錄不可用時快取最近發現的「良好」IP。



附註：有關針對DynDNS的攻擊的詳細資訊，請參閱：http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_at

由於我們的服務採用結構化方式，Umbrella的DNS服務無法抵禦針對外部權威DNS伺服器或Web伺服器的DDoS攻擊。

對於此類攻擊，我們建議提供或管理Web應用程式防火牆和授權DNS的服務。CloudFlare就是這種補充服務的例子。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。