UmbrellaがDDoS攻撃を阻止する仕組みの理解

内容

はじめに

このドキュメントでは、Umbrellaが分散型DoS攻撃に対する保護をどのように提供するかについて説明します。

背景説明

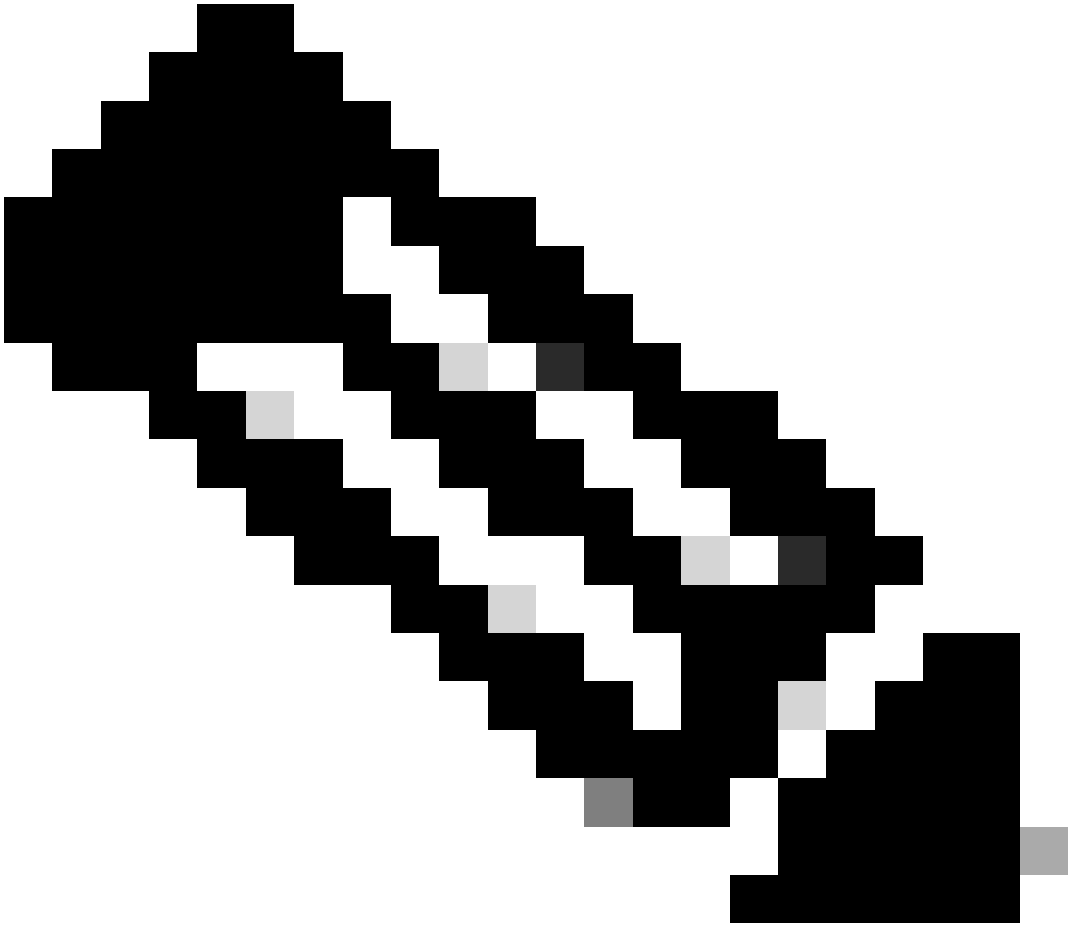
DDoS攻撃または分散型サービス拒絶攻撃（DDoS攻撃）は、悪意のある攻撃者が感染したコンピュータのネットワークを使用して、オンラインサイトまたはサービスへのトラフィックを飽和状態にし、ターゲットを使用できないようにする方法です。

Umbrellaが提供するサービスには、Security Category for Preventionのコマンド&コントロールコールバックおよびマルウェアに対する保護が含まれます。これは、マルウェアを防ぎ、さらに重要なことに、再帰DNS解決によるコマンド&コントロールコールバックを含めることで、インフラストラクチャが他の企業に対するDDoS攻撃のラウンチパッドとして使用されるのを防ぐのに役立ちます。

Umbrellaの機能

マルウェアを含むコンピュータがDDOS攻撃を使用して別のサイトを攻撃しようとすると、Umbrellaによってそのサイトへの到達が阻止されます。ローミング中のコンピュータを含む拡張ネットワーク内のコンピュータがコマンド&コントロールコールバック攻撃に参加しないようにすることで、この種の攻撃の発生源と見なされることを回避できます。

SmartCacheテクノロジーは、WebサイトのDNSレコードが利用できなくなったときに最新の「正常な」IPをキャッシュするため、DynDNSに対する攻撃など、特定の種類の攻撃はUmbrellaによって軽減できます。



注:DynDNSに対する攻撃の詳細については、
http://www.theregister.co.uk/2016/10/21/dns_devastation_as_dyn_dies_under_denialofservice_atta
照してください。

当社のサービスの構造上、UmbrellaのDNSサービスは、権威のあるDNSサーバやWebサーバを外部からターゲットとするDDoS攻撃から保護することができません。

このような攻撃に対しては、Webアプリケーションファイアウォールと権威DNSを提供または管理するサービスを推奨します。このような補完的なサービスの一例がCloudFlareです。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。