Umbrella Roaming Clientを使用したサードパーティ製VPNの検出ヒューリスティックについて

内容

はじめに

このドキュメントでは、Umbrellaクライアントのサードパーティ VPN検出ヒューリスティックについて説明します。

背景説明

Umbrellaクライアントには、VPNの変更に対応してDNS機能を維持するための自動検出メカニズムが実装されています。これにより、VPNが接続されている間、クライアントが一時的に保護されないままになる可能性があります。これらのメカニズムを次にまとめます。

サードパーティ製VPN検出ヒューリスティック

このドキュメントでは、VPNクライアントとの競合を回避するために、Umbrella Roaming Client(URC)がWindowsシステム上でVPNアクティビティを検出してDNS保護アクティビティを一時停止するために使用する3種類の一般的なヒューリスティックについて説明します。中断された保護ローミングクライアントは、保護されていない状態になります。

ケース1:VPNクライアントがDNSリゾルバのリストの先頭に自身のDNS IPアドレスを付加する

URCがUmbrellaリゾルバにトラフィックをアクティブにリダイレクトする場合、システム上のさまざまなネットワークアダプタがDNSサーバとして127.0.0.1または：:1を使用するように設定されます（URCはそのIPアドレスでローカルDNSプロキシを実行し、ポート53でリスニングします）。ネットワークイベントが検出されると、 DNS設定が変更されると、URCは各ネットワークアダプタのDNS IPアドレスのリストで127.0.0.1または：:1（ネットワークスタックに応じて、IPv4の場合は127.0.0.1、IPv6の場合は：:1）を検索します。IPアドレスが見つかり、プレフィックスが付けられている場合（10.0.0.23、192.168.2.23、127.0.0.1 DNS設定など）、URCは保護を中断します。 この状態は、アクティブなネットワークインターフェイスの数が変更されてクライアントの状態がリセットされるまで有効です。

ケース2:DNSリゾルバが変更されると、VPNクライアントがそのリゾルバを監視してリセットします。

一部のVPNクライアントでは、DNS設定の設定後にこれらの設定をアクティブに監視し、VPNク

ライアントで指定されている設定から逸脱している場合はリセットします。 URCはDNSアドレスの復帰を監視し、復帰が20秒以内に3回発生した場合、URCは保護を中断します。このセクションでは、5秒以内のペースで行われる復元について説明します。この状況は、アクティブなネットワークインターフェイスの数が変更され、クライアントの状態がリセットされるまで有効です。

ケース3:VPNクライアントがネットワーク層でAおよびAAAAレコードを代行受信してリダイレクトする

一部のVPNクライアントは、AレコードとAAAAレコードに干渉し（つまり、これらのレコードタイプだけをリダイレクトし）、他のレコードタイプは放置します。 この場合、URCはTXTなどの問題なくUmbrellaリゾルバと通信しますが、AレコードとAAAAレコードにはUmbrellaリゾルバを介して応答しないため、実質的に保護は適用されません。実際にDNS保護を適用する前に、URCはUmbrellaにテストレコードを送信してAおよびAAAAレコードの干渉をチェックします。応答が返されない場合、または期待される応答でない場合、URCは保護を中断します。 この場合はネットワークイベントがトリガーされないため、URCはこの状態を定期的にチェックします。このメカニズムは、Netskopeのようなソフトウェアプロキシが存在する場合にもトリガーされます。

その他

一部のVPNクライアントには、Umbrellaによって追加された明示的な互換性があります。このサポートは、Dell(Aventail)VPNクライアントおよびPulse Secureクライアントに対して明示的に行われます。

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。