Comprendre l'heuristique de la détection VPN tierce avec le client d'itinérance Umbrella

Table des matières

Introduction

Ce document décrit l'heuristique de détection VPN tierce du client Umbrella.

Informations générales

Le client Umbrella a mis en oeuvre des mécanismes de détection automatisés pour réagir aux changements de VPN afin de garantir le maintien de la fonctionnalité DNS. Cela peut entraîner le client à rester temporairement non protégé pendant que le VPN est connecté. Nous résumerons ces mécanismes ci-dessous.

Heuristiques de détection VPN tiers

Ce document présente trois heuristiques génériques différentes que le client d'itinérance Umbrella (URC) utilise pour détecter l'activité VPN sur un système Windows afin de suspendre l'activité de protection DNS pour éviter tout conflit avec le client VPN. Un client d'itinérance avec protection suspendue passe à l'état non protégé.

Cas 1 : Le client VPN ajoute sa propre adresse IP DNS à la liste des résolveurs DNS

Lorsque l'URC redirige activement le trafic vers un résolveur Umbrella, les différentes cartes réseau du système sont configurées pour utiliser 127.0.0.1 ou ::1 comme serveur DNS (l'URC exécute un proxy DNS local sur cette adresse IP, à l'écoute sur le port 53). Lorsqu'un événement réseau est détecté et que les paramètres DNS ont été modifiés, l'URC recherche 127.0.0.1 ou ::1 (selon la pile réseau, 127.0.0.1 pour IPv4 et ::1 pour IPv6) dans la liste des adresses IP DNS pour chaque carte réseau. Si elle est trouvée et si une adresse IP a été préfixée (par exemple 10.0.0.23, 192.168.2.23, 127.0.0.1 paramètres DNS), alors l'URC suspend la protection. Cet état reste en vigueur jusqu'à ce que le nombre d'interfaces réseau actives change et réinitialise l'état du client.

Cas 2 : Le client VPN surveille et réinitialise les résolveurs DNS lorsqu'ils changent

Certains clients VPN, après avoir défini la configuration DNS, surveillent activement ces paramètres et les réinitialisent s'ils s'écartent de la configuration spécifiée par le client VPN.

L'URC surveille les réversions d'adresse DNS et si des réversions se produisent 3 fois en 20 secondes, l'URC suspend la protection. Cela couvre tout retour qui se produit sur une cadence de toutes les 5 secondes ou moins. Cette situation reste en vigueur jusqu'à ce que le nombre d'interfaces réseau actives change et que l'état du client soit réinitialisé.

Cas 3 : Le client VPN intercepte et redirige les enregistrements A et AAAA sur la couche réseau

Certains clients VPN interfèrent avec les enregistrements A et AAAA (c'est-à-dire qu'ils redirigent uniquement ces types d'enregistrements) tout en laissant les autres types d'enregistrements tranquilles. Dans ce cas, l'URC communique avec le résolveur Umbrella sans problème pour TXT, et plus encore. , mais aucune protection n'est effectivement appliquée car les enregistrements A et AAAA ne reçoivent pas de réponse via le résolveur Umbrella. Avant d'appliquer réellement la protection DNS, l'URC vérifie les interférences d'enregistrement A et AAAA en envoyant certains enregistrements de test à Umbrella. Si la réponse ne revient pas ou n'est pas ce qui est attendu, l'URC suspend la protection. Étant donné qu'aucun événement réseau n'est déclenché dans ce cas, l'URC vérifie régulièrement cette condition. Ce mécanisme peut également se déclencher en présence d'un proxy logiciel comme Netskope.

Autres cas

Certains clients VPN ont une compatibilité explicite ajoutée par Umbrella. Cette prise en charge est explicite pour les clients VPN Dell (Aventail) et Pulse Secure à l'avenir.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.