Comprender la heurística de detección de VPN de terceros con Umbrella Roaming Client

Contenido

Introducción

Este documento describe la heurística de detección de VPN de terceros del cliente Umbrella.

Antecedentes

El cliente Umbrella ha implementado mecanismos de detección automatizados para reaccionar a los cambios de VPN con el fin de garantizar que se mantenga la funcionalidad de DNS. Esto puede hacer que el cliente permanezca temporalmente desprotegido mientras la VPN está conectada. A continuación resumimos estos mecanismos.

Heurística de detección de VPN de terceros

Este documento describe tres heurísticas genéricas diferentes que Umbrella Roaming Client (URC) utiliza para detectar la actividad VPN en un sistema Windows con el fin de suspender la actividad de protección DNS para evitar conflictos con el cliente VPN. Un cliente de roaming de protección suspendida ingresa en el estado sin protección.

Caso 1: El cliente VPN antepone la lista de resolvers DNS con su propia dirección IP DNS

Cuando el URC está redirigiendo activamente el tráfico a una resolución de Umbrella, los diversos adaptadores de red del sistema están configurados para utilizar 127.0.0.1 o ::1 como servidor DNS (el URC ejecuta un proxy DNS local en esa dirección IP, escuchando en el puerto 53). Cuando se detecta un evento de red y se cambia la configuración de DNS, el URC busca 127.0.0.1 o ::1 (dependiendo de la pila de red, 127.0.0.1 para IPv4 y ::1 para IPv6) en la lista de direcciones IP de DNS para cada adaptador de red. Si se encuentra, y si se ha asignado un prefijo a una dirección IP (por ejemplo, la configuración de DNS 10.0.0.23, 192.168.2.23, 127.0.0.1), el URC suspende la protección. Este estado permanece vigente hasta que el número de interfaces de red activas cambia y restablece el estado del cliente.

Caso 2: El cliente VPN monitorea y restablece los resolvers DNS cuando cambian

Algunos clientes VPN, después de establecer la configuración DNS, supervisan activamente esta configuración y la restablecen si se desvían de la configuración especificada por el cliente VPN.

El URC monitorea las reversiones de direcciones DNS, y si las reversiones ocurren 3 veces en 20 segundos el URC suspende la protección. Esto cubre cualquier inversión que se produzca en una cadencia de cada 5 segundos o menos. Esta situación permanece en vigor hasta que cambia el número de interfaces de red activas y se restablece el estado del cliente.

Caso 3: El cliente VPN intercepta y redirige los registros A y AAAA en la capa de red

Algunos clientes VPN interfieren con los registros A y AAAA (es decir, solo redirigen estos tipos de registro) mientras dejan otros tipos de registro solos. En este caso, el URC se comunica con el Umbrella resolver sin problema para TXT, y más. pero, en la práctica, no se aplica ninguna protección porque los registros A y AAAA no se responden mediante la resolución de Umbrella. Antes de aplicar la protección de DNS, el URC comprueba las interferencias de los registros A y AAAA enviando algunos registros de prueba a Umbrella. Si la respuesta no regresa o no es lo que se espera, la URC suspende la protección. Debido a que en este caso no se desencadenan eventos de red, el URC comprueba periódicamente esta condición. Este mecanismo también puede activarse en presencia de un proxy de software como Netskope.

Otros casos

Algunos clientes VPN tienen compatibilidad explícita añadida por Umbrella. Esta compatibilidad es explícita para el cliente VPN Dell (Aventail) y el cliente Pulse Secure en el futuro.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).