Understand Third-Party VPN Detection Heuristics with the Umbrella Roaming Client

Contents

Introduction

This document describes the Umbrella client's third-party VPN detection heuristics.

Background Information

The Umbrella client has implemented automated detection mechanisms to react to VPN changes to ensure that DNS functionality is maintained. This can cause the client to temporarily remain unprotected while the VPN is connected. We summarize these mechanisms below.

Third-Party VPN Detection Heuristics

This document discusses three different generic heuristics the Umbrella Roaming Client (URC) uses to detect VPN activity on a Windows system in order to suspend DNS protection activity to avoid conflicting with the VPN client. A suspended protection roaming client enters the unprotected state.

Case 1: VPN client prepends the list of DNS resolvers with its own DNS IP address

When the URC is actively redirecting traffic to an Umbrella resolver, the various network adapters on the system are set to use 127.0.0.1 or ::1 as their DNS server (the URC runs a local DNS proxy on that IP address, listening on port 53). When a network event is detected, and the DNS settings have been changed, the URC looks for 127.0.0.1 or ::1 (depending on the network stack, 127.0.0.1 for IPv4 and ::1 for IPv6) in the list of DNS IP addresses for each network adapter. If found, and if an IP address has been prefixed (for example 10.0.0.23, 192.168.2.23, 127.0.0.1 DNS settings), then the URC suspends protection. This state remains in effect until the number of active network interfaces changes and resets the client state.

Case 2: VPN client monitors and resets the DNS resolvers when they change

Some VPN clients, after setting DNS configuration, actively monitor these settings, and reset them if they deviate from the configuration specified by the VPN client. The URC monitors for DNS address reversions, and if reversions happen 3 times within 20 seconds the URC suspends protection. This covers any revert that occurs on a cadence of every 5 seconds or less. This situation remains in effect until the number of active network interfaces changes and the client state resets.

Case 3: VPN client intercepts and redirects A and AAAA records at the network layer

Some VPN clients interfere with A and AAAA records (that is, they redirect these record types only) while leaving other record types alone. In this case, the URC communicates with the Umbrella resolver without issue for TXT, and more. records, but effectively no protection is applied because A and AAAA records are not answered via the Umbrella resolver. Before actually applying DNS protection, the URC checks for A

and AAAA record interference by sending some test records to Umbrella. If the response either does not come back or is not what is expected, the URC suspends protection. Because no network events triggered in this case, the URC periodically checks this condition. This mechanism can also trigger in the presence of a software proxy like Netskope.

Other cases

Some VPN clients have explict compatibility added by Umbrella. This support is explicit for the Dell (Aventail) VPN client and the Pulse Secure client in the future.