

Begrijp VPN-detectieheuristieken van derden met de Umbrella Roaming Client

Inhoud

[Inleiding](#)

[Achtergrondinformatie](#)

[VPN-detectieheuristieken van derden](#)

Inleiding

Dit document beschrijft de VPN-detectieheuristieken van derden van de Umbrella-client.

Achtergrondinformatie

De Umbrella-client heeft geautomatiseerde detectiemechanismen geïmplementeerd om te reageren op VPN-wijzigingen om ervoor te zorgen dat de DNS-functionaliteit wordt gehandhaafd. Dit kan ertoe leiden dat de client tijdelijk onbeschermd blijft terwijl de VPN is verbonden. We vatten deze mechanismen hieronder samen.

VPN-detectieheuristieken van derden

Dit document bespreekt drie verschillende generieke heuristieken die de Umbrella Roaming Client (URC) gebruikt om VPN-activiteiten op een Windows-systeem te detecteren om de DNS-beveiligingsactiviteit op te schorten om conflicten met de VPN-client te voorkomen. Een opgeschorte bescherming roamingclient komt in de onbeschermd staat.

Geval 1: VPN-client stelt de lijst met DNS-resolvers op met een eigen DNS IP-adres

Wanneer de URC actief verkeer doorstuurt naar een Umbrella resolver, worden de verschillende netwerkadapters op het systeem ingesteld op gebruik van 127.0.0.1 of ::1 als hun DNS-server (de URC voert een lokale DNS-proxy uit op dat IP-adres, luisterend naar poort 53). Wanneer een netwerkgebeurtenis wordt gedetecteerd en de DNS-instellingen zijn gewijzigd, zoekt de URC naar 127.0.0.1 of ::1 (afhankelijk van de netwerkstack, 127.0.0.1 voor IPv4 en ::1 voor IPv6) in de lijst met DNS IP-adressen voor elke netwerkadapter. Indien gevonden, en als een IP-adres is voorafgegaan (bijvoorbeeld 10.0.0.23, 192.168.2.23, 127.0.0.1 DNS-instellingen), dan is de URC opgeschort bescherming. Deze status blijft van kracht totdat het aantal actieve netwerkinterfaces verandert en de status van de client opnieuw wordt ingesteld.

Geval 2: VPN-client bewaakt en reset de DNS-resolvers wanneer ze veranderen

Sommige VPN-clients controleren deze instellingen actief na het instellen van de DNS-configuratie en stellen ze opnieuw in als ze afwijken van de configuratie die is opgegeven door de VPN-client.

De URC bewaakt voor DNS-adresomkeringen en als omkeringen 3 keer binnen 20 seconden plaatsvinden, schort de URC de bescherming op. Dit omvat elke omkering die plaatsvindt op een cadans van elke 5 seconden of minder. Deze situatie blijft van kracht totdat het aantal actieve netwerkinterfaces verandert en de clientstatus wordt hersteld.

Geval 3: VPN-client onderschept en stuurt A- en AAAA-records door op de netwerklaag

Sommige VPN-clients interfereren met A- en AAAA-records (dat wil zeggen dat ze alleen deze recordtypen omleiden) terwijl andere recordtypen alleen worden gelaten. In dit geval communiceert de URC met de Umbrella resolver zonder probleem voor TXT, en meer. records, maar effectief wordt geen bescherming toegepast omdat A- en AAAA-records niet worden beantwoord via de Umbrella resolver. Voordat de URC DNS-bescherming daadwerkelijk toepast, controleert de URC op A- en AAAA-recordinterferentie door enkele testrecords naar Umbrella te sturen. Als de reactie niet terugkomt of niet is wat wordt verwacht, schort de URC de bescherming op. Omdat er in dit geval geen netwerkgebeurtenissen zijn geactiveerd, controleert de URC deze voorwaarde periodiek. Dit mechanisme kan ook worden geactiveerd in de aanwezigheid van een softwareproxy zoals Netskope.

Andere gevallen

Sommige VPN-clients hebben expliciete compatibiliteit toegevoegd door Umbrella. Deze ondersteuning is expliciet voor de Dell (Aventail) VPN-client en de Pulse Secure-client in de toekomst.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.