Überblick über die Heuristiken der VPN-Erkennung von Drittanbietern mit dem Umbrella Roaming Client

Inhalt

Einleitung

In diesem Dokument wird die Heuristik zur VPN-Erkennung des Umbrella-Clients von Drittanbietern beschrieben.

Hintergrundinformationen

Der Umbrella-Client hat automatisierte Erkennungsmechanismen implementiert, um auf VPN-Änderungen zu reagieren und so sicherzustellen, dass die DNS-Funktionalität erhalten bleibt. Dies kann dazu führen, dass der Client vorübergehend ungeschützt bleibt, während das VPN verbunden ist. Diese Mechanismen werden im Folgenden zusammengefasst.

Heuristik zur VPN-Erkennung von Drittanbietern

In diesem Dokument werden drei verschiedene generische Heuristiken erläutert, die der Umbrella Roaming Client (URC) verwendet, um VPN-Aktivitäten auf einem Windows-System zu erkennen und so die DNS-Schutzaktivitäten auszusetzen, um Konflikte mit dem VPN-Client zu vermeiden. Ein Roaming-Client mit angehaltenem Schutz wechselt in den ungeschützten Zustand.

Fall 1: VPN-Client stellt Liste der DNS-Resolver eine eigene DNS-IP-Adresse voran

Wenn der URC den Datenverkehr aktiv an einen Umbrella-Resolver umleitet, verwenden die verschiedenen Netzwerkadapter des Systems 127.0.0.1 oder ::1 als ihren DNS-Server (der URC führt einen lokalen DNS-Proxy auf dieser IP-Adresse aus und überwacht Port 53). Wenn ein Netzwerkereignis erkannt wird und die DNS-Einstellungen geändert wurden, sucht der URC in der Liste der DNS-IP-Adressen für jeden Netzwerkadapter nach 127.0.0.1 oder ::1 (je nach Netzwerkstapel, 127.0.0.1 für IPv4 und ::1 für IPv6). Wenn eine gefundene IP-Adresse mit einem Präfix versehen wurde (z. B. DNS-Einstellungen für 10.0.0.23, 192.168.2.23 oder 127.0.0.1), wird der Schutz durch den URC ausgesetzt. Dieser Status bleibt aktiv, bis sich die Anzahl der aktiven Netzwerkschnittstellen ändert und den Client-Status zurücksetzt.

Fall 2: VPN-Client überwacht und setzt die DNS-Resolver zurück, wenn sie sich ändern

Einige VPN-Clients überwachen diese Einstellungen nach dem Einrichten der DNS-Konfiguration aktiv und setzen sie zurück, wenn sie von der vom VPN-Client festgelegten Konfiguration abweichen. Der URC überwacht die DNS-Adressumkehr. Wenn die Umkehr innerhalb von 20 Sekunden dreimal erfolgt, setzt der URC den Schutz aus. Dies gilt für alle Reverts, die bei einem Rhythmus von höchstens 5 Sekunden auftreten. Diese Situation bleibt so lange bestehen, bis sich die Anzahl der aktiven Netzwerkschnittstellen ändert und der Client-Status zurückgesetzt wird.

Fall 3: VPN-Client fängt A- und AAAA-Datensätze auf Netzwerkebene ab und leitet sie um

Einige VPN-Clients stören A- und AAAA-Datensätze (d. h. sie leiten nur diese Datensatztypen um), während andere Datensatztypen ungestört bleiben. In diesem Fall kommuniziert der URC mit dem Umbrella Resolver ohne Probleme mit TXT usw. Datensätze, aber es wird praktisch kein Schutz angewendet, da A- und AAAA-Datensätze nicht über den Umbrella Resolver beantwortet werden. Bevor der DNS-Schutz tatsächlich angewendet wird, überprüft der URC einige Testdatensätze an Umbrella auf eine A- und AAAA-Datensatzstörung. Wenn die Antwort nicht zurückkommt oder den Erwartungen nicht entspricht, setzt der URC den Schutz aus. Da in diesem Fall keine Netzwerkereignisse ausgelöst werden, überprüft der URC diese Bedingung regelmäßig. Dieser Mechanismus kann auch bei Vorhandensein eines Software-Proxys wie Netskope ausgelöst werden.

Andere Fälle

Einige VPN-Clients verfügen über eine von Umbrella hinzugefügte explizite Kompatibilität. Diese Unterstützung ist explizit für den VPN-Client von Dell (Aventail) und den Pulse Secure-Client in der Zukunft vorgesehen.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.