# 使用Umbrella漫遊客戶端瞭解第三方VPN檢測試探法

## 目錄



## 簡介

本檔案介紹Umbrella使用者端的第三方VPN檢測試探法。

## 背景資訊

Umbrella客戶端已實施自動檢測機制來響應VPN更改，以確保維持DNS功能。這可能導致客戶端在VPN連線時暫時處於未保護狀態。我們總結以下這些機制。

## 第三方VPN檢測試探法

本文檔討論傘狀漫遊客戶端(URC)用於檢測Windows系統上的VPN活動以避免與VPN客戶端衝突的3種不同的一般啟發式方法，以便暫停DNS保護活動。暫停的保護漫遊客戶端進入未保護狀態。

案例 1:VPN客戶端使用自己的DNS IP地址在DNS解析器清單前新增字首

當URC主動將流量重新導向到Umbrella解析程式時，系統上的各種網路介面設定為使用127.0.0.1或::1作為其DNS伺服器（URC在該IP位址上執行本地DNS代理，在連線埠53上偵聽）。 檢測到網路事件且DNS設定已更改時，URC將在每個網路介面卡的DNS IP地址清單中查詢127.0.0.1或::1（具體取決於網路堆疊，127.0.0.1用於IPv4,127.0.0.1用於IPv6）或::1。如果找到IP地址，且其IP地址已預先設定（例如10.0.0.23、192.168.2.23、127.0.0.1 DNS設定），則URC會暫停保護。 此狀態將一直生效，直到活動網路介面的數量發生變化並重置客戶端狀態為止。

案例 2:VPN客戶端在DNS解析器更改時監控並重置

某些VPN客戶端在設定DNS配置後，主動監視這些設定，並在這些設定與VPN客戶端指定的配置不同時重置這些設定。 URC會監視DNS地址還原，如果在20秒內發生3次還原，則URC會暫停保護。這涵蓋每5秒或更短時間間隔內發生的任何恢復。在活動網路介面數量發生變化且客戶端狀態重置之前，此情況始終有效。

案例 3:VPN客戶端在網路層截獲和重新定向A和AAAA記錄

有些VPN客戶端會干擾A和AAAA記錄（也就是說，它們僅重定向這些記錄型別），而保留其他記錄型別為獨有。 在這種情況下，URC會與Umbrella解析程式進行通訊，而不會出現TXT等更多問題。記錄，但實際上未應用任何保護，因為A和AAAA記錄未通過Umbrella解析程式應答。在實際應用

DNS保護之前，URC通過向Umbrella傳送一些測試記錄來檢查A和AAAA記錄干擾。如果響應未恢復或者未達到預期，則URC將暫停保護。 由於在這種情況下不會觸發任何網路事件，因此URC會定期檢查此情況。此機制也可以在像Netskope這樣的軟體代理存在時觸發。

其他案件

有些VPN客戶端已解釋了Umbrella新增的相容性。此支援明確面向未來的Dell(Aventail)VPN客戶端和Pulse Secure客戶端。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。