Umbrella Roaming Client를 사용한 서드파티 VPN 탐지 휴리스틱 이해

목차

소개

이 문서에서는 Umbrella 클라이언트의 서드파티 VPN 탐지 추측에 대해 설명합니다.

배경 정보

Umbrella 클라이언트는 VPN 변경에 대응하여 DNS 기능이 유지되도록 자동화된 탐지 메커니즘을 구현했습니다. 이로 인해 VPN이 연결되는 동안 클라이언트가 일시적으로 보호되지 않은 상태로 유지될 수 있습니다. 이러한 메커니즘을 아래에 요약합니다.

서드파티 VPN 탐지 휴리스틱

이 문서에서는 URC(Umbrella Roaming Client)가 VPN 클라이언트와의 충돌을 방지하기 위해 DNS 보호 활동을 일시 중단하기 위해 Windows 시스템에서 VPN 활동을 탐지하는 데 사용하는 세 가지 일반적인 휴리스틱에 대해 설명합니다. 일시 중단된 보호 로밍 클라이언트가 보호되지 않은 상태로 들어갑니다.

사례 1: VPN 클라이언트는 DNS 리졸버 목록 앞에 자체 DNS IP 주소를 추가합니다

URC가 능동적으로 트래픽을 Umbrella 확인기로 리디렉션하는 경우 시스템의 다양한 네트워크 어댑터는 127.0.0.1 또는 ::1을 DNS 서버로 사용하도록 설정됩니다(URC는 포트 53에서 수신 대기, 해당 IP 주소에서 로컬 DNS 프록시를 실행함). 네트워크 이벤트가 탐지되고 DNS 설정이 변경된 경우 URC는 각 네트워크 어댑터의 DNS IP 주소 목록에서 127.0.0.1 또는 ::1(네트워크 스택에 따라 IPv4는 127.0.0.1, IPv6는 ::1)을 찾습니다. IP 주소가 앞에 붙으면(예: 10.0.0.23, 192.168.2.23, 127.0.0.1 DNS 설정) URC는 보호를 일시 중단합니다. 이 상태는 활성 네트워크 인터페이스의 수가 변경되고 클라이언트 상태가 재설정될 때까지 유효합니다.

사례 2: VPN 클라이언트는 DNS 확인자가 변경될 때 이를 모니터링하고 재설정합니다

일부 VPN 클라이언트는 DNS 컨피그레이션을 설정한 후 이러한 설정을 능동적으로 모니터링하고 VPN 클라이언트에서 지정한 컨피그레이션에서 벗어나는 경우 재설정합니다. URC는 DNS 주소 반전을 모니터링하며, 20초 내에 3번 반전이 발생하면 URC는 보호를 중단합니다. 이는 5초 이하의 주기로 발생하는 모든 되돌리기를 포함합니다. 이 상황은 활성 네트워크 인터페이스의 수가 변경되고 클라이언트 상태가 재설정될 때까지 계속 적용됩니다.

사례 3: VPN 클라이언트는 네트워크 레이어에서 A 및 AAAA 레코드를 가로채고 리디렉션합니다.

일부 VPN 클라이언트는 A 및 AAAA 레코드를 간섭하지만(즉, 이러한 레코드 유형만 리디렉션) 다른 레코드 유형만 남겨 둡니다. 이 경우, URC는 TXT 등에 대한 문제 없이 Umbrella 레졸버와 통신합니다. A 및 AAAA 레코드는 Umbrella 확인기를 통해 응답하지 않으므로 레코드는 사실상 보호가 적용되지 않습니다. 실제로 DNS 보호를 적용하기 전에 URC는 일부 테스트 레코드를 Umbrella로 전송하여 A 및 AAAA 레코드 간섭을 확인합니다. 응답이 반환되지 않거나 예상과 다른 경우 URC는 보호를 중단합니다. 이 경우 트리거되는 네트워크 이벤트가 없으므로 URC는 주기적으로 이 조건을 확인합니다. 이 메커니즘은 Netskope와 같은 소프트웨어 프록시가 있는 경우에도 트리거될 수 있습니다.

기타 케이스

일부 VPN 클라이언트는 Umbrella에서 명시적 호환성을 추가했습니다. 이 지원은 향후 Dell(Aventail) VPN 클라이언트 및 Pulse Secure 클라이언트에 명시적으로 제공됩니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.