Entender a Heurística de Detecção de VPN de Terceiros com o Umbrella Roaming Client

Contents

Introdução

Este documento descreve a heurística de detecção de VPN de terceiros do cliente Umbrella.

Informações de Apoio

O cliente Umbrella implementou mecanismos de detecção automatizados para reagir a alterações de VPN para garantir que a funcionalidade de DNS seja mantida. Isso pode fazer com que o cliente permaneça temporariamente desprotegido enquanto a VPN está conectada. Resumimos esses mecanismos abaixo.

Heurística de detecção de VPN de terceiros

Este documento discute três heurísticas genéricas diferentes que o Umbrella Roaming Client (URC) usa para detectar atividade de VPN em um sistema Windows a fim de suspender a atividade de proteção de DNS para evitar o conflito com o cliente VPN. Um cliente móvel de proteção suspensa entra no estado desprotegido.

Caso 1: O cliente VPN acrescenta à lista de resolvedores DNS seu próprio endereço IP DNS

Quando o URC está redirecionando ativamente o tráfego para um resolvedor Umbrella, os vários adaptadores de rede no sistema são definidos para usar 127.0.0.1 ou ::1 como seu servidor DNS (o URC executa um proxy DNS local nesse endereço IP, ouvindo na porta 53). Quando um evento de rede é detectado e as configurações DNS foram alteradas, o URC procura 127.0.0.1 ou ::1 (dependendo da pilha da rede, 127.0.0.1 para IPv4 e ::1 para IPv6) na lista de endereços IP DNS para cada adaptador de rede. Se encontrado, e se um endereço IP tiver sido prefixado (por exemplo, 10.0.0.23, 192.168.2.23, 127.0.0.1 configurações DNS), o URC suspenderá a proteção. Esse estado permanece em vigor até que o número de interfaces de rede ativas mude e redefina o estado do cliente.

Caso 2: O cliente VPN monitora e redefine os resolvedores DNS quando eles mudam

Alguns clientes VPN, depois de definir a configuração DNS, monitoram ativamente essas configurações e as redefinem se desviarem da configuração especificada pelo cliente VPN. O

URC monitora as reversões de endereço DNS e, se as reversões ocorrerem 3 vezes em 20 segundos, o URC suspende a proteção. Isso abrange qualquer reversão que ocorra em uma cadência de 5 segundos ou menos. Essa situação permanece em vigor até que o número de interfaces de rede ativas mude e o estado do cliente seja redefinido.

Caso 3: O cliente VPN intercepta e redireciona registros A e AAAA na camada de rede

Alguns clientes VPN interferem nos registros A e AAAA (ou seja, eles redirecionam apenas esses tipos de registro) enquanto deixam outros tipos de registro sozinhos. Nesse caso, o URC se comunica com o Umbrella Resolver sem problemas para TXT e muito mais. registros, mas efetivamente nenhuma proteção é aplicada porque os registros A e AAAA não são respondidos através do Umbrella resolver. Antes de realmente aplicar a proteção DNS, o URC verifica a interferência de registros A e AAAA enviando alguns registros de teste para o Umbrella. Se a resposta não voltar ou não for o esperado, o URC suspende a proteção. Como nenhum evento de rede disparado nesse caso, o URC verifica periodicamente essa condição. Esse mecanismo também pode ser acionado na presença de um proxy de software como o Netskope.

Outros casos

Alguns clientes VPN têm compatibilidade explícita adicionada pelo Umbrella. Este suporte é explícito para o cliente VPN da Dell (Aventail) e o cliente Pulse Secure no futuro.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.