Comprendere l'euristica di rilevamento VPN di terze parti con il client di roaming Umbrella

Sommario

Introduzione

Questo documento descrive l'euristica di rilevamento VPN di terze parti del client Umbrella.

Premesse

Il client Umbrella ha implementato meccanismi di rilevamento automatico per reagire alle modifiche VPN per garantire il mantenimento della funzionalità DNS. In questo modo il client potrebbe rimanere temporaneamente non protetto mentre la VPN è connessa. Riassumiamo questi meccanismi qui di seguito.

Euristica di rilevamento VPN di terze parti

In questo documento vengono descritte tre diverse euristiche generiche utilizzate da Umbrella Roaming Client (URC) per rilevare l'attività VPN su un sistema Windows in modo da sospendere l'attività di protezione DNS per evitare conflitti con il client VPN. Un client in roaming con protezione sospesa entra nello stato non protetto.

Caso 1: Il client VPN precede l'elenco dei resolver DNS con il proprio indirizzo IP DNS

Quando l'URC reindirizza attivamente il traffico a un sistema di risoluzione Umbrella, le varie schede di rete del sistema sono impostate per utilizzare 127.0.0.1 o ::1 come server DNS (l'URC esegue un proxy DNS locale su tale indirizzo IP, in ascolto sulla porta 53). Quando viene rilevato un evento di rete e le impostazioni DNS sono state modificate, l'URC cerca 127.0.0.1 o ::1 (a seconda dello stack di rete, 127.0.0.1 per IPv4 e ::1 per IPv6) nell'elenco di indirizzi IP DNS per ogni scheda di rete. Se viene trovato un indirizzo IP con prefisso (ad esempio, 10.0.0.23, 192.168.2.23, 127.0.0.1 impostazioni DNS), l'URC sospende la protezione. Questo stato rimane attivo fino a quando il numero di interfacce di rete attive non viene modificato e lo stato del client non viene reimpostato.

Caso 2: Il client VPN esegue il monitoraggio e la reimpostazione dei resolver DNS quando vengono modificati

Alcuni client VPN, dopo aver impostato la configurazione DNS, monitorano attivamente queste

impostazioni e le reimpostano se deviano dalla configurazione specificata dal client VPN. L'URC monitora le reversioni degli indirizzi DNS e se le reversioni avvengono 3 volte entro 20 secondi l'URC sospende la protezione. In questo modo vengono coperti tutti i ripristini che si verificano a una cadenza pari o inferiore a 5 secondi. Questa situazione rimane attiva fino a quando il numero di interfacce di rete attive non viene modificato e lo stato del client non viene ripristinato.

Caso 3: Il client VPN intercetta e reindirizza i record A e AAAA a livello di rete

Alcuni client VPN interferiscono con i record A e AAAA, ovvero reindirizzano solo questi tipi di record, lasciando gli altri tipi di record da soli. In questo caso, l'URC comunica con il risolutore Umbrella senza problemi per TXT, e altro ancora. ma non viene applicata alcuna protezione poiché i record A e AAAA non ricevono risposta tramite il sistema di risoluzione Umbrella. Prima di applicare effettivamente la protezione DNS, l'URC verifica l'interferenza tra i record A e AAAA inviando alcuni record di test a Umbrella. Se la risposta non ritorna o non è quella prevista, l'URC sospende la protezione. Poiché in questo caso non viene attivato alcun evento di rete, l'URC controlla periodicamente questa condizione. Questo meccanismo può essere attivato anche in presenza di un proxy software come Netskope.

Altri casi

Alcuni client VPN hanno compatibilità esplicita aggiunta da Umbrella. Questo supporto è esplicito per il client VPN Dell (Aventail) e il client Pulse Secure in futuro.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).