Configura Umbrella per bloccare Tor

Sommario

Introduzione

Questo documento descrive come bloccare Tor con Umbrella.

Panoramica

La rete Tor utilizza relè gestiti da volontari per ospitare una rete anonima distribuita. Garantisce che nessun singolo punto possa collegare un utente alla sua destinazione, con l'obiettivo di ridurre i rischi dell'analisi del traffico. Anche se Tor ha molti usi legittimi, ci sono ragioni per cui un amministratore di rete vuole bloccare tutto il traffico basato su Tor su una rete aziendale.

In breve, non è possibile bloccare completamente Tor con Umbrella. Quando si blocca la categoria Proxy/Anonimizzatore, torproject.org viene bloccato; tuttavia, i dispositivi di proprietà dell'utente potrebbero avere già installato il browser Tor e collegarlo alla rete.

Spiegazione

Tor funge da proxy. Dopo aver aperto una connessione TCP, al nodo di uscita viene inviato un payload che codifica l'indirizzo e la porta dell'host di destinazione. Alla ricezione di questo messaggio, il nodo di uscita risolve l'indirizzo come necessario.

Per ulteriori informazioni, leggere quanto segue:

- I servizi Tor Onion utilizzano il TLD .onion, che non è riconosciuto dai server DNS radice. Tor è necessario per accedere ai domini .onion.
- Il modo più comune per bloccare il traffico Tor sarebbe quello di individuare un elenco di aggiornamento dei nodi di uscita Tor e configurare un firewall per bloccare questi nodi. Anche una politica aziendale per prevenire l'uso di Tor può fare molto per smettere di usarlo.
- Sfortunatamente, le singole configurazioni non sono qualcosa che OpenDNS/Cisco Umbrella è in grado di supportare, in quanto ogni firewall ha un'interfaccia di configurazione unica e queste variano molto. In caso di dubbi, è possibile controllare la documentazione del router o del firewall o contattare il produttore per verificare se è possibile.

Per ulteriori informazioni sul blocco di Tor, vedere le [domande frequenti sugli abusi del progetto Tor](#). Le domande frequenti collegate sono rivolte principalmente ai provider di servizi che desiderano impedire agli utenti Tor di accedere ai propri servizi, ma contengono anche

collegamenti utili per gli amministratori di rete.

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).