Rivelato un nuovo metodo per identificare gli indirizzi IP su Tor

Maria Cattini | 29/06/2023 | Tips tools

Cosa significa per l'anonimato nel Dark Web

Rivelato un nuovo metodo per identificare gli indirizzi IP su Tor.

Il browser Tor è da tempo noto per offrire agli utenti un elevato livello di anonimato e protezione contro l'identificazione e il tracciamento online.

Tuttavia, una recente scoperta ha sollevato preoccupazioni sulla vulnerabilità di questa protezione. Secondo il sito di sicurezza informatica e cybercrime Red Hot Cyber, è stato individuato un nuovo metodo che consente di rilevare gli indirizzi IP reali degli utenti che utilizzano Tor attraverso un'intestazione HTTP chiamata Etag.

Rilevare gli indirizzi IP su Tor tramite l'utilizzo dell'Etag

L'Etag è un identificatore univoco generato dal server quando un client richiede una risorsa. Viene utilizzato per determinare se la versione della risorsa è aggiornata e, se non cambia, il client passa alla versione in cache, ottimizzando così i download. Tuttavia, l'Etag può anche essere utilizzato come strumento di tracciamento, poiché può contenere informazioni sensibili come l'indirizzo IP del server, l'ora o l'hash.

La scoperta evidenzia che quando si richiede la stessa risorsa da diversi servizi Tor nascosti appartenenti allo stesso server, il client può ricevere lo stesso Etag, rivelando così l'indirizzo IP reale del server. Un esempio pratico di questa vulnerabilità è stato dimostrato attraverso un articolo su Medium, in cui l'utilizzo degli strumenti curl e torsocks ha consentito di rivelare l'indirizzo IP di un servizio Tor legato al ransomware RagnarLocker. Tutti gli Etag sono risultati identici e contenevano un hash dell'indirizzo IP del server, fornendo così l'indirizzo e la posizione reali.

Implicazioni per l'anonimato e la lotta alle attività illegali

Questo nuovo metodo di rilevamento degli indirizzi IP su Tor ha implicazioni significative per l'anonimato nel Dark Web. Mentre gli utenti si affidano a Tor per nascondere la propria identità online, questa vulnerabilità mette in discussione l'efficacia di tale anonimato. Inoltre, è importante considerare il ruolo delle forze dell'ordine nella lotta alle attività illegali su Tor. L'utilizzo di questo metodo potrebbe consentire loro di identificare utenti e fornitori di servizi nascosti, aprendo nuove prospettive nella lotta contro la criminalità online.

Misure di protezione e mitigazione

Nonostante questa scoperta preoccupante, Red Hot Cyber suggerisce alcune misure che possono essere adottate per proteggersi da questa vulnerabilità. Una soluzione è disabilitare l'Etag sul server, in modo che non venga generato e trasmesso ai client. Un'altra opzione è utilizzare un proxy per modificare l'Etag in transito, in modo da evitare la correlazione

Cosa sono gli Indirizzi IP?

Un indirizzo IP (Internet Protocol) è un identificatore unico assegnato a ogni dispositivo connesso a una rete informatica che utilizza il protocollo IP.

Questo indirizzo viene utilizzato per identificare e localizzare un dispositivo all'interno di una rete, consentendo la comunicazione tra i vari dispositivi connessi a Internet.

Un indirizzo IP è costituito da una serie di numeri separati da punti, ad esempio 192.168.0.1.

Esistono due versioni principali di indirizzi IP: IPv4 (Internet Protocol versione 4) e IPv6 (Internet Protocol versione 6). IPv4 utilizza indirizzi a 32 bit e IPv6 utilizza indirizzi a 128 bit, consentendo un numero molto maggiore di combinazioni possibili.

Gli indirizzi IP sono utilizzati per indirizzare i pacchetti di dati inviati attraverso Internet.

Quando invii una richiesta a un sito web o quando ricevi una e-mail, il tuo dispositivo utilizza il proprio indirizzo IP per inviare e ricevere dati dai server che gestiscono quelle informazioni.

Gli indirizzi IP possono essere assegnati staticamente o dinamicamente.

Un indirizzo IP statico è un indirizzo fisso che viene configurato manualmente e rimane costante nel tempo.

Al contrario, un indirizzo IP dinamico viene assegnato automaticamente da un server DHCP (Dynamic Host Configuration Protocol) e può cambiare periodicamente.

In sintesi, gli indirizzi IP sono identificatori unici che consentono la comunicazione tra dispositivi collegati a Internet. Grazie a questi indirizzi, i dati possono essere inviati e ricevuti correttamente tra i vari dispositivi all'interno di una rete.