The Onion Router Software

Alexandre Costa[1] [48039]

Universidade de Évora, Évora, Portugal[1]

Abstract. Keywords: TOR · Navegador

1 The Onion Router

O The Onion Router (TOR), desenvolvido pelo Laboratório de Pesquisa Naval dos EUA em setembro de 2002, é uma rede de servidores distribuídos que permite a navegação anónima na internet. O TOR redireciona o tráfego da internet por uma série de computadores, tornando difícil rastrear a origem e o destino da comunicação. O navegador Tor, desenvolvido para ser usado com a rede TOR, apaga automaticamente o histórico de navegação a cada sessão e criptografa o tráfego, garantindo a privacidade e segurança dos utilizadores. Embora o TOR seja frequentemente associado à Deep Web, ele permite aceder a qualquer página da web, incluindo sites bloqueados por países.

1.1 Protocolo Onion routing

O funcionamento do Onion Routing é baseado num sistema de camadas, similar a uma cebola. As mensagens são criptografadas em várias camadas e enviadas através de diversos nós de rede, conhecidos como "roteadores cebola". Cada roteador remove uma camada de criptografia, revelando apenas as instruções de roteamento para o próximo destino.
O Onion Routing impede que os nós intermediários da rede identifiquem a origem e o destino da mensagem, protegendo a identidade dos utilizadores.
É importante ressaltar que o Onion Routing não é uma solução perfeita. A velocidade da rede pode ser inferior à de uma conexão direta, e o uso da tecnologia pode ser associado a atividades ilícitas.
A tecnologia mais utilizada para implementar o Onion Routing é o projeto Tor.

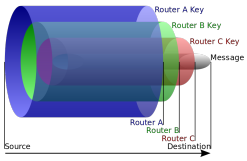

Fig. 1. Protocolo Onion routing. Fonte: Internet

1.2 O Navegador TOR

O navegador Tor, um software específico para utilizar a rede TOR, utiliza uma ampla rede de servidores distribuídos pelo mundo para ocultar o endereço IP do utilizador e proteger a sua conexão. O TOR redireciona o tráfego da internet do utilizador por uma série de servidores aleatórios, cada um criptografando o tráfego antes de enviá-lo para o próximo. O processo de navegação na rede TOR pode ser dividido em três etapas:

- Conexão à rede TOR: O navegador Tor conecta-se a um servidor de entrada TOR, que é um servidor aleatório na rede TOR.
- Routing do tráfego: O servidor de entrada criptografa o tráfego do utilizador e envia-o para um servidor intermediário TOR. O servidor intermediário criptografa o tráfego novamente e envia-o para um servidor de saída TOR.
- Saída da rede TOR: O servidor de saída TOR descriptografa o tráfego do utilizador e envia-o para o destino final.

Além disso, o TOR usa uma técnica chamada "circuito virtual" para garantir que o tráfego do utilizador não passe pelo mesmo servidor duas vezes. Isso ajuda a proteger a privacidade do utilizador e a evitar que sua identidade seja encontrada.

Fig. 2. Comunicação entre clientes TOR. Fonte: Internet

1.3 Ferramentas TOR

O TOR oferece diversas ferramentas para além do navegador Tor, como Hidden Services, OnionShare, Tails, Orbot, Vidalia, Tor Bridges, ferramentas de criptografia e segurança de rede, e ferramentas de anonimato.

Tor Hidden Services Os Tor Hidden Services são sites e serviços que só podem ser acedidos pela rede TOR. Isso torna-os muito difíceis de encontrar e bloquear. Os Tor Hidden Services são frequentemente usados por ativistas, jornalistas e outros indivíduos que precisam de proteger a sua privacidade.

OnionShare OnionShare é uma ferramenta que permite compartilhar arquivos e pastas de forma segura e anónima pela rede TOR.

Tails Tails é uma distribuição Linux live que pode ser usada para navegar na internet com segurança e anonimato. Tails é pré-configurado para usar o TOR e outras ferramentas de segurança.

Orbot Orbot é uma aplicação proxy que permite o uso do TOR com outras aplicações num dispositivo Android.

Vidalia Vidalia é uma aplicação que permite monitorizar o tráfego da rede TOR e visualizar a sua localização em tempo real

Tor Bridges Tor Bridges são servidores que permitem que se conecte à rede TOR mesmo se o TOR estiver bloqueado no país.

Ferramentas de criptografia O TOR oferece diversas ferramentas de criptografia para proteger os dados e comunicações dos utilizadores.

Ferramentas de segurança de rede O TOR oferece diversas ferramentas de segurança de rede para proteger dispositivos contra ataques. Essas ferramentas incluem TorGuard, Privoxy e uBlock Origin.

Ferramentas de anonimato O TOR oferece diversas ferramentas de anonimato para proteger a identidade online. Essas ferramentas incluem NoScript, HTTPS Everywhere e Tor Browser Bundle.

2 Conclusão

É importante ter em mente que o TOR não é uma solução perfeita. Apesar dos seus benefícios, o TOR pode ser rastreado por agências de inteligência com recursos suficientes e pode ser usado para atividades ilegais. É importante usar o TOR com cuidado e estar ciente de suas limitações.

References

1. TOR, , last accessed 2024/03/29
2. O navegador da dark web: O que é o Tor, ele é seguro e como usá-lo?, https://www.avast.com/pt-br/c-tor-dark-web-browser, last accessed 2024/03/29
3. Navegador Tor: conheça o software e veja como usá-lo, https://www.tecmundo.com.br/internet/243602-navegador-tor-conheca-software-veja-usa-lo.htm, last accessed 2024/03/29
4. What is Tor? A beginner's guide to the privacy tool, https://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser, last accessed 2024/03/30
5. Onion Routing, https://www.geeksforgeeks.org/onion-routing/, last accessed 2024/03/30