Ataques de Desanonimização Contra a Rede Tor

Leonardo Teodoro[1]

Resumo

Este artigo analisa as vulnerabilidades de segurança da rede Tor, um sistema de anonimização amplamente utilizado que emprega o "onion routing" para proteger a identidade dos usuários. O foco principal recai sobre os ataques que visam desanonimizar os clientes da rede, com ênfase no "Browser-Based Timing Attack". Nesse tipo de ataque, um invasor que controla tanto um nó de entrada quanto um nó de saída pode injetar JavaScript malicioso em páginas web, permitindo a coleta de informações sobre os usuários. O artigo também aborda técnicas de análise de tráfego que exploram padrões de conexão para identificar usuários. As defesas contra esses ataques, como a desativação da execução de JavaScript e o uso de HTTPS, são discutidas, ressaltando suas limitações. A desativação do JavaScript pode dificultar o acesso a muitos serviços web, enquanto a segurança do HTTPS depende da confiança nos certificados. Os resultados evidenciam que, apesar das defesas existentes, a segurança na rede Tor não é absoluta, o que demanda melhorias contínuas e conscientização dos usuários sobre as ameaças potenciais. Esta pesquisa contribui para a compreensão dos desafios enfrentados por redes de anonimização e enfatiza a importância de aprimorar a privacidade dos usuários em um cenário digital cada vez mais vigiado.

Palavras-chave: Tor. Anonimização. Desanonimização. Segurança. Ataques.

Abstract

This article analyzes the security vulnerabilities of the Tor network, a widely used anonymization system that employs onion routing to protect users' identities. The main focus is on attacks aimed at de-anonymizing network clients, with an emphasis on the “Browser-Based Timing Attack”. In this type of attack, an attacker who controls both an entry node and an exit node can inject malicious JavaScript into web pages, allowing information about users to be collected. The article also discusses traffic analysis techniques that exploit connection patterns to identify users. Defenses against these attacks, such as disabling JavaScript execution and using HTTPS, are discussed, highlighting their limitations. Disabling JavaScript can make it difficult to access many web services, while HTTPS security depends on trusting the certificates. The results show that, despite the existing defenses, security on the Tor network is not absolute, which requires continuous improvements and user awareness of potential threats. This research contributes to the understanding of the challenges faced by anonymization networks and emphasizes the importance of improving user privacy in an increasingly guarded digital landscape.

Keywords: Tor. Anonymization. De-anonymization. Security. Attacks.

[1] Especialista em Pentest. E-mail: teodoroleo96@gmail.com

Introdução

Nos dias atuais, a Internet representa um recurso fundamental para a vida cotidiana. Os aspectos de segurança na Internet assumem hoje um papel muito importante: sendo um elemento crucial para as atividades dos usuários, governos e sistemas de infraestrutura crítica, a Internet deve ser mantida como um local seguro para seus usuários e sistemas, garantindo comunicações seguras e garantia dos direitos dos usuários. Quando falamos de privacidade, é muito importante garantir que duas pessoas sejam capazes de trocar conteúdos e manter tanto a sua identidade quando as informações presentes nesses conteúdos ocultos.

A Internet não foi projetada com o anonimato em mente; na verdade, um dos objetivos originais do projeto era a responsabilidade. Cada pacote enviado por protocolos estabelecidos identifica ambas as partes. No entanto, a maioria dos usuários espera que suas comunicações na Internet sejam e devam permanecer anônimas.

Alguns países adotam uma política de censura e acabam prendendo pessoas por expressarem opiniões divergentes ao governo na Internet. O anonimato impede que essas opiniões sejam rastreadas até seus criadores, aumentando a liberdade de expressão.

Os sistemas de rede de anonimato foram projetados principalmente para preservar a privacidade das comunicações para usuários da Internet censurados. O anonimato é feito cobrindo os dados do usuário dentro de diferentes camadas de criptografia e encaminhando o tráfego por meio de um conjunto de nós de retransmissão/roteamento ou proxies. As redes Onion representam hoje uma das soluções disponíveis adotadas neste contexto. Essas redes são baseadas em abordagens "Onion routing", envolvendo procedimentos de criptografia tornando os nós de roteamento incapazes de ler dados trocados entre cliente e servidor.

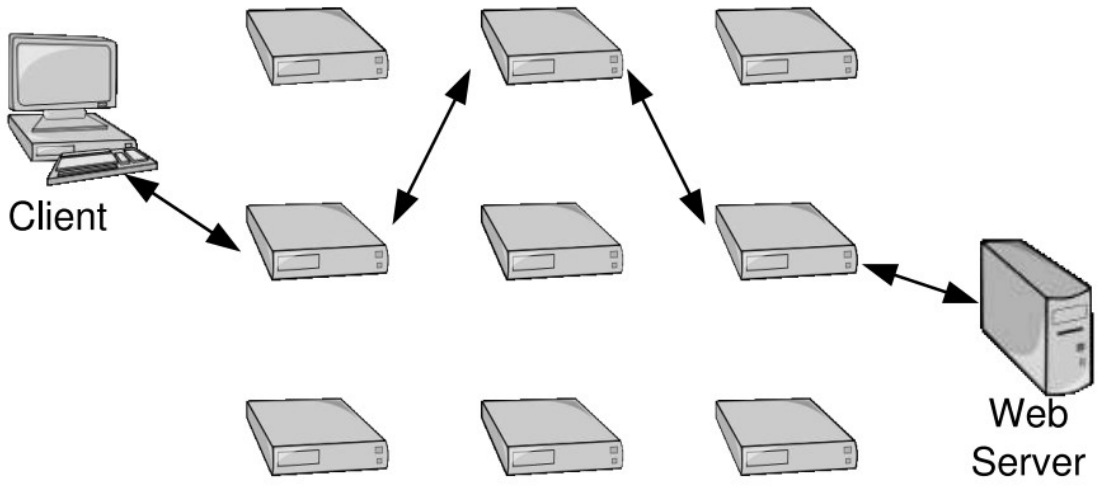
Existem várias redes de anonimização diferentes, como Freenet, I2P, MorphMix, Hornet ou Tarzan. No entanto, atualmente, a rede onion mais adotada é o Tor.

Nesse artigo, vamos focar na rede Tor, entender o seu funcionamento e abordar alguns ataques contra seus usuários.

Como o Tor funciona

O Tor é um protocolo de anonimização que usa o "onion routing" para esconder a origem do tráfego TCP. "Onion routing" é um protocolo de criptografia por camadas que foi desenvolvido primeiramente para anonimização de serviços de e-mail.

No Tor o tráfego do cliente é roteado por uma cadeia de pelo menos 3 nós que são selecionados pela rede. A comunicação entre cada nó acontece através de um "Diffie-Hellman handshakes", onde cada nó realiza uma troca de chaves simétricas para criptografia e descriptografia.



Os pacotes enviados pela rede são divididos em tamanhos fixos para que não seja possível identificar um usuário através do tamanho do pacote, e posteriormente cada pacote é criptografado sucessivamente, iniciando com a chave do nó de saída e finalizando com a chave do nó de entrada.

Usando esse protocolo o nó de entrada é o único que sabe a identidade do cliente, enquanto o nó de saída é o único que sabe o destino do pacote enviado (o site que está sendo acessado), os demais nós somente compartilham os pacotes criptografados. Os nós utilizados na comunicação são selecionados aleatóriamente e para isso são utilizados alguns dados de estatística da rede, preferências do cliente e histórico do cliente.

Tipos de ataque ao ecossistema Tor

Durante muito tempo, vários estudos foram realizados tendo como alvo a rede TOR, tendo em vista ela ser uma das redes mais utilizada hoje em dia. Considerando os aspectos de segurança da rede TOR, o atacante pode ter três tipos de alvo diferentes na rede:

- Cliente: nesse caso, o atacante tem como alvo um dos usuários da rede TOR;
- Servidor: nesse caso, um dos servidores TOR ocultos é alvo do atacante;
- Rede: nesse caso, a própria rede TOR é o alvo do atacante.

Nesse artigo vamos focar nos ataques que tem como alvo o cliente da rede e vamos descrever e analisar como esses ataques podem ser realizados para descobrir a verdadeira identidade desses usuários.

Ataques a clientes Tor

Sem dúvida, um dos maiores interesses de pesquisas e estudos realizados é de desenvolver ataques capazes de desanonimizar os usuários da rede TOR. Muitos desses estudos de fato conseguem esse resultado, seja explorando vulnerabilidades no navegador, que são removidas em atualizações, seja através de nós da rede comprometidos, as possibilidades são muitas.

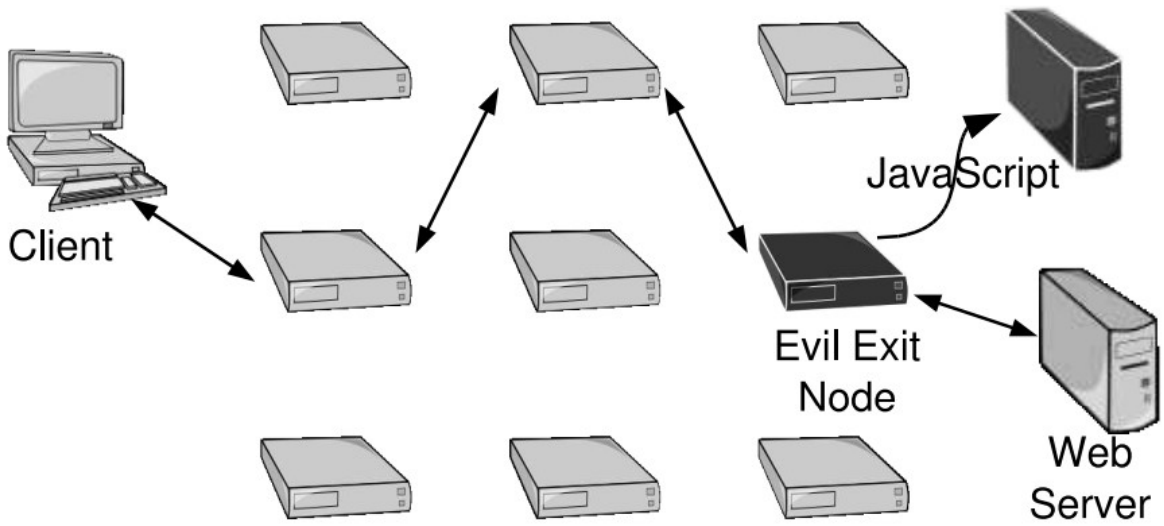
Vamos então, ver alguns desses ataques e como eles são realizados.

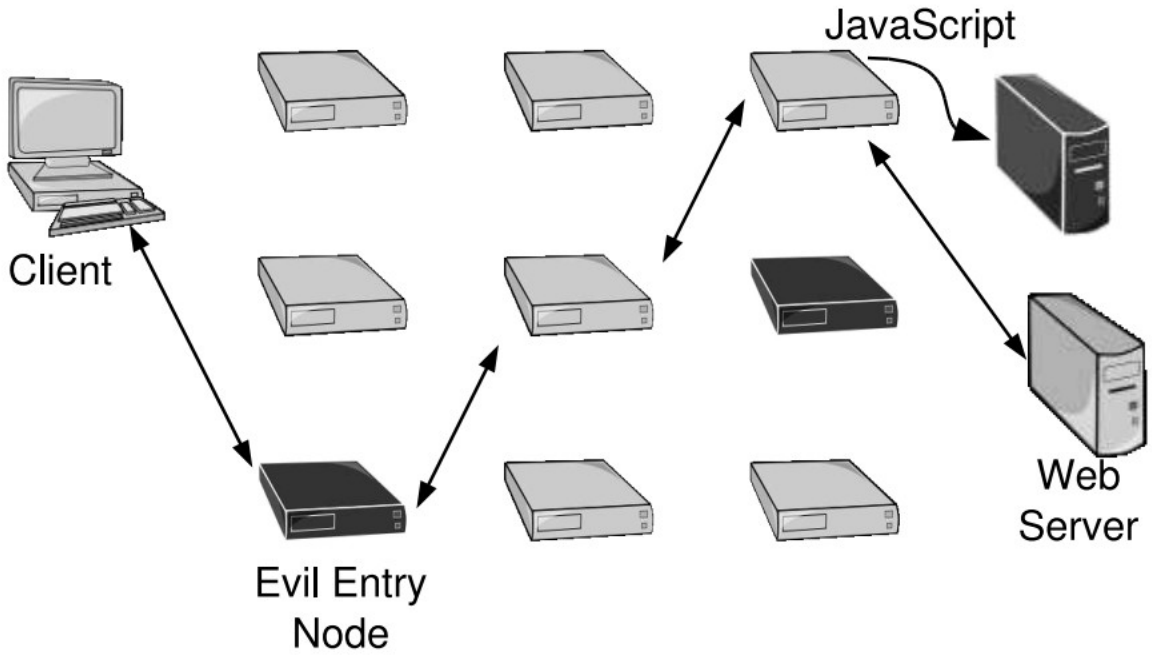
Browser-Based Timing Attack

Para realizar esse ataque, é necessário que o atacante seja o dono de dois nós na rede: um nó de entrada e um nó de saída, dessa forma é possível modificar o tráfego HTTP para inserir um iframe invisível contendo um JavaScript nas páginas solicitadas. Esse JavaScript realiza repetidas requisições para um servidor malicioso e envia um ID único para identificar o usuário posteriormente.

O passo a passo do ataque é o seguinte:

1. O atacante primeiro configura os recursos necessários.
   (a) O atacante insere dois nós maliciosos na rede Tor: um para atuar como um nó de entrada e o outro para atuar como um nó de saída.
   (b) Depois configura um servidor web que recebe e registra conexões JavaScript.
2. O nó de saída malicioso modifica todo o tráfego HTTP destinado aos clientes Tor para incluir um iframe contendo um JavaScript invisível que gera um ID único para cada cliente Tor.
3. O navegador web do cliente Tor executa o código JavaScript, enviando um ID para o servidor web. Esse tráfego passa pelo circuito Tor e o cliente ainda é anônimo.
4. Aproximadamente a cada dez minutos, o cliente Tor escolhe um novo circuito. Eventualmente, um dos clientes Tor vai escolher e usar o nó de entrada malicioso.
5. O invasor realiza uma análise de tráfego para comparar os IDs em cada circuito que passa por seu nó de entrada com os vários IDs recebidos pelo servidor web. Quando esses IDs são iguais, é possível identificar o usuário, dessa forma revelando a identidade do cliente Tor e seu histórico de tráfego correspondente durante o tempo em que usou o nó de saída malicioso.





Browser-Based Timing Attack Usando Somente HTML

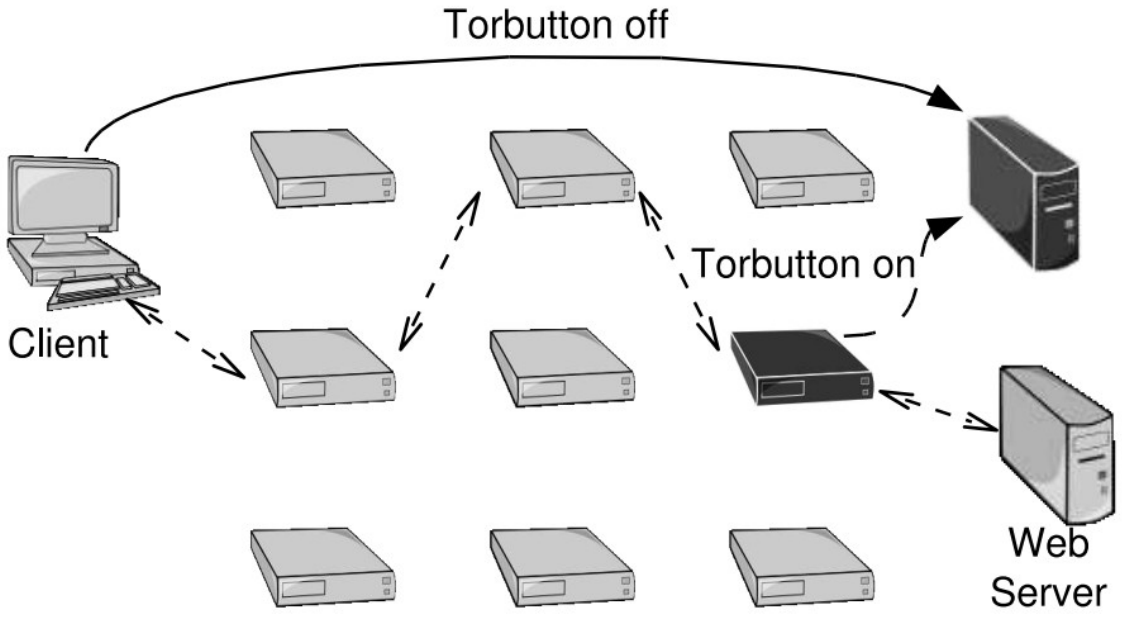
O ataque que acabamos de descrever depende de a vítima ter o JavaScript ativado. Porém caso esse recurso esteja desabilitado também é possível realizar o mesmo ataque através da tag meta do HTML. Nesta versão do ataque, a página da web é modificada para que seja atualizada automaticamente pelo navegador da web após um período de tempo. O atacante gera o sinal de tráfego desejado variando dinamicamente os atrasos de atualização ou o tamanho da página cada vez que a página da Web é atualizada.

A versão HTML do ataque é mais visível do que a versão JavaScript porque os navegadores geralmente indicam quando estão recarregando uma página da Web. Assim, é mais fácil para o usuário observar a versão HTML do ataque do que a do JavaScript. Isso pode ser mitigado executando esse ataque apenas em sites que já possuem uma tag de meta-refresh. Mesmo em páginas que normalmente não teriam a tag, o ataque HTML pode se tornar menos óbvio se a primeira atualização ocorrer com um grande atraso, quando é menos provável que o usuário esteja parado na frente do computador. Após um atraso inicial de algumas horas, as atualizações subsequentes podem ocorrer a cada poucos segundos para gerar o sinal para um ataque de temporização.

Torbutton

O Torbutton é uma extensão do Firefox que permite o usuário alternar a conexão do navegador para um proxy Tor com um único clique. Normalmente essa extensão é utilizada pela facilidade do uso da rede Tor, quando o usuário quer acessar um site que ele acredite que não precise manter o anonimato ele pode simplesmente desativar o proxy e com isso não sofre com a lentidão da rede, como acontece com o navegador.

O ataque acontece quando um usuário desativa o proxy Tor usando Torbutton, mas deixar uma guia aberta com um dos sites contendo o código JavaScript malicioso, o mesmo usado nos ataques que vimos acima. Ao desativar o proxy, na próxima requisição que o código fizer enviando o ID do usuário para o servidor malicioso, a verdadeira identidade do usuário vai ser descoberta. Na prática, esse ataque relativamente simples é eficaz, mas limitado a descobrir clientes Tor que param de usar o proxy Tor enquanto o navegador ainda está aberto. Torbutton torna mais fácil para os usuários serem descuidados desta forma.



Low-Cost Traffic Analysis of Tor

Este ataque utiliza técnicas de analise de tráfego para vincular o fluxo de conexão à quem originou essa conexão. O termo baixo custo (Low-Cost) é utilizado para indicar que o invasor não precisa de recursos de nível global, em vez disso, é necessário apenas uma visão parcial da rede. Ao contrário do que acredita os designers do Tor, os ataques de temporização são possíveis mesmo com um modelo de threads limitado.

Como até mesmo uma conexão extra em um nó Tor resulta em carga mais alta, um invasor pode se conectar por meio de nós Tor direcionados e medir as latências das mensagens. A estimativa da carga de tráfego de um nó Tor pode ser analisada em relação ao padrão de tráfego conhecido.

De acordo com Murdoch e Danezis, uma variante desse ataque pode conter um servidor malicioso, que envia dados para a vítima em um padrão. Esse padrão é observado criando uma conexão por meio dos roteadores onion candidatos e executando a análise de tráfego.

Defesa contra os principais ataques

Analisando os ataques citados acima, podemos definir alguns tipos de defesa contra eles.

Desativar a Execução de JavaScript

A principal defesa contra ataques baseados em navegador é desabilitar todos os sistemas de conteúdo ativo, como Java e JavaScript no navegador. A desvantagem dessa defesa, no entanto, é que desativar os sistemas de conteúdo ativo impediria o uso de muitos serviços da Web populares no processo.

O ataque utilizando somente HTML através da tag meta também mostra que essa defesa tem as suas limitações e não resolve 100% dos problemas.

HTTPS

O uso do HTTPS impede que um nó de saída malicioso leia ou modifique os dados que está transportando. Na prática, essa defesa só será eficaz se o usuário

também fizer a sua parte e não aceitar o uso de certificados autoassinados.

O uso de HTTPS fornece segurança razoável contra esse ataque, desde que o cliente possa confiar e verificar corretamente os certificados. Se o servidor não for confiável, ele pode incluir o código de ataque JavaScript malicioso no próprio site e assiná-lo com um certificado SSL válido. Usando os métodos que descrevemos, o servidor pode identificar seus visitantes.

Considerações Finais

A rede Tor desempenha um papel crucial na promoção da privacidade e anonimato na internet, especialmente em contextos onde a liberdade de expressão é ameaçada. No entanto, como demonstrado ao longo deste artigo, a segurança da rede não é infalível. Os ataques direcionados a clientes Tor, como o "Browser-Based Timing Attack", evidenciam as vulnerabilidades que podem ser exploradas por agentes maliciosos, comprometendo a identidade e a segurança dos usuários.

É fundamental que os usuários da rede Tor estejam cientes dos riscos associados e adotem práticas de segurança, como a desativação de JavaScript e a utilização de conexões HTTPS, embora essas medidas não garantam proteção total. Além disso, a comunidade de desenvolvedores e pesquisadores devem continuar a investigar e implementar melhorias na arquitetura da rede Tor, visando fortalecer suas defesas contra ataques emergentes.

A privacidade na internet é um direito essencial, e a proteção dos usuários deve ser uma prioridade contínua. À medida que a vigilância digital se intensifica, a necessidade de redes de anonimização robustas e eficazes se torna ainda mais premente. Portanto, é imperativo que tanto os usuários quanto os desenvolvedores permaneçam vigilantes e proativos na busca por soluções que garantam um ambiente online seguro e anônimo.

Referências

Enrico Cambiaso, Ivan Vaccari, Luca Patti, and Maurizio Aiello. Darknet Security: A Categorization of Attacks to the Tor Network.

Tim Abbott, Katherine Lai, Michael Lieberman, Eric Price. Browser-Based Attacks on Tor

Juha Salo. Recent Attacks On Tor.