Instituto politécnico da Guarda

Escola Superior de Tecnologia e Gestão

Trabalho 04

Anonimato na internet

Sylvain Júlio - 1707279

Curso

TeSP Cibersegurança

Unidade Curricular

Técnicas de Hacking

Ano Letivo: 2023/2024
Docente: Pedro Pinto
Coordenador: Fernando Melo Rodrigues

Sumário executivo

Índice

1. Introdução

Neste trabalho, iremos desenvolver um relatório sobre o anonimato na internet. Iremos tratar de entender o que é a rede TOR, como usar o Privoxy, iremos ainda falar sobre o sistema operativo TAILS e por fim, iremos discutir sobre a importância do anonimato para o black hat hacker, as dificuldades que enfrentam as autoridades contra o anonimato e por fim, iremos falar sobre a importância da coordenação e cooperação internacional para combater o cibercrime.

2. Anonimato na internet

O anonimato na internet é um assunto muito importante, pois permite que os utilizadores possam navegar na internet sem que sejam identificados. É um assunto muito relevante para quem se preocupa com a sua privacidade e segurança, mas é primordial para pessoas que vivem em países onde a liberdade de expressão é limitada. É ainda crítico para pessoas que trabalham em áreas sensíveis, como jornalistas, ativistas, denunciantes, etc. E claro, para quem pratica atividades ilegais, como o cibercrime.

2.1. Rede TOR

A rede TOR (The Onion Router) é uma rede de computadores que permite que os utilizadores possam navegar na internet de forma anónima. A rede TOR é composta por milhares de servidores, chamados de relays, que são mantidos por voluntários. Estes servidores são responsáveis por encaminhar o tráfego dos utilizadores, de forma a que o seu endereço IP não seja revelado. Como aceder à rede TOR?

2.1.1. TOR Browser

O TOR Browser é o browser mais conhecido e desenvolvido para aceder à rede TOR, de código aberto. É um browser baseado no Firefox, que permite que os utilizadores possam navegar na internet de forma anónima. O Tor Browser oculta o endereço IP e a atividade de navegação redirecionando o tráfego da web por uma série de roteadores diferentes, conhecidos como nós. Além disso, o tráfego da web é criptografado com um tipo de criptografia especial originalmente desenvolvida pela Marinha dos EUA para ajudar a proteger as comunicações de inteligência americanas.

Além de ser um browser "normal", o Tor também fornece serviços onion por meio de sua rede onion para permitir o anonimato de sites e servidores. Um endereço web ***".onion"***, acessível exclusivamente através do navegador Tor, protege a identidade do site e dos visitantes.

Com uma conexão complexa e criptografada que oferece anonimato para hosts e visitantes, o Tor é frequentemente usado para criar e acessar a dark web. Como tal, o Tor é a própria definição de um navegador da dark web.

2.1.2. Como funciona o Tor?

O Tor funciona em 3 fases:

1. Nó de entrada/guarda: O utilizador liga-se a um servidor aleatório de entrada, também chamado de nó de entrada. Este servidor é responsável por encriptar o tráfego do utilizador e introduzir o tráfego na rede TOR. A informação é encapsulada em várias camadas de criptografia, daí o nome "The Onion Router" que irão ser descascadas à medida que o tráfego é encaminhado para o nó de saída.

2. Nós intermediários: O tráfego é então encaminhado de forma totalemnte criptografados por vários servidores, chamados de nós intermediários. Estes servidores são responsáveis descascar uma camada por nó e por encaminhar o tráfego para o nó de saída.
3. Nó de saída: O tráfego é então encaminhado para o nó de saída que encaminha o tráfego para o destino.

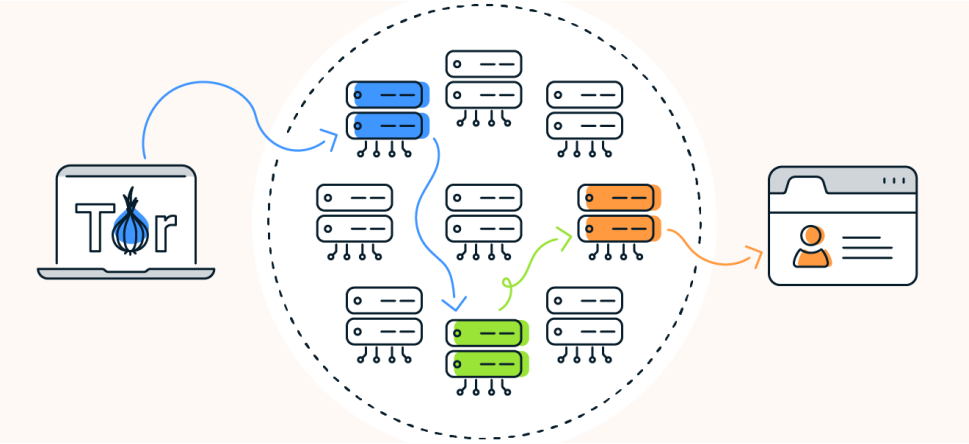

Figura 1: Funcionamento da rede TOR
Fonte: www.avast.com/pt-br/c-tor-dark-web-browser

2.1.3. O navegador TOR

Apesar de todo este processo ser complexo, o utilizador não precisa de saber como funciona a rede TOR para a usar. Ele é um browser baseado no Firefox que permite que os utilizadores possam navegar na internet de forma anónima e já vem configurado e pronto a usar. O TOR Browser é um browser de código aberto, que pode ser descarregado em https://www.torproject.org/.

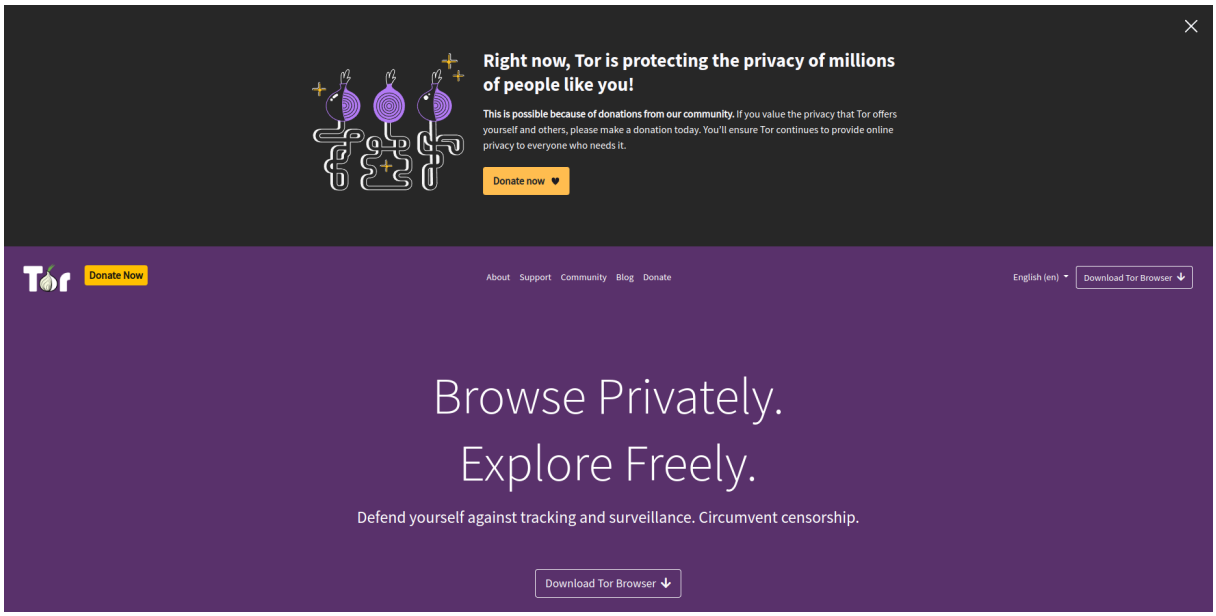

Figura 2: Screenshot do Website do TOR
Fonte: www.torproject.org

Pode ainda ser instalado pela linha de comando, em sistemas Linux, como o Ubuntu, com o seguinte comando:

```
sudo apt install torbrowser-launcher
torbrowser-launcher  # Para instalar o TOR Browser pela primeira vez, e para o iniciar
depois
```

Para verificar que estamos devidamente conectados à rede TOR, basta aceder ao site https://check.torproject.org/.

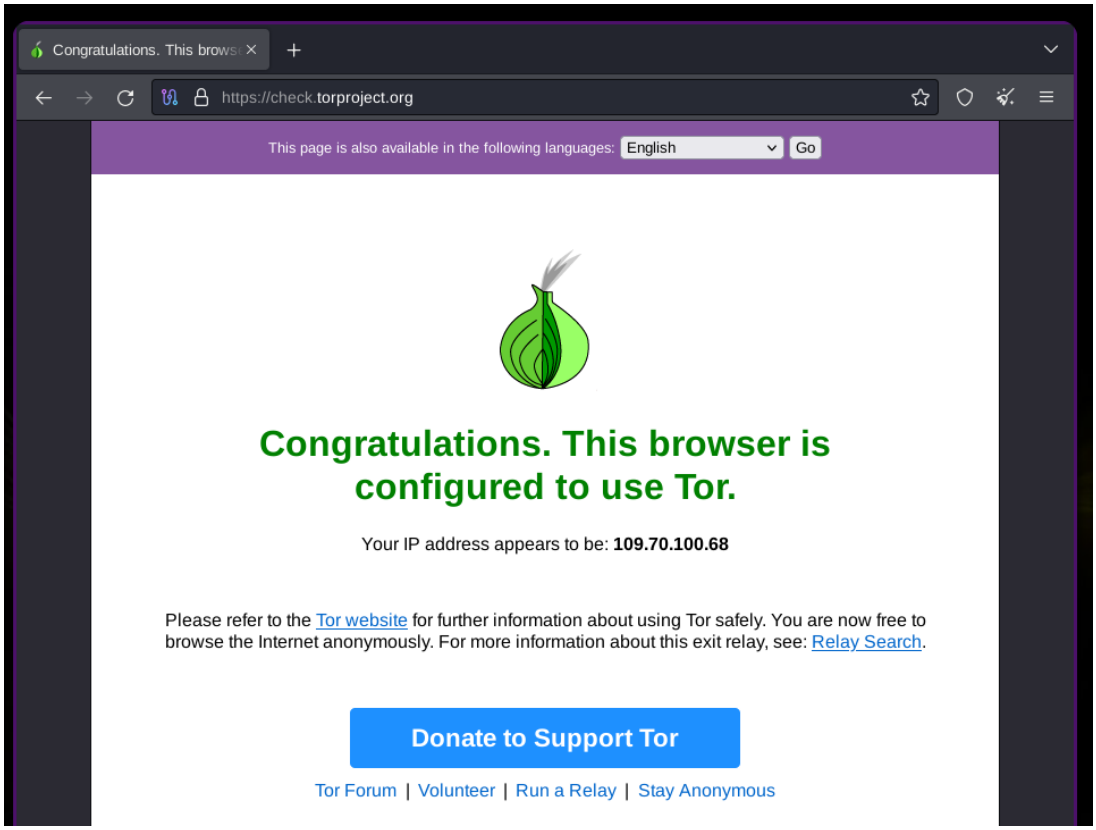

Figura 3: Screenshot do TOR Browser
Fonte: check.torproject.org

2.1.4. A rede TOR é segura?

Bem, a rede em si é criptografada. Mas criptografia não significa segurança. Significa simplesmente que, neste caso, o transporte e as comunicações entre nós são cifradas, ou seja, ilegíveis sem as chaves para as decifrar. De facto, se o utilizador clicar num link malicioso, ou se o site que o utilizador está a visitar tiver código malicioso, o utilizador será comprometido da mesma forma que num browser "normal". O TOR não é um escudo, mas é uma ferramenta muito útil para quem se preocupa com a sua privacidade.

2.1.5. É possível ser identificado através da rede TOR?

Resposta curta: SIM! Existe diversos pontos a ter em conta ao usar a internet em geral. Por exemplo, se usar uma conta pessoal, dados pessoais, etc, não importa usar a rede TOR ou não, porque estarão a identificar-se no ponto de chegada da comunicação. Mesmo que não use nenhum dado pessoal, existem dois pontos fracos neste tipo de rede: O nó de entrada (que contém toda a informação sobre IP e os dados que se quer acessar), e o de saída (onde até

poderá ser intercetado). Mas existe ainda mais um recurso que se pode usar para resolver o problema do nó de entrada. Poderá usar uma VPN-over-TOR. A VPN tratará de criptografar a informação inicial antes de chegar ao primeiro nó de entrada da rede TOR.

No entanto, mesmo assim, podemos afirmar que não estamos 100% anónimos. Isto porque existe ainda uma falha de privacidade na internet que não podemos controlar. Os IPS (provedores de internet) são os primeiros a receber os dados que o nosso router de casa envia, ou de qualquer router por onde estejamos diretamente conectados. E assim para todas as pessoas do mundo que tem internet. Alguma empresa está a fornecer a internet, e será então essa empresa o primeiro ponto de passagem. Posto isso, podemos concluir que, como essas empresas são obrigadas a conhecer um IP de origem e um IP de destino, poderá facilmente reconstruir-se o caminho todo por onde um pacote circula. Teoricamente, sim. Mas ao analisar, vemos que aí reside a força desta rede!

Como a rede TOR faz questão de enviar o trafego por vários nós, ficamos assim quase totalmente oculos na internet pelo seguinte motivo: O trafego passa por diversos países. Países alguns que nem legislação tem. Isso traz grandes dificuldades em pedir registo de lOGS dos provedores de internet desses países. Além disso, a cooperação entre países é muitas vezes complicada, e torna complicado recolher todos os lOGS necessários á reconstrução do caminho de tráfego. E outro ponto importante também, as autoridades demoram a responder, a burocracia é penosa, e demora-se meses até conseguir talvez o primeiro LOG, para saber o nó seguinte e fazer novos pedidos e assim por diante. A grande maioria das vezes, quando não há falta de lOGS, há falta de tempo, e os crimes prescrevem.

2.1.6. Então porquê mesmo assim podemos não estar totalmente ocultos?

Existe outras formas de saber quem somos pela internet sem metermos os nosso dados. Existem dados nosso sobre tudo o que possamos imaginar e o que não imaginamos gravados na internet Um expert em OSINT consegue fazer ligações inimagináveis para determinar com um grau de certezas muito elevado que foi tal ou tal pessoa a fazer algo pela internet. Exemplos:

Exitem diversos dados que enviamos através do nosso browser que nos identificam, e outros que são acessíveis por código javascript que o nosso browser executa. Dados como:

```
- tamanho do ecrã
- tamanho usável do browser
- user-agent
- Do Not Track header
- Timezone
- Content language
- layout de teclado
- Lista de fontes instaladas
- Lista de plugins instalados
- WebGL Renderer
```

```
- permissões do browser
- e muitos outros
```

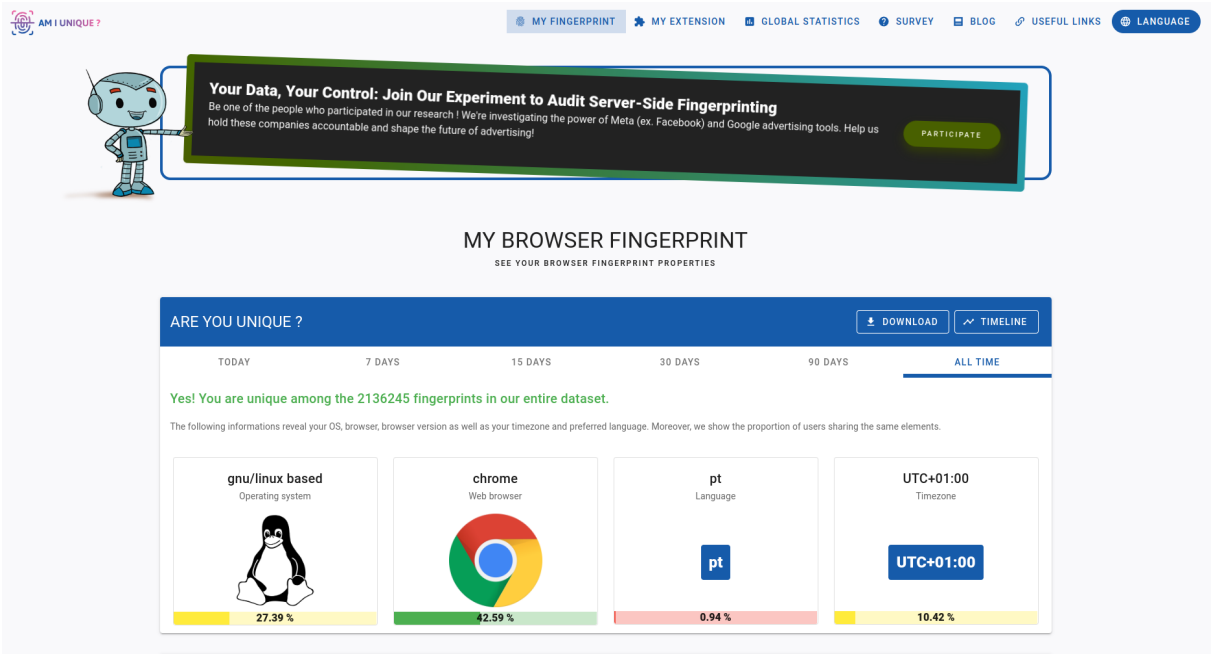

Figura 4: Screenshot do site https://amiunique.org/fingerprint **Fonte:** https://amiunique.org/fingerprint

No meu caso em particular, sou único. totalmente identificável pela internet... Também posso dizer que talvés me ponho a geito. Teclado e linguagem em Portugues, computador Linux, fontes (tipos de letras) como "*firacode*" entre outras coisas fazem que não haja outra configuração igual.

E no caso de usar TOR? De certeza que não iria ser possível obter tanta informação, mas mesmo assim, seriam perfeitamente suficientes para me identificarem.

2.1.7. Como tentar ficar anónimo pela internet?

Vimos anteriormente várias falhas no anonimato perfeito... Mas vamos tentar otimizar tudo para ficarmos o mais anónimos possível. Vimos que o nosso sistema fala para a internet. Isso é um problema para quem quiser ficar anónimo. Temos então que usar, para além do TOR e de uma VPN-over-TOR, podemos usar uma ferramenta que irá alterar todos esses elementos identificáveis do browser. Essa ferramenta é o privoxy.

2.2. Privoxy

O privoxy é uma simples proxy, mas que pode ser configurado para mudar elementos que se enviam para os diferentes servidores WEB. Pode-se controlar que HEADERS se irão enviar, entre muitas outras coisas.

A sua instalação é básica:

```
sudo apt install privoxy
```

O seu ficheiro de configurações tem mais de duas mil linhas, com explicações de cada função. É por si só um manual e o ficheiro de configurações. Está localizado em **/etc/privoxy/config**

Para emparelhar o TOR e o privoxy, teremos de iniciar o serviço privoxy:

```
sudo systemctl start privoxy.service
```

Termos ainda que informar ao TOR Browser (ou outro browser) que queremos primeiro passar por um proxy, e só depois continuar a circular a informação normalmente pela rede TOR. Para isso, temos de saber onde está o nosso servidor proxy:

```
cat config | grep -v "^#" | grep listen-address
    listen-address  127.0.0.1:8118
    listen-address  [::1]:8118
```

3. Bibliografia

- https://www.torproject.org/
- https://www.avast.com/pt-br/c-tor-dark-web-browser