ACEBOLE O SEU FLUXO DE TRABALHO

COMPARTILHE ARQUIVOS DE FORMA SEGURA E PUBLIQUE O CONTEÚDO USANDO ONIONSHARE

OnionShare é uma ferramenta de código aberto que permite compartilhar arquivos de forma segura e anônima, hospedar websites e conversar com amigos usando a rede Tor.

`onionshare.org`

COMPARTILHE E RECEBA DOCUMENTOS DE FORMA SEGURA USANDO SECUREDROP

SecureDrop é um sistema de código aberto para envio de denúnicas que as organizações de mídia e organizações não governamentais podem instalar para receber documentos de fontes anônimas de forma segura.

`securedrop.org`

TENHA UMA COMUNICAÇÃO LIVRE DE METADADOS COM RICOCHET

Ricochet Refresh é um app de comunicação par a par que utiliza o Tor para conectar os clientes. Quando você inicia o Ricochet Refresh, um serviço onion é criado no seu computador.

`ricochetrefresh.net`

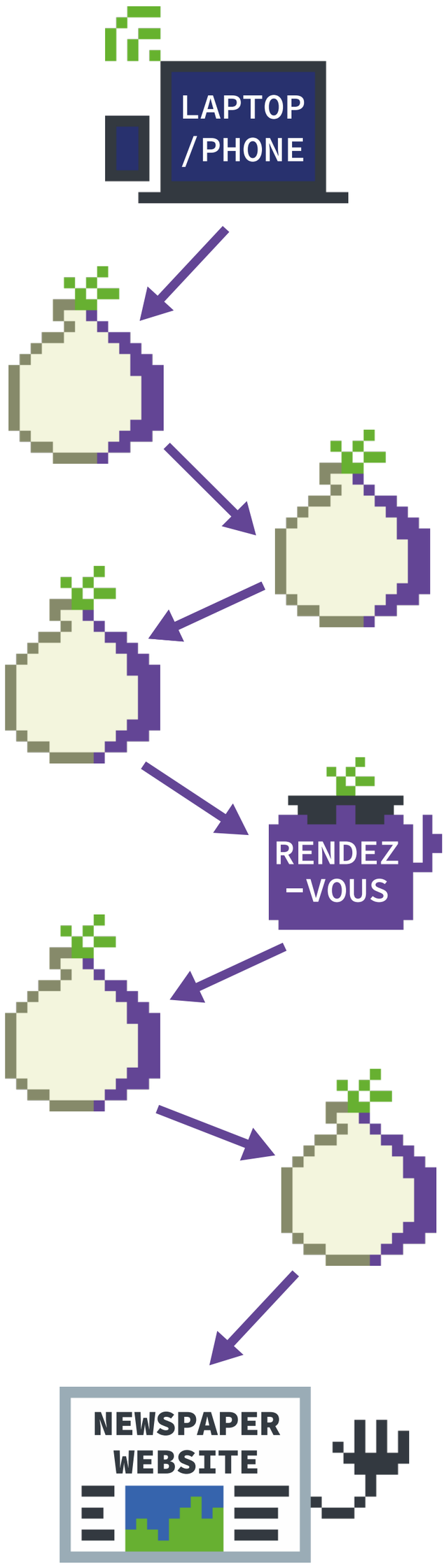
`https://community.torproject.org/onion-services/advanced/opsec/`

Cultive a sua cebola

O FUTURO É CIBERFEMINISTA

Fernanda participa de um coletivo de mulheres sobre direitos reprodutivos no Brasil, país onde o aborto é ilegal. Fernanda e suas amigas criaram um site com informações sobre acesso a aborto, controle de natalidade e outros materiais para pessoas em busca informação reprodutiva. Se este site estivesse ligado a elas, elas poderiam ser presas - ou pior.

Para se proteger, Fernanda e suas amigas criaram um site usando os Serviços Onion do Tor. Assim, não só elas se **protegem de serem descobertas como as responsáveis pelo serviço**, mas também ajudam a **proteger os/as visitantes** de seu site ao tornar obrigatório o uso do Navegador Tor.



COMO OS SERVIÇOS ONION FUNCIONAM?

Um usuário em potencial já deve ter ouvido falar do Projeto Tor, da rede e até dos relays do Tor, e isso é ótimo! Mas os serviços onion não são como um relay na rede Tor.

Um serviço onion se conecta aos nós de encontro (rendezvous) na rede Tor. Por sua vez, uma conexão de um cliente com o serviço onion faz o mesmo. Isto significa que as conexões do cliente com o servidor nunca saem da rede Tor.

Ao contrário de rodar um relay do Tor, operar um serviço onion não resulta em ter o seu endereço IP listado publicamente em qualquer lugar, nem o seu serviço retransmitirá trafégo da rede Tor.

Do ponto de vista da rede, o serviço onion é como qualquer outro cliente conectado na rede Tor. Isso significa que os operadores de serviços onion não precisarão se preocupar em ter o endereço IP do servidor vinculado, sinalizado ou incluído em listas de bloqueio como parte da rede Tor.

Para mais informações sobre os serviços onion, leia o portal da Comunidade do Projeto Tor:

https://community.torproject.org/onion-services/overview

IDENTIFIQUE A CEBOLA

Ícone da cebola
Um ícone de uma cebolinha pode ajudá-lo a identificar os serviços Onion. Procure por ele no Navegador Tor.

TLD .onion
O endereço de um serviço onion é gerado automaticamente, de modo que os operadores não precisam comprar um nome de domínio; a URL .onion também ajuda o Tor a garantir que você está se conectando ao endereço correto e que a conexão não está sendo manipulada.

Endereço Onion
Um endereço onion é uma seqüência de 56 (e no formato V2, 16) na maioria das vezes letras e números aleatórios, seguidos por ".onion". Todo o tráfego entre os usuários do Tor e os serviços onion é criptografado de ponta a ponta, portanto você não precisa preocupar-se em conectar usando HTTPS.

PLANTE A SUA CEBOLA

Como configurar um serviço onion para o seu site num sistema operacional basedo no Debian.

! Nota: O símbolo # refere-se à execução do código como root.

Fazer o Tor funcionar

Para configurar o repositório de pacotes Tor, ative o repositório de pacotes Torproject seguindo estas instruções:

1. Instale apt-transport-https

Para habilitar todos os gerenciadores de pacote que usam a biblioteca do libapt-pkg para acessar os metadados e pacotes disponíveis em fontes acessíveis através de https (Hypertext Transfer Protocol Secure).

```
# apt install apt-transport-https
```

2. Adicione as seguintes linhas em /etc/apt/sources.list ou em um novo arquivo em /etc/apt/sources.list.d/

```
deb https://deb.torproject.org/torproject.org buster main
deb-src https://deb.torproject.org/torproject.org buster main
```

3. Então adicione a chave gpg usada para assinar os pacotes, executando os seguintes comandos em seu prompt de comando

```
# wget -qO- https://deb.torproject.org/torproject.org/A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89.asc | gpg --import
# gpg --export A3C4F0F979CAA22CDBA8F512EE8CBC9E886DDD89 | apt-key add -
```

4. Instale tor e o chaveiro debian do tor

Nós fornecemos um pacote Debian para ajudar a manter atualizada a nossa chave de assinatura. É recomendado utilizá-lo. Instale através dos seguintes comandos:

```
# apt update
# apt install tor deb.torproject.org-keyring
```

Fazer o servidor web funcionar

Nginx está disponível no repositório principal de múltiplas distribuições Linux e *BSD. Para instalar o pacote nginx:

```
$ sudo apt install nginx
```

Por padrão, o servidor web estará acessível em localhost:80 no final da instalação.

Uma vez configurado seu servidor web, certifique-se de que ele funciona: abra seu navegador e vá para http://localhost/.

Em seguida, tente colocar um arquivo html no diretório principal e certifique-se de que ele apareça quando você acessar o site.

Configure o seu serviço onion

O próximo passo é abrir o arquivo de configuração do Tor (torrc) e aplicar as configurações apropriadas para configurar um serviço onion.

Dependendo de seu sistema operacional e configuração, seu arquivo de configuração do Tor pode estar em um local diferente ou parecer diferente.

```
HiddenServiceDir /var/lib/tor/onion_service/
HiddenServicePort 80 127.0.0.1:80
```

Reinicie o Tor e verifique se funcionou.

```
$ sudo systemctl restart tor
```

Se o Tor iniciar novamente, ótimo. Caso contrário, alguma coisa está errada. Primeiro verifique os seus arquivos de log para encontrar pistas.

Editar arquivo de configuração do site

Se você estiver rodando vários sites onion no mesmo servidor web, lembre-se de editar seu arquivo host virtual do servidor web e adicionar o endereço onion de cada site.

Teste se o seu serviço onion funciona

Para obter o endereço do seu serviço onion, vá para seu diretório 'HiddenServiceDir' e encontre um arquivo chamado 'hostname'. O arquivo hostname em seu diretório de configuração do serviço onion contém o nome da máquina para seu novo serviço onion v3. Os outros arquivos são suas chaves de serviço onion, portanto é imperativo que sejam mantidos em sigilo.

Se as suas chaves vazarem, outras pessoas podem passar-se por seu serviço onion, comprometendo-o, tornando inútil e perigoso de ser visitado.

Agora você pode conectar-se ao seu serviço onion usando o Navegador Tor!

Mais Recursos

Como próximo passo, você pode habilitar o Onion-Location e anunciar seu site onion para todos os/as usuários/as do Navegador Tor, quando o visitarem:

https://community.torproject.org/onion-services/advanced/onion-location/

Se é a primeira vez que seu/sua amigo/a utiliza serviços onion, compartilhe com ele/a o Manual de Usuário do Navegador Tor:

https://tb-manual.torproject.org/pt-BR/onion-services/

Também é possível fazer um serviço onion muito privado, protegido por uma chave privada e autorização de usuário. Saiba mais:

https://community.torproject.org/onion-services/advanced/client-auth/

Por que usar serviços onion?

Descentralização
Não há nenhuma autoridade central que aprove ou rejeite serviços onion. O endereço de um serviço onion é gerado automaticamente. Os operadores não utilizam a infra-estrutura DNS padrão e não precisam comprar ou registrar um nome de domínio.

Ofuscação ou eliminação de metadados
Quando você usa a rede Tor para navegar na web, você não está enviando nenhuma informação por padrão sobre quem você é ou de onde está se conectando. Os serviços onion usam a rede Tor para eliminar informações sobre onde eles estão situados. O seu uso elimina todos os metadados que poderiam estar associados de alguma forma ao serviço.

Sustentabilidade da rede
Os serviços onion utilizam a rede Tor para eliminar informações sobre onde eles estão localizados. O tráfego gerado por eles não sai da rede Tor e, portanto, estes circuitos onion diminuem a carga no tráfego de nós de saída para os/as outros/as usuários/as. Além disso, quando um serviço está disponível via serviços onion, ele acrescenta diversidade à rede Tor, pois usa um conjunto diferente de circuitos na rede, evitando totalmente os relays de saída.

Aumente a privacidade dos seus serviços
Além de websites e sites onion, é possível fazer muitas coisas com serviços onion, por exemplo, e-mail. Lembre-se, uma cebola por dia mantém afastada a vigilância!

Liberdade de imprensa e evasão da censura
As conexões regulares do Tor já proporcionam a evasão à censura, mas somente os serviços onion podem anonimizar ambas as partes da comunicação - usuários e provedor -, criando uma comunicação livre de metadados entre o usuário do serviço e o próprio serviço.

As tecnologias de censura estão sendo implementadas por diferentes atores, como governos e provedores de Internet em todo o mundo, para bloquear o acesso à imprensa livre e às ferramentas de privacidade. Para proteger a liberdade de expressão e a liberdade de opinião em espaços censurados, as principais organizações da imprensa disponibilizaram nos últimos anos os seus websites via serviços onion.

Esse é o caso do NY Times, ProPublica, Deutsche Welle, BBC, The Markup e outras redações.

Proteger fontes, denunciantes e jornalistas
Muitos jornalistas e organizações da mídia utilizam ferramentas baseadas em serviços onion para proteger as suas fontes. Eles compartilham e recebem documentos de fontes anônimas usando ferramentas como SecureDrop, GlobaLeaks, e OnionShare.

Educar usuários/as sobre privacidade por design
Os serviços onion são um excelente exemplo de tecnologia de privacidade por design, onde uma pessoa está segura e anônima por padrão. Tornar o seu serviço disponível via serviços onion é uma oportunidade de educar o público em geral sobre Tor e como uma forma mais segura de acessar a internet pode ser: fácil como navegar numa página da web.

Lembre-se: uma cebola por dia mantém afastada a vigilância!