Aprendendo sobre...

OS SEGREDOS DA

DARK WEB

Como entrar e ser anônimo em uma rede desconhecida?

ACKERDEMY
ALESTAN ALVES

Sumário

I

Introdução

Passei bastante tempo vagando pela Dark Web para estudar o que ocorre por lá e assim conseguir trazer para vocês alguns conceitos importantes para navegar nessa rede.

Vale lembrar que todos os conceitos e ensinamentos desse livro servem para estudo em Cibersegurança e Ethical Hacking, nunca vamos incentivar e ser a favor dos crimes que são cometidos. Somos a favor do aprendizado e do anonimato nas redes para que todos tenham sua privacidade estabelecida.

“Antes mesmo que comecemos nosso dia, diversas organizações já sabem que estamos acordados. Eles conhecem nossos horários, nossa agenda e têm conhecimento de nossos gostos e inclinações. Por meio das nossas redes, expomos nossa privacidade a essa indústria digital. Sem nossa permissão, conhecem nossos segredos e traçam formas de manipular nosso comportamento. A tecnologia digital usa nossos dados para exercer poder sobre nossas escolhas. Para retomar o poder da nossa privacidade, precisamos proteger nossos dados.” - Livro Privacidade é Poder - Carissa Véliz

O anonimato traz grandes benefícios, afinal, você consegue ter a tão sonhada liberdade de expressão e se manter longe de qualquer ideologia autoritária ou de formas de manipulação em massa. Todavia, o anonimato pode trazer malefícios a depender da finalidade em que é utilizado, colaborando para que muitos se expressem sem o devido bom senso.

Portanto, fique ciente que nosso propósito sempre será o ensino em Cybersecurity e Anonimato e nunca o incentivo a práticas ilícitas.

Não utilizem esses ensinamentos para prática de atos ilegais, mas sim como forma de aprendizado e estudo.

“Lembre-se que as pessoas podem tirar tudo de você, menos o seu conhecimento”

Albert Einstein

hello friend

II

O que é Deep Web?

A "deep web" nada mais é que um termo abrangente utilizado para se referir às partes da internet que não são acessíveis se forem procuradas através dos mecanismos de pesquisa padrão (Google, Bing e Yahoo). Seu conteúdo é composto por páginas que não foram indexadas por mecanismos de busca, sites pagos, bancos de dados privados e dark web.

Todo mecanismo de pesquisa usa bots para rastrear a web e adicionar o novo conteúdo encontrado ao índice do mecanismo de pesquisa. Não se sabe o tamanho da deep web, mas muitos especialistas estimam que os mecanismos de busca rastreiam e indexam menos de 1% de todo o conteúdo que pode ser acessado pela internet. O conteúdo pesquisável da web é referido como a web de superfície.

Grande parte do conteúdo da deep web é de natureza legítima e não criminosa, o que inclui mensagens de e-mail ou bate-papo, conteúdo privado em sites de mídia social, extratos bancários eletrônicos, registros eletrônicos de saúde (EHR), além de outros conteúdos acessíveis na Internet.

Qualquer site com acesso pago, como o texto de artigos de notícias ou site de conteúdo educacional que exija uma assinatura, também é bloqueado para bots de mecanismos de pesquisa. Sites de taxa por serviço como o Netflix também não são rastreados pelos bots.

Por esse motivo, existem algumas vantagens na deep web. Para começar, grande parte do seu conteúdo é irrelevante e só tornaria as pesquisas muito mais difíceis, e há também uma questão de privacidade; ninguém gostaria que os bots do Google rastreassem suas visualizações da Netflix ou a conta da Fidelity Investments.

III

As profundezas da internet

O termo deep web foi criado por Michael K. Bergman, fundador da Bright Planet, empresa especializada em coletar, classificar e procurar conteúdo na deep web para uso corporativo. De acordo com Bergman, a importância da coleta de informações na web e o papel inquestionável dos mecanismos de busca –mais a frustração expressada por usuários em relação à eficiência desses mecanismos –fazem deles o foco óbvio de investigação. A fim de melhor expressar a importância da coleta de informações da deep web, Bergman acrescenta ainda que: “Até Van Leeuwenhoek haver observado pela primeira vez uma gota d’água sob o microscópio no final dos anos 1600, a pessoas não tinham ideia que havia um mundo inteiro de 'animálculos' além de sua visão”.

Ainda de acordo com esse autor, os mecanismos de busca obtêm suas listagens (indexam o conteúdo) de duas maneiras diferentes: (a) os autores cadastram suas web pages diretamente nesses mecanismos ou, (b) elas são rastreadas seguindo seus hyperlinks. Esta última é a forma que retorna o maior volume de informações. Em seu trabalho, Pompéo e Seefeldt (2013) afirmam que a deep web é constituída por sites dispersos por toda a Internet, os quais, entretanto, são propositalmente programados para não serem encontrados, mantendo, dessa forma, a deep web oculta do grande público, nas “profundezas” da rede.

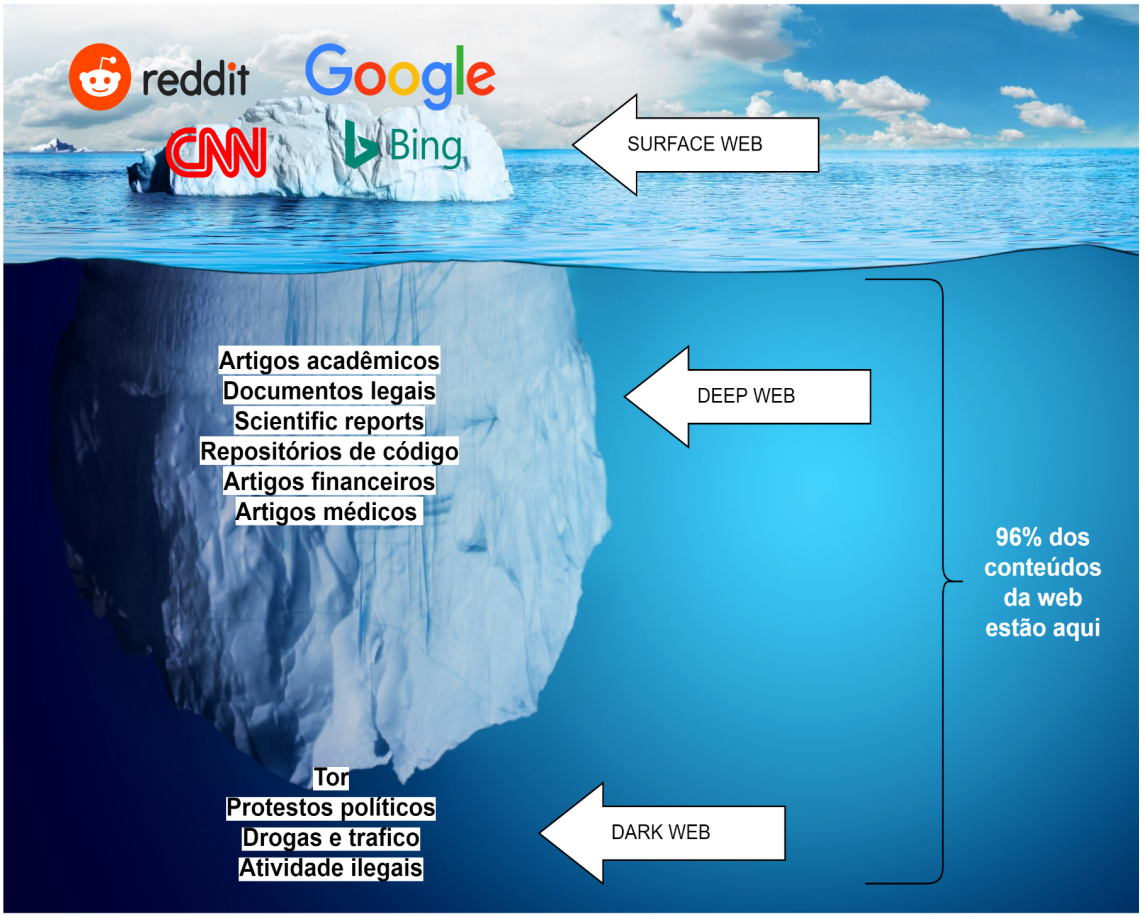


Imagem que reflete a profundeza da internet através de um iceberg @ackercode content

Por que os sites da Deep Web não são indexáveis?

Existem vários métodos que impedem que as páginas da Web sejam indexadas pelos mecanismos de pesquisa tradicionais. Eu os categorizei para sua referência abaixo.

- **Web context:** páginas com conteúdo variado para diferentes contextos de acesso.
- **Conteúdo dinâmico:** páginas dinâmicas que são retornadas em resposta a uma consulta enviada ou acessadas apenas por meio de um formulário, especialmente se forem usados elementos de entrada de domínio aberto; tais campos são difíceis de navegar sem conhecimento de domínio.
- **Conteúdo de acesso limitado:** Sites que limitam o acesso às suas páginas de forma técnica (por exemplo, usando o Robots Exclusion Standard ou CAPTCHAs, ou

a diretiva no-store que proíbe os mecanismos de pesquisa de navegar e criar cópias em cache).

- **Conteúdo não HTML/texto:** conteúdo textual codificado em arquivos multimídia (imagem ou vídeo) ou formatos de arquivo específicos não manipulados por mecanismos de pesquisa.
- **Web Privada:** Sites que exigem registro e login (recursos protegidos por senha).
- **Conteúdo com script:** páginas que só são acessíveis por meio de links produzidos por JavaScript, bem como conteúdo baixado dinamicamente de servidores da Web por meio de soluções Flash ou Ajax.
- **Software:** Certo conteúdo é intencionalmente oculto da Internet comum, acessível apenas com software especial, como Tor, I2P ou outro software darknet. Por exemplo, o Tor permite que os usuários acessem sites usando o endereço do servidor .onion anonimamente, ocultando seu endereço IP.
- **Conteúdo não vinculado:** páginas que não estão vinculadas por outras páginas, o que pode impedir que programas de rastreamento da Web acessem o conteúdo. Esse conteúdo é chamado de páginas sem backlinks (também conhecidas como inlinks). Além disso, os mecanismos de pesquisa nem sempre detectam todos os backlinks das páginas da Web pesquisadas.
- **Arquivos da Web:** os serviços de arquivamento da Web, como o Wayback Machine, permitem que os usuários vejam versões arquivadas de páginas da Web ao longo do tempo, incluindo sites que se tornaram inacessíveis e não são indexados por mecanismos de pesquisa como o Google.

IV

Dark Web vs Deep Web

A deep web é muitas vezes confundida com a dark web, os dois termos tornaram-se intercambiáveis na cultura popular, mas representam coisas muito diferentes. O primeiro se refere a todas as informações armazenadas on-line que não são indexadas por mecanismos de pesquisa tradicionais.

Muitas informações na deep web estão escondidas de muitas pessoas porque não pertencem diretamente a elas. Isso inclui bancos de dados que o Google não pode acessar, dados desatualizados em revistas acadêmicas ou registros judiciais antigos sem mais relevância; todas essas coisas ficam lá fora, não indexadas pelo Google, mas ainda presentes online para qualquer outra pessoa que queira.

Cabe ressaltar que a deep web é responsável por cerca de 90% de todo o tráfego da web!

Enquanto a deep web contém informações como bancos de dados acadêmicos, bancos online e outras páginas de login, muitos sites hospedados na dark web são acessíveis apenas para aqueles que possuem um conjunto específico de credenciais. Por exemplo, se o seu provedor de saúde tiver um portal on-line que exibe exames de sangue e for acessado por meio deste site profundo sem ser indexado - você precisará de permissão

especial deles para que o acesso seja concedido. Outro exemplo da dark web seria um site oculto que só é acessível por meio de um link especial encontrado em um fórum online.

A internet foi dominada principalmente por gigantes corporativos. No entanto, ainda existem alguns lugares para encontrar as informações obscuras e difíceis de encontrar que você precisa em mecanismos de pesquisa da deep web, como Ahmia ou the www Virtual Library.

Então… o que é a dark web? Para você, a dark web pode ser algo que você não espera. O Google não permite essas coisas, que estão disponíveis na dark web. De um lugar de escuridão, esta rede guarda segredos e mistérios que certamente manterão seu interesse por anos - mesmo que nem sempre sejam bons! A dark web está intencionalmente escondida na deep web para proteger a identidade de seus usuários!

V

O Tor

De acordo com o projeto, para que a rede Tor seja eficaz, alguns hábitos de navegação do usuário deverão ser mudados ao utilizar o Tor browser. O Tor não protege todo o tráfego enviado pelo usuário à Internet, mas sim, apenas o tráfego das aplicações devidamente configuradas para enviar seu tráfego à Internet através do Tor. Para evitar problemas com a configuração Tor, o site do projeto recomenda o uso de seu próprio navegador (Tor browser), uma vez que este já é pré-configurado para proteger a privacidade e o anonimato do usuário na web.

Não fazer torrent sobre o Tor.

Foi observado que aplicativos para compartilhamento de arquivos tipo torrent ignoram as configurações de proxy, estabelecendo conexões diretas mesmo quando instruídos a usar o Tor. Mesmo que o aplicativo torrent se conecte exclusivamente por meio do Tor, o endereço IP real do usuário será frequentemente enviado na solicitação GET do tracker, dada a forma como os aplicativos torrent funcionam. Isso acabará não apenas com o anonimato do tráfego torrent, mas também com o anonimato de qualquer outro tráfego web simultâneo do usuário via Tor, causando ainda lentidão a toda a rede (Tor).

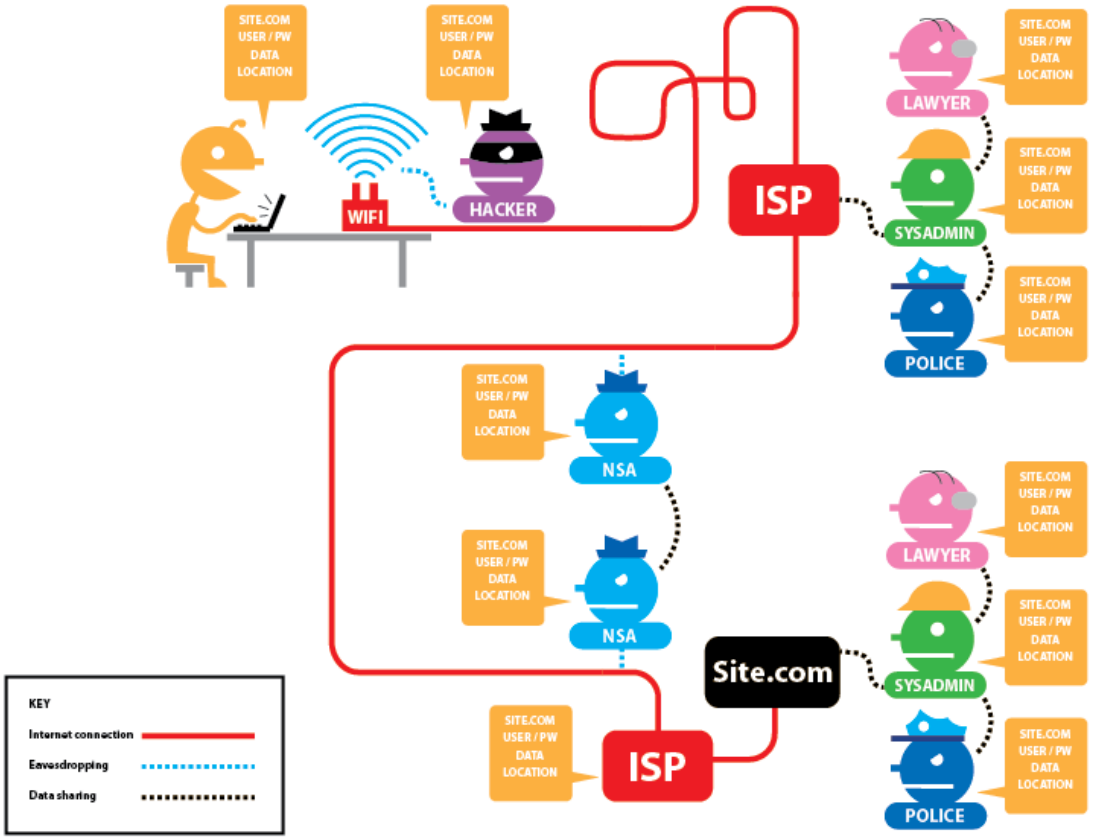
Não instalar ou habilitar plugins no navegador.

O navegador Tor bloqueará plugins, como Flash, RealPlayer, Quicktime e outros, uma vez que eles podem ser manipulados para revelar o endereço IP do usuário. Da mesma forma, o projeto TOR não recomenda a instalação de complementos ou plugins adicionais em seu

navegador, pois eles podem ignorar o Tor ou prejudicar o anonimato e a privacidade do usuário.

Utilizar as versões HTTPS dos sites.

O Tor criptografa o tráfego enviado para, e através, da rede Tor já a criptografia do tráfego enviado ao website de destino depende desse website. A Figura “Tor e HTTPS” ilustra o funcionamento do Tor com HTTPS.



Tor e HTTPS - Imagem Tor browser (torproject.org)

O Tor browser inclui o HTTPS Everywhere para forçar o uso do HTTPS com os sites que o suportem, no entanto, mesmo assim, deve-se observar a barra de URL do navegador para garantir que os sites aos quais o usuário fornece informações confidenciais mostrem um botão azul ou verde, incluam https:// na URL e, ainda, exibem o nome esperado para o website.

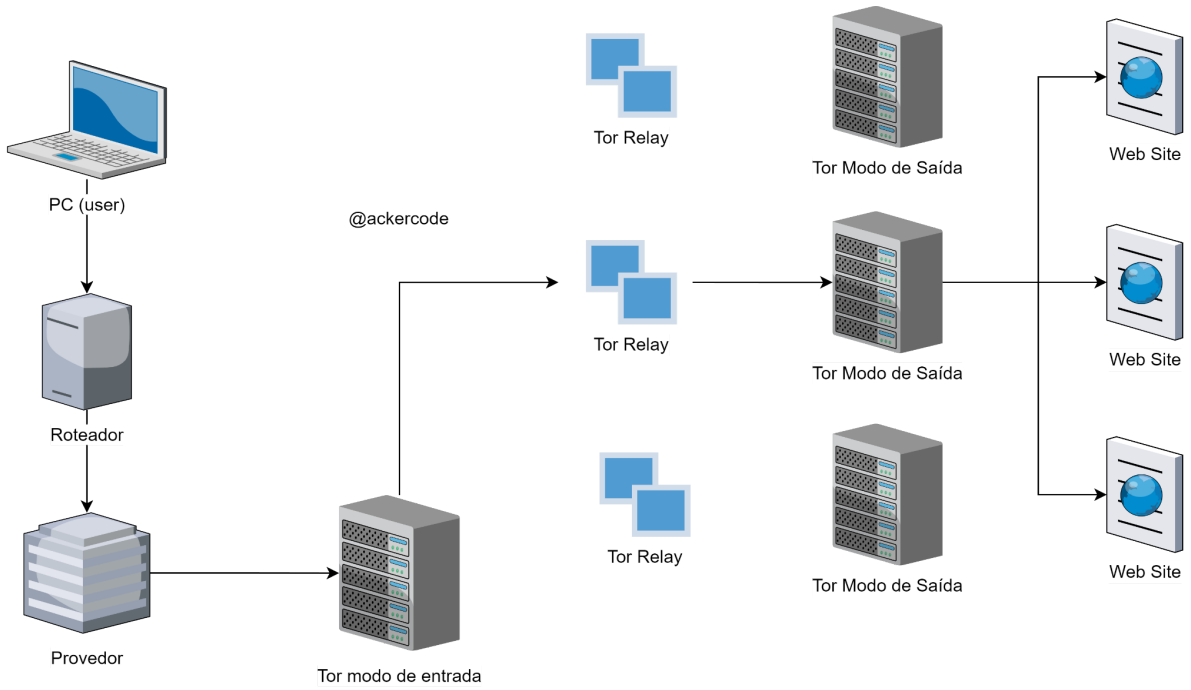
Uma dica importante é não abrir documentos baixados por meio do Tor enquanto estiver online, mas caso isso ocorra, é importante passar o documento por uma análise no "virustotal.com". O navegador Tor notificará o usuário caso ele tente abrir automaticamente documentos que possam ser manipulados por aplicativos externos. Tal aviso não deverá ser ignorado, e é necessário ser cuidadoso ao baixar documentos via Tor – especialmente arquivos do tipo .DOC e .PDF, a menos que o usuário utilize o visualizador PDF integrado ao Tor browser. Isso porque esses documentos podem conter recursos da Internet que serão baixados fora do Tor pelo aplicativo que os abre, revelando, assim, o endereço IP não Tor. Se o usuário precisar trabalhar com arquivos DOC e/ou PDF, recomenda-se fazê-lo a partir de um computador desconectado, em máquina virtual com rede desativada ou usando o Tails. Entretanto, sob nenhuma circunstância, o uso conjunto do BitTorrent e do Tor é seguro.

Ao Utilizar bridges O Tor tenta impedir que invasores venham a descobrir a quais sites o usuário deseja se conectar. No entanto, por padrão, isso não impede que alguém que esteja monitorando o tráfego da Internet saiba que o usuário se utiliza do Tor. Se isso for relevante para o usuário, ele poderá mitigar esse risco, configurando o Tor para usar uma Tor bridge ao invés de se conectar diretamente à rede pública do Tor. Em última análise, a melhor proteção poderá ser uma abordagem social: quanto mais usuários Tor, e mais próximos entre si estiverem esses usuários; e ainda, quanto mais diversificados forem seus interesses, menor será o risco para todos eles.

Tor onion services

Resumidamente, o Tor pode ser definido como um software livre e uma rede aberta, destinados a auxiliar na preservação da privacidade do usuário quando do exercício de suas atividades na Internet. A rede Tor consiste em um grupo de servidores operados por voluntários, na qual seus usuários se conectam por meio de uma série de túneis virtuais ao invés de uma conexão direta, permitindo a ambos – indivíduos e organizações – compartilharem informações através de redes públicas, preservando sua privacidade.

Conexão Tor Simplificada



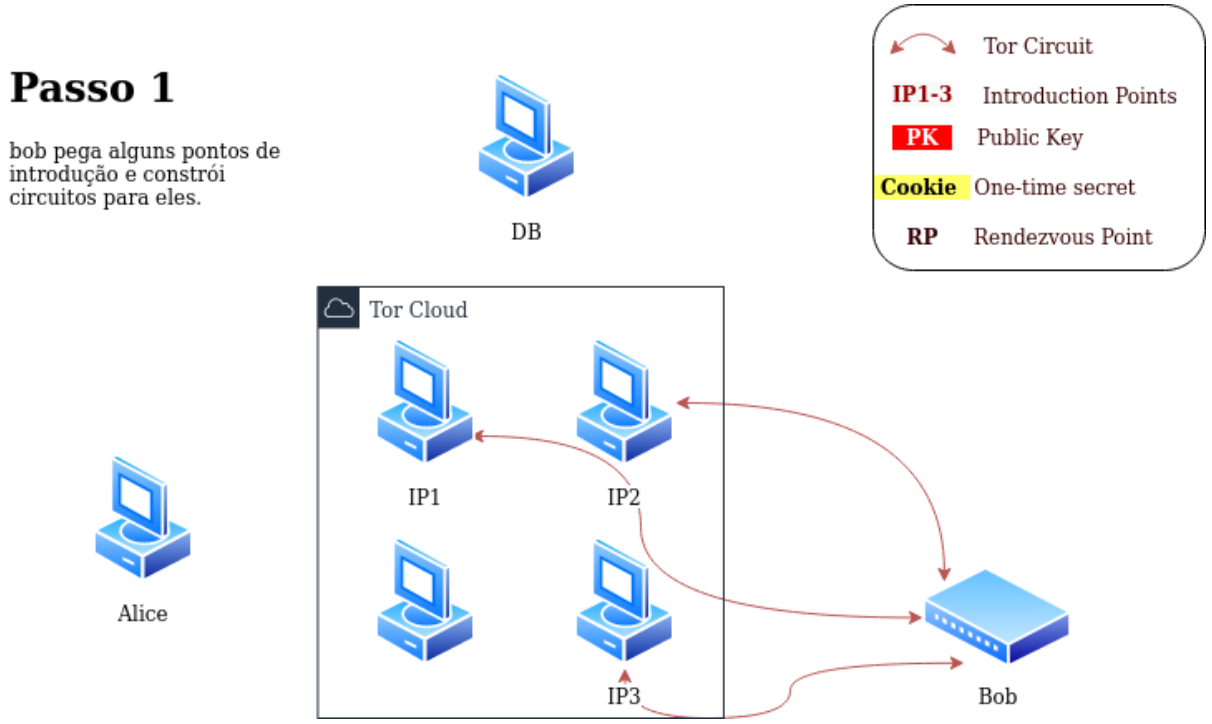
Exemplo simples da conexão da rede Tor @ackercode content

O Tor se apresenta ainda como uma ferramenta eficaz para que o usuário possa se esquivar também de algum tipo de censura, conseguindo assim, acesso a destinos ou conteúdos inicialmente bloqueados. Desenvolvedores de softwares podem usar o Tor como blocos de construção para novas ferramentas de comunicação com recursos de privacidade integrados. Os onion services do Tor, anteriormente referidos como hidden services, permitem a publicação de websites e outros serviços sem necessidade de revelar a localização destes e podem ser usados para comunicações sociais com teor sensível, a exemplo de salas de bate-papo e fóruns para vítimas de estupro, dentre outras possibilidades. Simonsen(2014) afirma ser de suma importância que o cidadão brasileiro tenha conhecimento de seus direitos e acesso a ferramentas que possam lhe auxiliar na manutenção de sua privacidade on-line, como, por exemplo, VPNs, AdBlock, Ghostery e o Tor, entre outros.

Entretanto, há que se destacar que o Tor não poderá garantir a privacidade de seu usuário sob toda e qualquer circunstância, pois caso o usuário venha a se logar no Google ou no Facebook, eles poderão monitorar as comunicações do usuário dentro de seus sistemas. Vale destacar ainda que, se alguém puder monitorar os dois lados de uma conexão, a análise estatística do tráfego poderá vir a identificar a origem desse tráfego.

Como é de nosso entendimento, o Tor fornece anonimização para usuários querendo acessar serviços, também é possível esconder um serviço para que seus usuários não saibam seu endereço e localização.

Como seu endereço é escondido e consequentemente seu host, o servidor deve anunciar seu serviço à rede Tor elegendo alguns nós para serem pontos de introdução. Isso é feito construindo circuitos para os onion routers escolhidos e compartilhando-se as chaves entre os nós/servidor.



Onion services fase 1.0 Onion Service Router @ackercode produções

Para que os usuários possam saber do serviço, o servidor envia para um servidor de diretório – fora da rede Tor – um sumário com a descrição do serviço oferecido e sua chave pública para que os outros possam acessá-lo. Essa transação é feita por dentro do Tor, de modo a proteger a identidade do servidor. Nesta etapa, o servidor de diretório gera um nome para o serviço com caracteres aleatórios, do tipo ackercodexxx.abc.onion, os usuários da rede Tor usam esse nome para acessar o serviço escondido, via HTTP, FTP, etc.

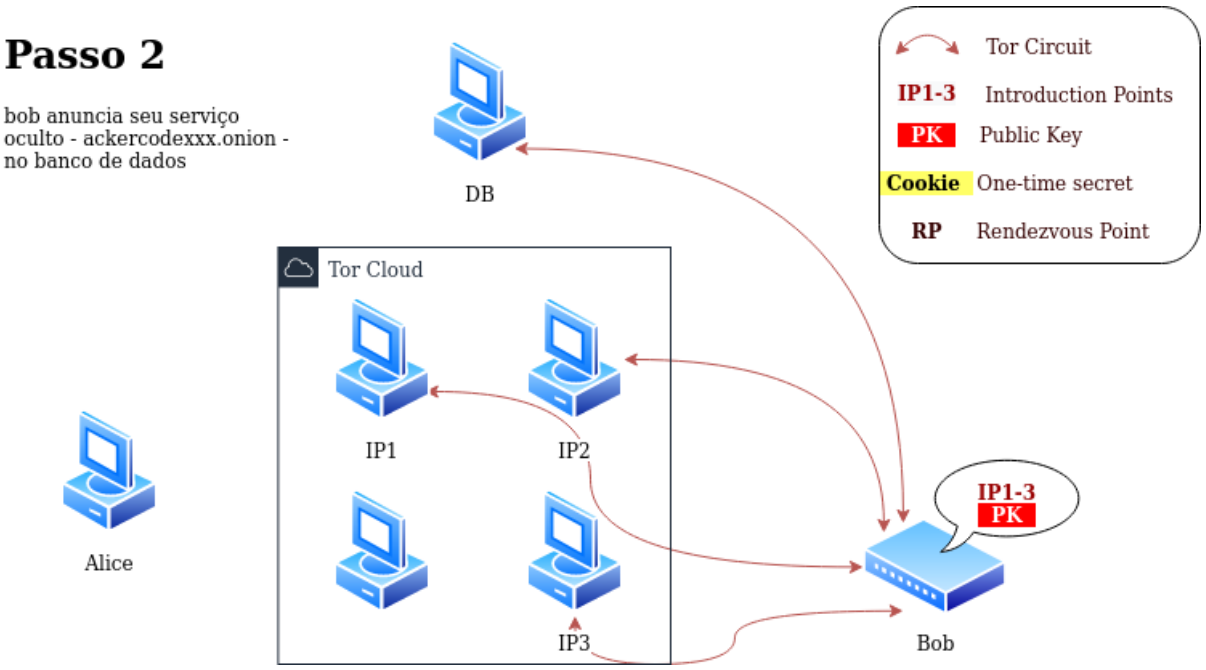


Imagem 2 Onion Service Router @ackercode produções

Para um usuário (Alice) acessar o serviço, ela deve buscá-lo no servidor de diretório, obtendo sua chave pública e o ponto de introdução. Ao invés de Alice se conectar diretamente no ponto de introdução, é selecionado um onion router para atuar como *rendezvous point* (ponto de encontro).

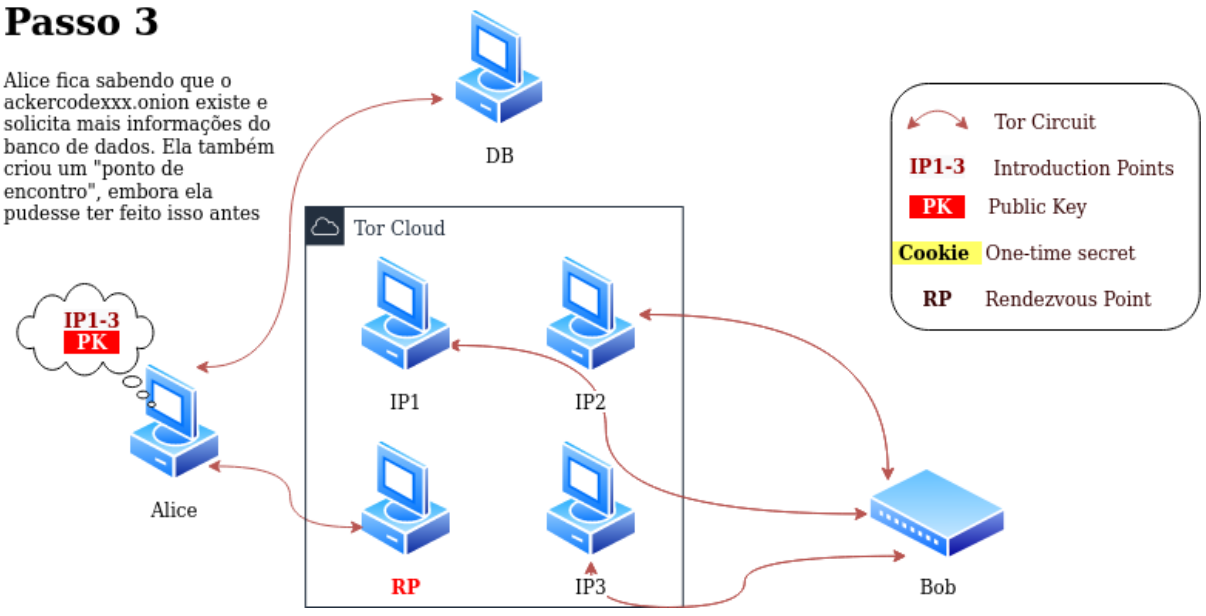


Imagem 1.2 Onion Service Router @ackercode produções

Alice envia um pedido de conexão no serviço contendo o *rendezvous point* escolhido. Esta mensagem é criptografada com a chave pública do servidor, portanto só ele pode decodificá-la. O servidor pode negar ou aceitar a conexão.

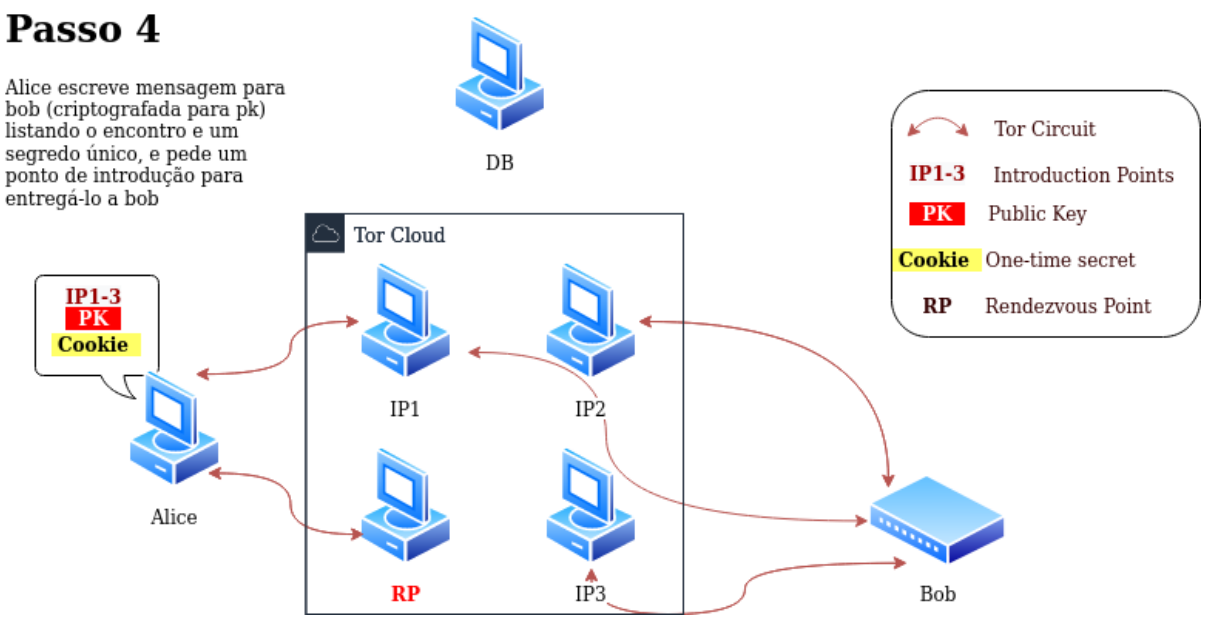


Imagem 1.3 Onion Service Router @ackercode produções

O servidor aceita a conexão e procede para utilizar o *rendezvous point*. O uso deste mecanismo de ponto de encontro é feito para um serviço poder negar conexões, reduzir a sobrecarga em cima dos pontos de introdução e distribuir o tráfego para não criar pontos de atenção na rede.

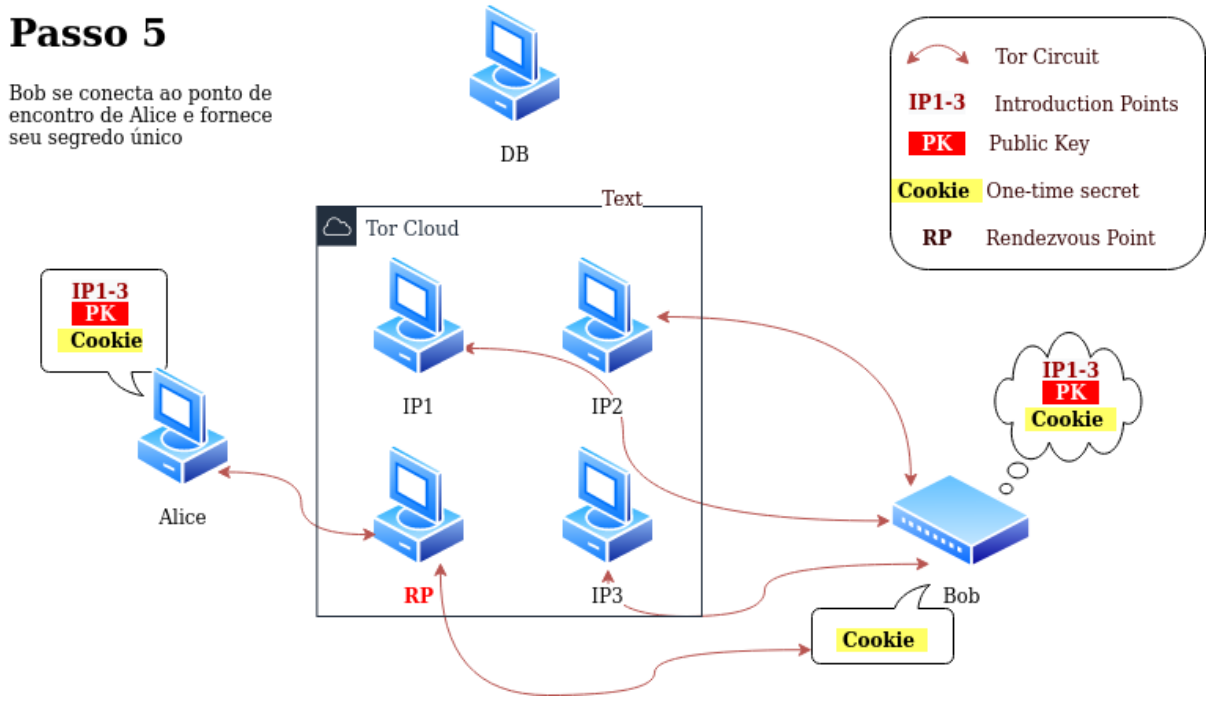


Imagem 1.4 Onion Service Router @ackercode produções

Depois disso, o servidor e o usuário se comunicam via *onion router* normalmente.

Tor versus proxies tradicionais

Um provedor de proxy típico configura um servidor em algum lugar da Internet e permite que você o use para retransmitir seu tráfego. Isso cria uma arquitetura simples e fácil de manter. Todos os usuários entram e saem pelo mesmo servidor. O provedor pode cobrar pelo uso do proxy ou financiar seus custos através de anúncios no servidor, na configuração mais simples, você não precisa instalar nada. Você apenas precisa apontar o navegador para o servidor proxy. Provedores de proxy simples são ótimas soluções se você não deseja proteções para sua privacidade e anonimato online e confia que o provedor não fará coisas ruins. Alguns provedores de proxy simples usam SSL para proteger sua conexão com eles, o que os protege contra intrusos locais, como os de um café com Internet Wi-Fi gratuita.

Provedores de proxy simples também criam um único ponto de falha. O provedor sabe quem você é e o que você navega na Internet. Eles podem ver seu tráfego enquanto ele passa pelo servidor deles. Em alguns casos, eles podem até ver dentro do seu tráfego criptografado enquanto o retransmitem para o seu site bancário ou para as lojas de

comércio eletrônico. Você precisa confiar que o provedor não está assistindo seu tráfego, injetando seus próprios anúncios em seu fluxo de tráfego ou gravando seus dados pessoais.

O Tor passa seu tráfego por pelo menos três servidores diferentes antes de enviá-lo ao destino. Como há uma camada separada de criptografia para cada um dos três relés, alguém assistindo à sua conexão com a Internet não pode modificar ou ler o que você está enviando para a rede Tor. Seu tráfego é criptografado entre o cliente Tor (no seu computador) e onde ele sai em algum outro lugar do mundo.

Baixando o tor

Tá bom, mas e agora como baixar o Tor? Neste tópico deixarei o passo a passo de como baixá-lo em uma máquina virtual para mais downloads só acessar https://www.torproject.org/download/

Primeiro vamos criar uma máquina virtual de preferência (ambiente mais seguro que o comum) se quiser só instalar o Tor direto na sua máquina, não tem problema, mas é necessário seguir todos os padrões de segurança citados neste livro.

Item	Specs
Hypervisor	VirtualBox
SO	Ubuntu (Última Versão Stable)
Memória Ram	4GB
Rede	NAT
Disco	10gb
vCPU	1

Após logar na máquina com um usuário sem privilégios, baixar o Tor no link abaixo:

https://www.torproject.org/download/

O Tor está disponível em muitos sistemas operacionais, baixe a versão correta para o Linux.

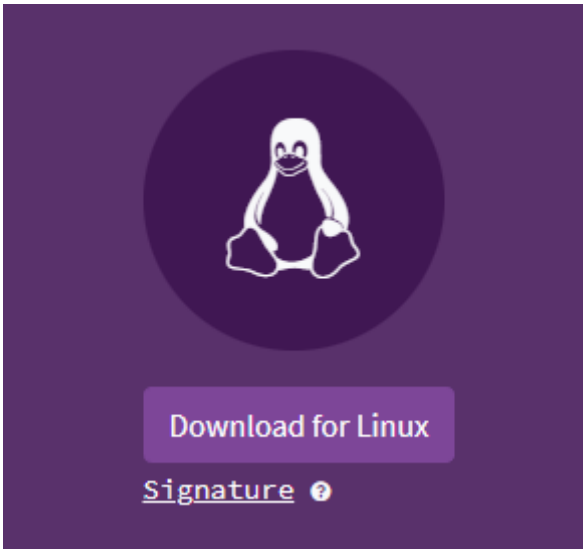


Imagem 2.0 - Download Tor - @ackercode produções

E se caso preferir que o Tor esteja em portugues basta clicar em “Download in another language or platform”:

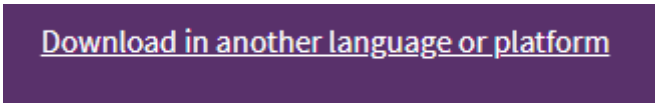


Imagem 2.1 - Download Tor - @ackercode produções

Instale o Tor descompactando o arquivo baixado e rodando no terminal:

```
.start-tor-browser.desktop dentro da pasta tor-browser
```

Agora basta entrar no Tor e começar a navegar na Dark Web.

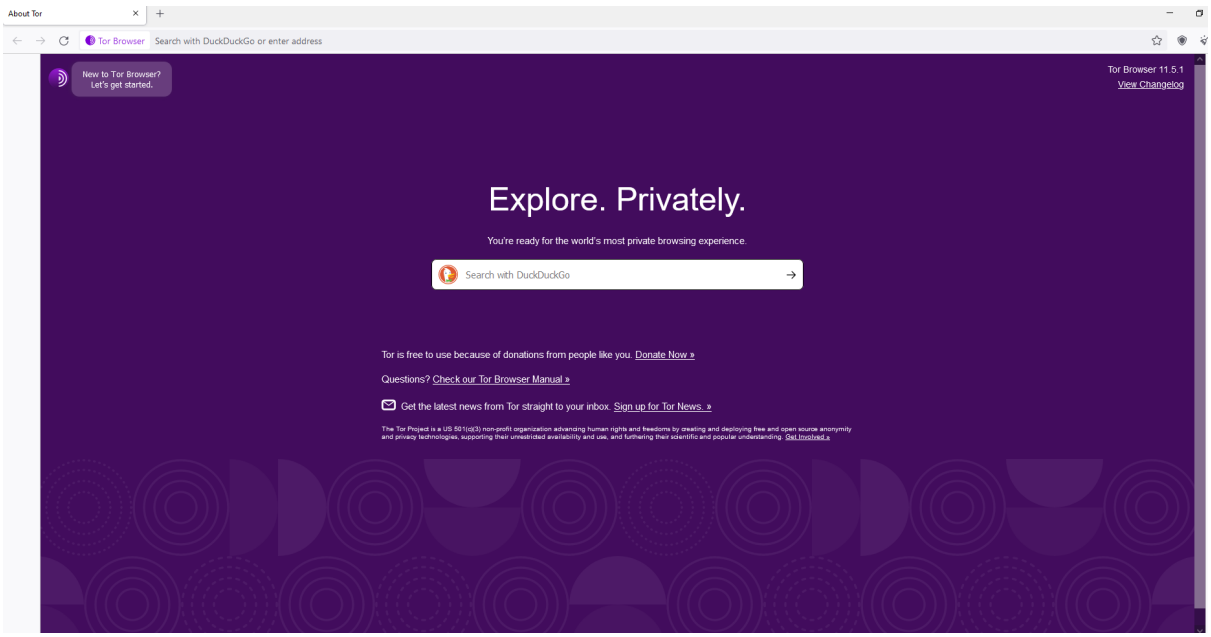


Imagem 2.2 - Download Tor - @ackercode produções

Para sua navegação ser mais segura, clique no ícone de escudo no canto superior direito:

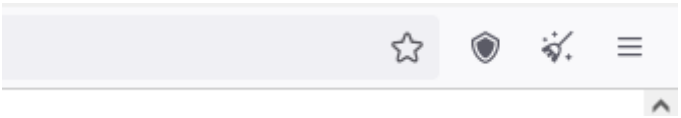


Imagem 2.3 - Download Tor - @ackercode produções

Clique em modificar a segurança e depois coloque a última opção como na imagem abaixo:

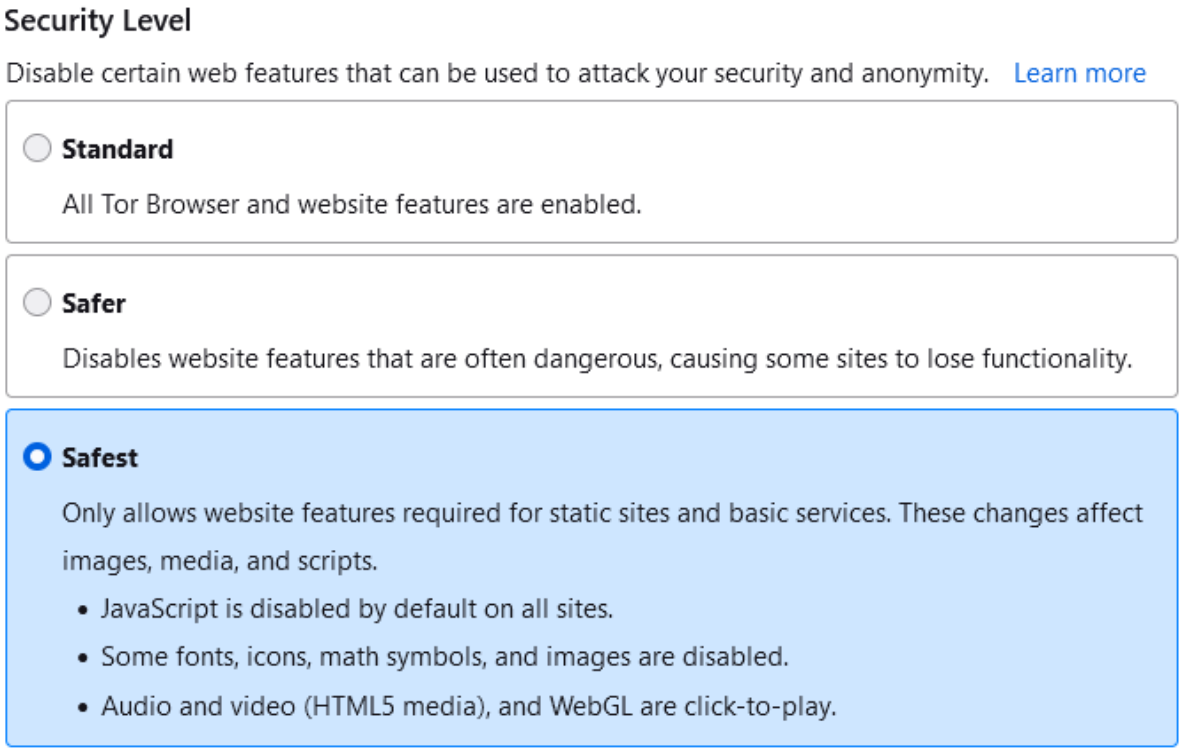


Imagem 2.4 - Download Tor - @ackercode produções

Continue na mesma tela vá para baixo e ative a opção HTTPS Only mode, para o tráfego de rede sempre seja criptografado forçando o Tor a navegar apenas em protocolo HTTPS:

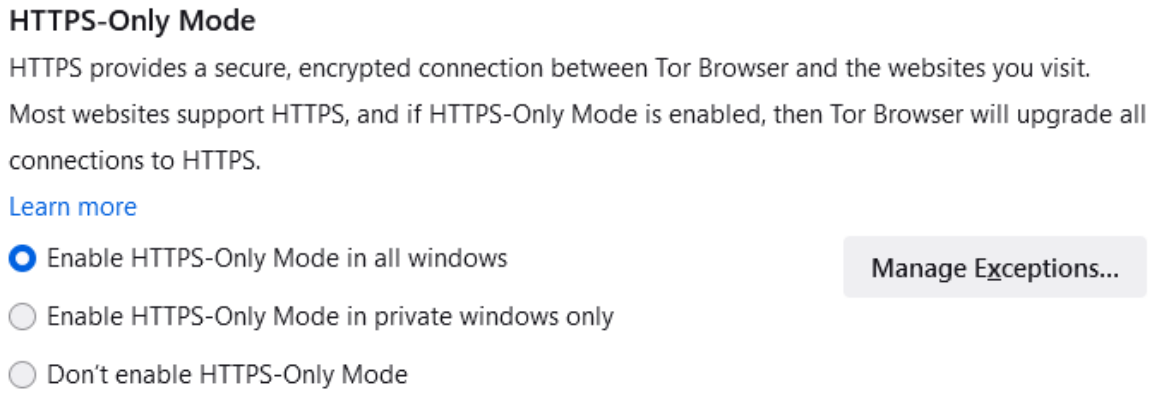


Imagem 2.5 - Download Tor - @ackercode produções

Configurando assim o Tor terá uma maior segurança, apesar de ser um browser bem seguro já por padrão.

Outra forma de navegar é utilizando o Navegador Brave (https://brave.com/pt/), além de ser um navegador muito mais rápido que o Tor, ele conta com diversos benefícios já configurados como:

- Anúncios invasivos bloqueados
- Rastreadores cross-site bloqueados
- Cookies bloqueados
- Impressões digitais bloqueadas (rastreadores sem cookies)
- Proteção contra malware e phishing
- Proteção contra rastreamento de redirecionamento
- Roteamento de rede anonimizado (modo Tor)
- Privacy by Default
- Consegue importar todos os recursos do seu Chrome

Ainda mais, o Brave possui a funcionalidade de abrir uma guia anônima utilizando o Tor, basta pressionar Alt+Shift+N ou clicar sobre o menu superior direito em *abrir janela anônima com Tor*.

VI

O que você deve saber antes de visitar a Dark Web?

1. **Logins, plugins e pagamentos devem ser evitados**

Para permanecer seguro enquanto navega na dark web, é essencial que você mantenha seu anonimato intacto o tempo todo. Fazer login em determinadas extensões online ou contas bancárias compromete isso e fará com que qualquer atividade nesses sites seja atribuída a você. Portanto, recomendamos não fazer login em nenhum perfil ao visualizar o conteúdo de tais sites por meio de extensões do navegador Tor, como “NoScript” para Firefox/Chrome etc.

Algumas pessoas podem não estar cientes dos plugins que habilitaram em seus navegadores. Como resultado, essas extensões podem coletar informações pessoais e confidenciais sobre você enquanto navega online, por isso é importante saber quais você precisa!

2. **Visitar a Dark web não é ilegal**

Vender e comprar produtos e serviços ilegais são! Mesmo que a dark web exista para facilitar essas coisas, tecnicamente não é um crime navegar lá. No entanto, fornecer ou comprar qualquer coisa desses sites pode levar você a problemas legais, portanto, certifique-se de que qualquer conteúdo que você considere acessar on-line tenha sido minuciosamente pesquisado antes de dedicar algum tempo para visitá-los. Dessa forma, você evitará quaisquer riscos potenciais envolvidos na pesquisa através de links da Dark Web nos serviços ocultos do Tor em todos os momentos!

3. **Traga um amigo**

A dark web pode ser perigosa, por isso é sempre bom ter alguém com você ao explorar esses sites - mesmo que esperemos que você nunca esteja em uma situação em que realmente precise disso! Certifique-se e confie na pessoa que você está trazendo com você também, pois há muitas pessoas desonestas que estão apenas esperando para tirar vantagem de você se tiverem a chance.
Também é bom que uma pessoa tenha uma ideia clara sobre o que não fazer nesses sites, porque embora existam muitas coisas que podem ser feitas sem muito perigo envolvido, algumas tarefas devem ser evitadas a todo custo!

4. **BTC**

Bitcoin é a criptomoeda mais conhecida, mas não oferece anonimato garantido. O Bitcoin tem vários problemas de privacidade, como reutilização de endereços e nós conectados que possibilitam vincular os dados pessoais de alguém a transações de bitcoin; isso pode ser um problema se você estiver procurando sigilo total ao fazer compras on-line ou enviar dinheiro para casa de sua empresa no exterior. Existem também outras opções disponíveis como alternativas - duas populares sendo Monero e Zcash.
Esteja ciente de que, se você quiser comprar algo na dark web, há uma chance de que seja **ilegal**. Muitos mercados vendem itens que não são permitidos e comprá-los pode colocar o comprador e o vendedor em problemas com as autoridades - portanto, certifique-se antes de comprar se é **legal ou não**, sempre!

5. **Sempre haverá riscos ao visitar a Dark Web**

Embora você possa melhorar sua segurança na dark web, nada é infalível. Os hackers encontram constantemente novas maneiras de contornar os sistemas e configurações de segurança, o que significa que sempre há uma chance de fornecer informações pessoais ou clicar em um link infectado. Além disso, uma vez que o malware tenha sido instalado no hardware do computador, eles são comprometidos em qualquer uso da Internet, pois levará apenas alguns segundos para os hackers acessarem essas informações de sua sessão de navegação - mesmo que apenas lendo mensagens de bate-papo de texto!

6. **Faça uso dos recursos disponíveis**

Utilize os recursos disponíveis – incluindo guias como este, que podem ajudá-lo a se manter seguro na dark web!
Não há pressa e é melhor você tomar seu tempo para avaliar cada site e o que está sendo oferecido, ao fazer isso, você estará aproveitando ao máximo sua experiência na dark web!
A Dark Web pode ser um ótimo lugar para pessoas que desejam evitar a vigilância do governo ou apenas desejam permanecer privadas online - mas é importante que os usuários não subestimem quanto trabalho é necessário para garantir sua segurança!

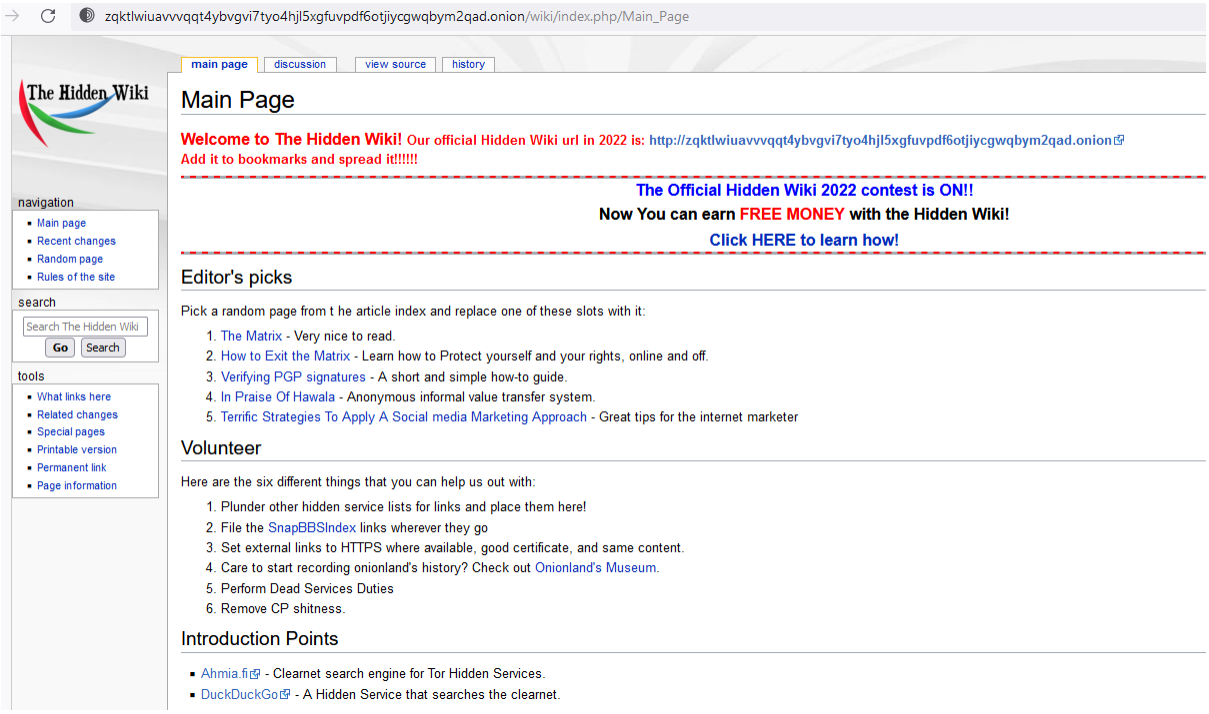
7. **Faça um plano para onde você quer ir**

Há muitos lugares que você deve evitar na dark web e não é aconselhável vagar sem rumo. Tenha um plano do que você quer fazer e veja antes de entrar, pois isso o ajudará a ficar seguro e focado na tarefa em mãos!
A dark web pode ser um ótimo lugar para encontrar ofertas de itens que não estão disponíveis em seu país, mas esteja ciente dos golpes. Muitos mercados oferecem produtos a preços incrivelmente baixos que podem ser comparados a lojas legítimas ao seu redor; eles operam pedindo o pagamento adiantado e nunca enviam o produto. Certifique-se de fazer sua pesquisa em um mercado antes de fazer qualquer compra! Abaixo, abordaremos os maiores mercados da Dark Web!

VII

Visitando a dark web com Tor

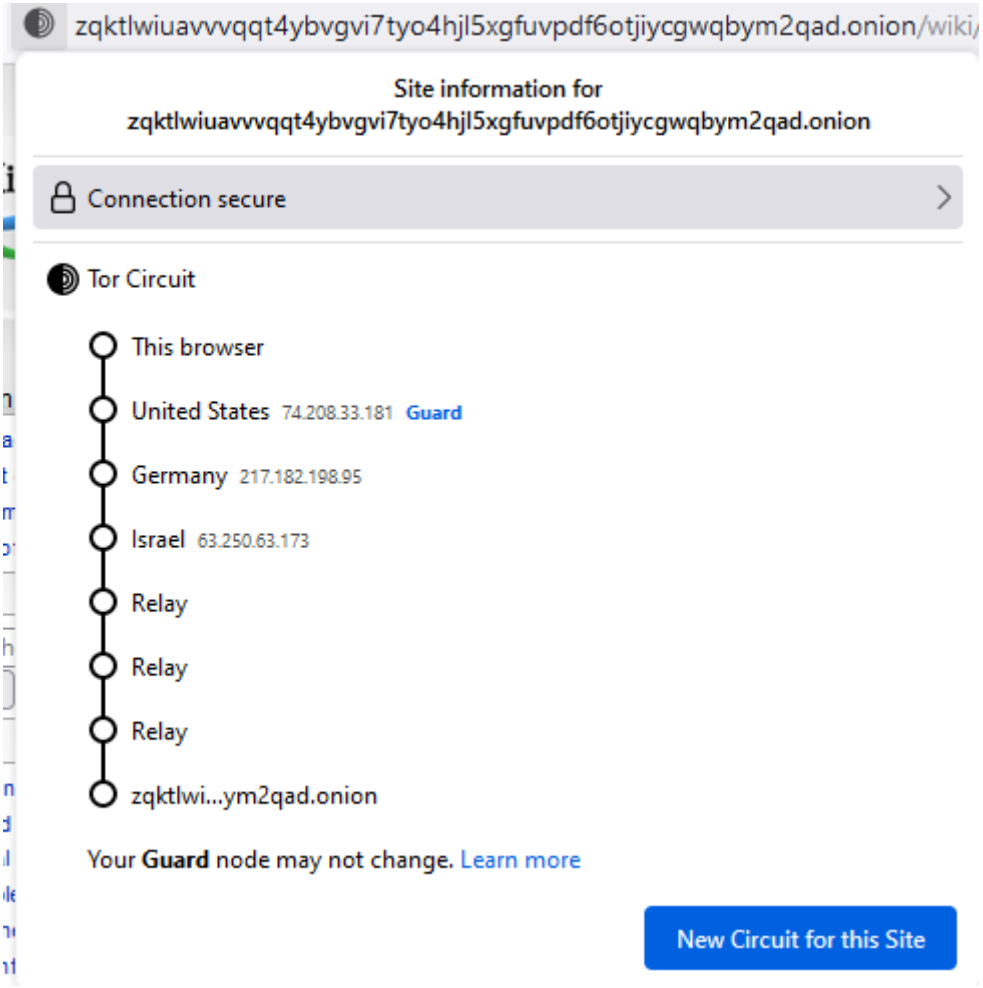
Agora vamos começar nossa análise dentro do Tor browser, vamos utilizar o link mais utilizado de todos o The Hidden Wiki: <http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/index.php/Main_Page/>



Dizem que a *The Hidden Wiki* é a wikipedia da Dark Web, nela você encontra diversos links para sites dentro da Dark Web, é um site centralizador de links. Disclaimer: use essa url com sabedoria não entre em onion sites sem saber o que quer ver.

Tenha cuidado. Não clique em um link para algo que não deseja ver, porque o Hidden Wiki não indexa apenas sites legais. De fato, existem muitos sites diferentes dentro “Hidden Wiki” por aíO Hidden Wiki costumava ser conhecido por hospedar ou, pelo menos, indexar vários sites pedófilos e, portanto, foi alvo de ataques cibernéticos pelo FBI e pelo Anonymous (o que nos da Acker Code, somos sempre a favor). Muitos copycats e spin-offs do Hidden Wiki também foram criados. Não se surpreenda se você se deparar com “The Official Hidden Wiki” ou “The Uncensored Hidden Wiki”. É melhor ficar longe desses sites secundários. A maioria dos sites da Hidden Wiki até hoje fornece links para algumas partes da dark web que você não gostaria de visitar. A melhor maneira de lidar com isso é seguir as categorias que são relativamente livres de riscos.

Para saber como está sua conexão dentro do Tor Onion Ring basta clicar no ícone ao lado do site (onion) e ver como está sua conexão e até podendo mudar a rota da conexão quantas vezes quiser.



Verificamos que nosso site passa por diversos onion rings que fica em Israel, Alemanha até chegar no site principal que está nos Estados Unidos.

Observação importante: o Tor acaba sendo um pouco lento devido a sua rede de serviço complexa, use somente para manter sua identidade privada, caso queira navegar na internet no dia a dia mantenha sempre um navegador como o Brave.

VIII

The Hidden Wiki

O wiki oculto é uma ótima maneira de começar na dark web. Depois de navegar por ele, com alguma prática, será fácil encontrar o que você está procurando!

Devido ao seu grande tamanho e ao grande número de visitantes por dia, encontrar um item específico pode levar tempo – então seja paciente.

Este site contém basicamente uma lista de links que descrevem todos os tipos de tópicos sobre os serviços ocultos do Tor, incluindo revisões/classificações de diretórios, etc. São atualizados regularmente pelos usuários que usam o onion land, os principais sites ou wikis afiliados do And que extraem esses links de outras fontes, como tópicos do Reddit, é por isso que o conteúdo pode variar um pouco em alguns lugares. No entanto, pesquisar por categorias pode ajudar a economizar tempo de caça, o que é necessário ao tentar encontrar o mercado perfeito!

Este site é destinado principalmente a comerciantes da dark web, e tem links para muitos dos mercados mais populares que operam hoje. Ele fornece uma visão geral de cada mercado, com um link para o site oficial para obter mais informações sobre os recursos oferecidos, ou seja, essa ferramenta pode ser boa e ruim, pois se você decidir que não é isso que você está procurando, há ainda muita pesquisa a fazer para encontrar um que atenda às suas necessidades!

O Hidden Wiki é um site onde você pode encontrar informações úteis sobre a dark web. Existem muitos sites nesta vasta rede, mas alguns têm descrições que os tornam mais fáceis de entender para aqueles que podem não estar familiarizados com eles, como por exemplo, o que eles contêm ou como tudo funciona em geral. Meu conselho seria ficar com as escolhas do editor, pois geralmente são os sites mais seguros e confiáveis.

O Torch é uma ótima opção para escolher quando você procura um lugar para acessar o wiki oculto, e o que pode ser visto na superfície parece completamente inofensivo. No entanto, é importante que os usuários ainda tomem precauções, pois ainda que o Hidden Wiki seja uma boa opção, é possível que contenha links que levam a sites maliciosos, ou outros perigos, como páginas de phishing junto com links contendo conteúdo terrível e vírus!

IX

Como visitar a Dark Web com segurança

Com a dark web, há muita coisa que pode dar errado. Está cheio de golpistas e sites de phishing que querem tirar seu dinheiro, colocando malware ou outras coisas prejudiciais em nossos computadores, principalmente quando não sabemos o que eles estão fazendo.

Para que isso seja evitado, você deve analisar bem antes de entrar em algo ruim. Uma sugestão é fazer qualquer pergunta através de fóruns on-line, porém certifiquem-se de ler este artigo na íntegra várias vezes para não esquecer nada.

Saiba o que deseja fazer antes de navegar na dark web, caso contrário, é provável que sua experiência seja menos agradável e frutífera, porque há muitas distrações nesses sites que podem atrapalhar a realização de algo significativo.

Você também precisará de mais do que apenas um computador para explorar esta parte do ciberespaço – lembre-se das preocupações de segurança! Certifique-se de tudo sobre o quão bem protegido tanto o hardware (computadores) quanto as plataformas de software.

1. **Use um sistema operacional via USB ou Virtualizado**

A dark web é um lugar para anonimato e privacidade. Quanto mais você se proteger, mais segura será sua experiência neste navegador de Internet oculto que não é adequado para proteger seus segredos quando o Windows 10 faz essas coisas:

A) Armazena todos os registros de sites no ONIDB – que já foi invadido por agências governamentais (incluindo a China)
B) Fornece acesso fácil ao Microsoft Edge devido aos recursos de rastreamento incorporados a ele.
C) Torna a navegação difícil porque as configurações de criptografia padrão são desativadas pelos usuários no primeiro uso.

Portanto, recomendamos o uso de um sistema operacional, como Tails OS ou Liberté Linux, que pode ser inicializado a partir de uma unidade USB. Ao contrário do Windows, esses sistemas são projetados para garantir que seu histórico de navegação e outros dados pessoais permaneçam confidenciais.

Muitos sistemas operacionais ativos, no entanto, não suportam VPNs, portanto, pode não ser uma boa ideia usar uma VPN se você quiser seguir a rota do SO, pois isso pode criar um nó de entrada e saída que pode facilitar a detecção por hackers. Se você quiser evitar a instalação do novo sistema operacional, que pode ser bastante técnico, certifique-se e siga estas próximas etapas.

2. **Use uma rede privada virtual (VPN) para protegê-lo**

O navegador Tor sozinho é conhecido por vazar o endereço IP real de um usuário. Isso significa que, mesmo que você use o navegador Tor, seu tráfego ainda pode ser rastreado por qualquer pessoa com tempo e conhecimento suficientes. É aqui que entra a VPN, no entanto. Uma Rede Privada Virtual (VPN) oculta seu endereço IP e criptografa seu tráfego para que ele não possa ser interceptado por mais ninguém enquanto você estiver navegando.
Recomendamos o uso de serviços como o Nord VPN, que custa menos de US $50 por ano e tem muitos servidores para escolher, caso você precise alterar sua localização.

3. Baixar o Tor

Agora que você tem sua VPN instalada, é hora de baixar o Tor. O Navegador Tor é um navegador da Web gratuito e de código aberto que criptografa e anonimiza seu tráfego, roteando-o por vários servidores antes de chegar ao seu destino. Isso torna difícil para qualquer pessoa rastreá-lo online ou descobrir sua verdadeira identidade.
É importante sempre baixar a versão correta do Tor em sua página oficial. Certifique-se de aprovar as atualizações assim que estiverem disponíveis para que seu sistema tenha um processo de instalação seguro e não encontre complicações durante a execução!
O navegador Tor permite acessar qualquer site, mas só funciona se o site tiver um endereço que termine em “cebola”. Muitos sites obscuros usam esse endereço e ele não será exibido quando acessado com um navegador de Internet comum por causa de como o anonimato é protegido por roteadores por meio de várias etapas, como criptografia ou rejeição de solicitações de vários nós antes de finalmente chegar ao destino.

4. Medidas extras de segurança

Mesmo que você tenha baixado sua VPN e Tor, você precisará realizar algumas etapas extras se quiser garantir que sua experiência seja a mais segura possível.
Antes de tudo, lembre-se de que muitos sites na dark web não têm SSL habilitado, o que significa que eles não podem verificar sua própria identidade ou criptografar o tráfego entre servidores e clientes – isso facilita a interceptação de comunicações por hackers. Por exemplo, a maioria dos números de cartão de crédito não são armazenados por criptografia, mas com texto simples, o que significa que qualquer pessoa pode roubá-los de uma rede insegura!

- Certifique-se de que qualquer site tenha um **“s” adicionado após “onion”** em seu endereço antes de inserir qualquer coisa sensível nele, como senhas ou dados bancários. Se não houver “s” no final, assuma que o site não é seguro e saia imediatamente sem usá-lo!
- Desative a configuração de localização do seu dispositivo. Seu endereço IP e seu dispositivo podem ser usados para determinar sua localização.
- Cubra sua webcam e microfone quando não estiver em uso. Hackers são conhecidos por obter acesso aos dispositivos das pessoas usando sua webcam e microfone sem o seu conhecimento!

5. **Feche todos os navegadores e gerenciadores de senhas.**

Quando terminar de navegar (ou mesmo enquanto ainda estiver na dark web), limpe o histórico do navegador, limpe os cookies e exclua quaisquer outros vestígios de atividade. Se possível, sempre use um sistema operacional que suporte criptografia completa de disco, como o Linux, porque, caso contrário, será fácil para alguém acessar tudo em seu computador se o roubar ou hackear.

6. **Altere os níveis de segurança no Tor**

Você pode alterar seu nível de segurança no Tor clicando no ícone “Configurações” e movendo o controle deslizante para cima ou para baixo. Quanto mais alto você for, no entanto, mais provável é que seu sinal seja interceptado, então escolha com cuidado! As seções mais seguras podem retardar sua conexão para um rastreamento, enquanto as menos seguras podem dificultar o acesso a alguns sites.

7. **Recursos extras no Tor que podem ser úteis incluem**

A capacidade de escolher qual navegador deve ser usado em páginas não-tor (geralmente esta é uma opção onde você tem vários navegadores instalados) para que a atividade de sua navegação regular na Internet não afete o Tor! Uma maneira de marcar páginas e encontrá-las facilmente digitando certas palavras-chave ou tags ao retornar em uma data posterior – lembre-se de que nem todos os sites suportam marcadores! O poder de bloquear scripts executados em sites, especialmente anúncios que são fontes conhecidas de malware. Você pode desativá-los com facilidade na maioria dos navegadores, mas se você usar o Tor, eles serão automaticamente ativados novamente.
Uma ferramenta de “Nova Identidade” que excluirá todo o histórico e cookies, além de configurar o Tor para usar um endereço IP diferente para que você possa limpar totalmente seus dados de navegação e começar do zero. Esse recurso também está disponível para outros navegadores como o Firefox, mas muitas pessoas não sabem como ele funciona ou o que exatamente ele faz.

A desativação de scripts no Tor também desativará alguns recursos em sites, então você pode experimentar um pouco para descobrir quais são importantes para você e quais você pode prescindir quando estiver navegando.

X

Como ser anônimo na internet e manter sua privacidade

Nos tempos atuais seus dados valem ouro para as empresas de marketing. Sabendo disso, muitas plataformas têm coletado todos os seus dados sem consentimento, refletindo na exposição de propagandas antes mesmo de você querer ou pensar em comprar algum item, eles já te recomendam utilizando técnicas de inteligência artificial. Com isso a privacidade e anonimato se tornam importantes não só para hackers como para pessoas comuns.

Ao navegar pela Internet, as pessoas deixam uma série de rastros online e informações sobre si. Isso porque elas utilizam navegadores, buscadores e serviços de e-mail que coletam e armazenam diversos dados pessoais. Mesmo que recorram ao modo anônimo do navegador para usar a web com mais privacidade, você não está completamente invisível.

A ótima notícia é que há uma série de plataformas e ferramentas que impossibilita ou, pelo menos, dificultam o rastreio de dados durante a navegação.

1. Substitua seu navegador pelo Tor. (Como boas práticas que já citamos neste livro)

Esse navegador roteia todo o tráfego pela sua própria rede (como explicado no tópico onion routers do livro) tornando a navegação praticamente anônima. Ao navegar usando-o, é muito difícil (perto do impossível) para seu provedor de internet, administrador de rede ou hacker em uma rede Wi-Fi ter acesso aos websites visitados ou contas acessadas.
Para isso, é importante baixar o Tor apenas pelo site oficial em https://www.torproject.org. Alem disso, caso não queira que o seu provedor de internet saiba que você usa o Tor, será preciso usá-lo em conjunto com uma VPN.

2. Use uma VPN (Virtual Private Network - Rede virtual privada).

Uma VPN criptografa tudo o que você faz na internet, mantendo seu tráfego quase que anônimo. A regra geral de uso é, ao usar um serviço consolidado de VPN, toda a sua atividade online permanecerá privada. Ela também previne que o seu provedor de internet tenha acesso ao seu histórico de navegação. No entanto, muitos servidores de VPN mantêm um registro das suas atividades, que pode ser utilizado pela justiça caso você seja suspeito de algum tipo de crime.
Embora seu provedor e outras pessoas na sua rede local não tenham acesso ao que você esteja fazendo na internet enquanto estiver usando uma VPN, o provedor da VPN terá acesso a esses dados. Infelizmente, não há como ter certeza se o seu serviço de VPN mantém um registro das suas atividades. Pesquise bem sobre as opções disponíveis ao contratar um serviço de VPN.

3. Altere seu endereço MAC.

O Mac é o endereço físico do hardware, identificando seu computador para o roteador. Sempre que você se conecta a uma rede, seu endereço Mac é transmitido para anunciar sua presença. Você pode usar um endereço Mac falso para tornar sua atividade anônima na rede, no entanto, os websites que você visitou e acessou ainda serão visíveis para o seu provedor de internet e administrador de rede, mas é possível usar uma VPN como camada extra de proteção.

4. Navegue usando pontos de acesso Wi-Fi públicos (a depender do caso).

Para realmente permanecer anônimo, sua conexão não deve envolver seu provedor de internet, por isso use um serviço de Wi-Fi público. Ainda assim, é muito importante que você não passe nenhuma informação pessoal ao usar essas redes, a menos que não tenha problema no caso de ela vazar.
Não se conecte a uma rede pública caso precise fazer algo privado em relação à sua própria identidade, como acessar conta bancária ou lidar com CPF ou outros documentos. Mesmo se você vir uma rede sem fio aberta disponível, verifique se ela é legítima do estabelecimento onde você está. Os hackers geralmente configuram redes sem fio semelhantes às de estabelecimentos especificamente para roubar dados de seus usuários. Mesmo se a rede sem fio for legítima, alguém mal-intencionado ainda poderá usar uma ferramenta para filtrar todo o tráfego da rede, se conecte a uma rede legítima de sua confiança.
Uma ótima solução é omitir seu endereço IP, conectar-se a um Wi-Fi público, conectar-se a uma VPN e navegar usando o Tor.
Se optar por utilizar sua rede padrão, lembre-se de seguir os passos anteriores.

5. Use mecanismos de busca alternativos com foco na privacidade.

Os mecanismos como o Google, Bing e Yandex armazenam seu histórico de busca juntamente com seu endereço IP (e contas abertas). Eles também podem usar cookies para rastrear como você pesquisa na internet e os sites acessados. Essa informação é compilada e analisada para exibir anúncios mais precisos e relevantes de acordo com suas pesquisas. Para evitar esse tipo de rastreamento, use alternativas com foco em privacidade, como o DuckDuckGo ou StartPage

6. Use um nickname ao navegar

Uma das melhores formas de permanecer anônimo na internet, é não utilizar seu próprio nome, apesar de ser uma dica simples, pouca gente segue. Ao deixar seu nome de lado e criar um nome aleatório faz com que as pessoas te conheçam por um vulgo e não mais por seu nome verdadeiro, deixando assim de lado seu dado pessoal. Então, caso queira manter seu anonimato na internet, mantenha seus dados pessoais longe.

7. Nunca utilize seus dados

Deixe de lado sua identidade, nunca utilize dados como email, telefone, identidades e todos seus dados pessoais, apenas utilize dados temporários ou até mesmo inexistentes criados para isto e que não vão se relacionar com você nunca.

8. No logs, no crime

Utilize técnicas para não deixar rastros em sua navegação, todas as dicas citadas acima devem ser levadas a sério, se você deixar algum rastro em sua navegação é possível de você ser rastreado. Atualmente a melhor forma de apagar seus rastros deixados no seu computador pessoal é queimando seu HD e Memoria Ram, técnicas utilizadas na série mr.robot sempre que os hackers percebem que estão sendo investigados.

O ambiente mais anônimo possível são os sistemas que possuem o princípio de “Tor First” desde sua concepção, projetos como The Amnesic Incognito Live System o famoso Tails OS são seguros de ponta a ponta e não deixam rastros.

Dicas finais de anonimato:

1. Não confie em ninguém na deep web.
2. Cubra sua webcam.
3. Se você tentar visitar os links da deep web, deverá estar protegido por uma VPN + Tor.
4. Antes de visitar a dark web, certifique-se de que uma extensão no navegador tor chamada “NoScript” esteja ativada e ative esta opção “Forbid Scripts Globally“
5. Se você quiser alguma proteção extra (ou talvez), digite “about config” na barra de endereço, role para baixo até “javascript_enabled” e altere o valor de “true” para “false”.
6. É possível rastrear seu endereço IP se você tentar acessar os sites Deep/Dark sem usar VPN. Não tenha problemas usando também uma VPN gratuita. Esteja seguro e tenha anonimato online. Obtenha o melhor serviço de VPN agora.
7. Por último, mas não menos importante, depois de abrir o wiki oculto, é altamente recomendável que você leia um artigo chamado “Como sair da matriz”.

Comunicação segura na Dark Web

A dark web é um lugar onde as pessoas se reúnem para fazer todo tipo de coisa. Uma maneira de manter contato com seus novos amigos e grupos na darknet, embora possa parecer contra-intuitivo à primeira vista, são serviços de e-mail ou mensageiros instantâneos, como o aplicativo comemorativo Tor Messenger (criado por pesquisadores de segurança). Essas plataformas permitem que os usuários entrem em contato sem revelar informações pessoais por meio de pesquisas na Internet. Um recurso útil ao tentar não apenas estabelecer relacionamentos, mas também fazer o trabalho!
Abaixo estão alguns exemplos de serviços de e-mail e plataformas de mídia social que fornecem anonimato.

E-mails

Secmail

Este é um serviço de e-mail gratuito que oferece a funcionalidade de qualquer outro cliente sem nenhum de seus inconvenientes. Você pode enviar e receber e-mails. Componha novos em movimento (mesmo sem internet), acompanhe quem está lendo. O que você enviou ou armazene-os em caixas de entrada - tudo isso mantendo sua privacidade!

Bitmail.la

Este é um serviço que permite enviar e-mails anonimamente através de seus servidores. Ele também oferece a chance de enviar mensagens criptografadas. Isso significa que eles não serão lidos por ninguém além da pessoa com quem você está se correspondendo.

Lelantos

Este é um provedor de serviços de e-mail seguro e anônimo. Isso permite o anonimato completo de seu usuário quando se trata de navegar na web ou se comunicar por e-mail. Você pode usar este serviço em qualquer dispositivo, desde que seu navegador suporta JavaScript. E não há como outra pessoa verificar quem enviou o quê e de onde. Portanto, se a privacidade é um problema, essa pode ser uma das melhores soluções disponíveis.

AnonInbox

Este é um serviço de e-mail que oferece um alto nível de segurança e privacidade para seus usuários. Não requer nenhuma instalação de software, senhas ou inscrições. Assim, você pode começar a usá-lo assim que se registrar e todas as mensagens forem criptografadas, tornando-as ilegíveis para qualquer pessoa, exceto o remetente e o destinatário.

O **melhor conselho** que poderia dar sobre esse item, se for se cadastrar em algum site ou plataforma que precise informar seu email ou telefone, utilize ferramentas que crie um email ou telefone temporário existem inúmeras como estas:

https://temp-mail.org/pt/ para criação de email temporário.
https://pt.mytempsms.com/receive-sms-online/country.html criação de número temporário.

Mídias sociais da Dark Web

Facebook Onion

Você sabia que o Facebook tem uma versão da dark web? Chama-se ‘Facebook onion’ e só pode ser acessado através do navegador Tor. Esta é uma plataforma de mídia social que permite que os usuários se comuniquem entre si, sem revelar suas identidades - perfeito para quem quer manter a privacidade! Abaixo estão algumas outras opções populares.

Minds

Este é outro site de mídia social que se concentra na liberdade de expressão, privacidade e descentralização. Tem um layout semelhante ao Facebook e Twitter, mas permite mais anonimato e privacidade para seus usuários. Você pode criar uma conta sem fornecer nenhuma informação pessoal. E converse com outros usuários no site sem que ninguém saiba sua identidade.

Twitter

Esta é provavelmente uma das plataformas de mídia social mais conhecidas por aí. E como você pode esperar, ele tem uma versão da dark web, sendo considerada a melhor ferramenta atualmente para comunicação global via Tor.
Na darknet, o nome do Twitter é 'Twitter Tor'. Você só pode navegar através do navegador Tor. Ele permite que os usuários postem tweets, sigam outros usuários, compartilhem fotos e vídeos, e se comuniquem uns com os outros sem revelar suas identidades.

Onion Link: **<https://twitter3e4tixl4xyajtrzo62zg5vztmjuricljdp2c5kshju4avyoid.onion/>**

XI

Monitoramento na Dark Web

A dark web de maneira geral, e especialmente a rede Tor, oferece uma plataforma segura para prática das mais diversificadas atividades que vão desde mercados anônimos a meios seguros de comunicação que proporcionem uma infraestrutura não rastreável e difícil de combater para a implementação de malwares e botnets. Assim sendo, o monitoramento e o rastreamento das atividades da dark web vêm se tornando cada vez mais relevantes para as agências de segurança, com especial atenção à rede Tor, possivelmente se estendendo também a outras tecnologias emergentes –I2P, por exemplo. Entretanto, dado seu intrincado projeto e encadeamento, grandes desafios emergem, sendo os esforços para endereçá-los especialmente concentrados em:

- **Mapeamento de serviços de diretório ocultos:** tanto o Tor quanto o I2P usam um domain database construído sobre um sistema distribuído conhecido como Distributed Hash Table(DHT). Um DHT funciona tendo nós no sistema colaborativamente responsáveis pelo armazenamento e manutenção de um subconjunto do banco de dados, na forma de key-value store. Graças a essa natureza distribuída de resolução de domínio de serviços ocultos, é possível implantar nós no DHT para monitorar solicitações provenientes de um determinado domínio (https://donncha.is/2013/05/trawling-tor-hidden-services/#comments). Ao fazer isso, é possível ter uma visão parcial do banco de dados de domínios e

inspecionar solicitações em andamento. Mesmo que isso não permita rastrear quem está tentando acessar um determinado serviço, ele oferece uma boa estimativa estatística dos novos domínios que estão ganhando popularidade. Além disso, a execução de mais desses nós fornecerá uma visão estatística melhor das solicitações gerais na rede.

- **Monitoramento dos dados dos clientes:** agências de segurança podem se beneficiar da análise dos dados de navegação web do cliente em busca de conexões com domínios não padrão. Dependendo do nível de uso da web no lado do cliente, isso pode não ajudar no rastreamento de links para a dark web, mas ainda pode fornecer insights sobre atividades hospedadas em domínios maliciosos de alto nível, sem invadir a privacidade do usuário, uma vez que somente os destinos das requisições precisam ser monitorados e não quem está se conectando a eles.

- **Monitoramento de site social:** sites como o Pastebin são frequentemente usados para a troca de informações e de endereços referentes a novos serviços ocultos (" hidden services") e, assim, devem ser mantidos sob ostensiva vigilância.

- **Monitoramento de serviços ocultos:** serviços ocultos tendem a ser muito voláteis, desaparecendo e, posteriormente, aparecendo, com novo nome de domínio. Dessa forma, é essencial tirar snapshots de cada novo site assim que ele venha a ser detectado, seja para posterior análise ou para monitoramento de suas atividades on-line. Embora o rastreamento na surface web seja uma prática, geralmente, envolvendo a recuperação de recursos relacionados a um site, isso não é recomendado na dark web, pois, por exemplo, há possibilidade de baixar automaticamente conteúdos como pornografia infantil, cuja simples posse é considerada ilegal na maioria dos países

- **Análise semântica:** depois que os dados de um serviço oculto (qualquer site da dark web) forem recuperados, a construção de um banco de dados semântico que contenha informações relevantes sobre esse site pode ajudar a rastrear futuras atividades ilegais nele e associá-las a agentes maliciosos.

- **Marketplace profiling:** finalmente, seria útil concentrar-se na construção dos perfis das transações efetuadas nos marketplaces (simplificadamente, pontos de comércio) na dark web, a fim de coletar informações a respeito dos vendedores,

usuários e tipos de mercadorias trocadas. Perfis individuais podem ser construídos ao longo do tempo.

Enfim, a deep web, mas especificamente as redes na dark web, a exemplo da Tor, podem acabar se tornando uma forma viável, também, para que agentes maliciosos venham a praticar condutas delituosas de forma anônima.

Um vídeo que acho super importante para saber como os agentes ilegais que trabalham na dark web foram pegos, foi tratado na **DefCon 22** e o link da apresentação se encontra aqui: https://www.youtube.com/watch?v=tlxmUfnpr8w

XII

Hackers na Dark Web

Como mencionamos, existem muitos serviços diferentes disponíveis na dark web, e um deles é o hacking. Esta pode ser uma ótima maneira de obter informações sobre conteúdos sobre hacker que você pode não encontrar em outro lugar.

Existem muitos hackers também que oferecem seus serviços na dark web, e a maioria deles tem sites onde você pode contratá-los. Uma coisa que você deve observar antes de contratar um hacker é que existem muitos golpes por aí. Por isso, é importante que você faça primeiro a sua pesquisa.

Há também muitos hackers legítimos que fornecerão um trabalho de qualidade. Então, tudo se resume ao que você está procurando e quanto dinheiro você está disposto a gastar. A melhor maneira de encontrar um hacker legítimo é usando o Hidden Wiki.

Quais são as razões para contratar um hacker? A maioria das pessoas faz isso porque precisa de informações que não estão disponíveis online, ou através de outras fontes, isso pode incluir qualquer coisa, desde vazamento de documentos confidenciais para se obter um rastro de alguém, vírus de computador para recuperar contas e etc. Também há usuários que procuram ajuda em um sentido mais geral, como obter acesso a contas de mídia social ou endereços de e-mail perdidos.

Os hackers podem ser muito úteis quando se trata de recuperar informações necessárias por motivos pessoais ou financeiros. Eles geralmente são qualificados em áreas como

hacking e recuperação de dados, e a segurança cibernética os torna a opção perfeita para quem precisa de ajuda nessa área.

Existem também formas de ser hackeado na Dark Web e para evitar você deve sempre usar um bom software antivírus, uma boa VPN e esteja ciente dos diferentes tipos de ataques de phishing. Certifique-se de que suas senhas sejam fortes e atualizadas. E nunca clique em links ou baixe arquivos de fontes desconhecidas.

Alguns dos principais tipos de ataques de phishing produzidos na Dark Web e fora dela incluem:

- ➢ Páginas de login falsas que roubam sua senha e/ou detalhes do cartão de crédito.
- ➢ E-mails que afirmam ser de empresas legítimas. Mas contêm links que levam a um site falso para que hackers tenham acesso a contas e informações pessoais.

XIII

Subindo seu site na Dark Web

Vamos configurar um servidor que hospeda um site estático na Dark Web. Usaremos os serviços do Tor e arquivos estáticos em html para simplicidade e segurança.

Este tutorial é destinado e testado em um servidor remoto executando o Ubuntu 18.04, e deve ser devidamente protegido para uso em produção. Cabe ressaltar que este tutorial também assumirá que você tem uma familiaridade básica com a Dark Web que já ensinamos neste livro e já possui o navegador Tor.

Tor

Em caso de erros entre no modo super user:

```
sudo su
```

Instale o Tor:

```
sudo apt-get update
```

Em seguida, instale o Tor:

```
sudo apt-get install tor
```

The hidden service

Precisamos editar o arquivo de configuração do Tor para habilitar nosso serviço oculto. Primeiro faremos um backup deste arquivo de configuração.

```
sudo cp /etc/tor/torrc /etc/tor/OLD.torrc
```

Em seguida, edite o arquivo de configuração:

```
sudo nano /etc/tor/torrc
```

Para sair do nano - ctrl + x e depois y para salvar

Por padrão, todos os serviços do cliente Tor, retransmissões e serviços ocultos são comentados e desabilitados. Vamos ativar o serviço oculto. Encontre a seção de serviços ocultos. Vai parecer algo assim:

```
############### This section is just for location-hidden
services ###
## Once you have configured a hidden service, you can look at
the
## contents of the file ".../hidden_service/hostname" for the
address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x
to the
## address y:z.
#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServiceDir /var/lib/tor/other_hidden_service/
```

```
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

Descomente as seguintes linhas:

```
#HiddenServiceDir /var/lib/tor/hidden_service/
#HiddenServicePort 80 127.0.0.1:80
```

A seção de serviços ocultos agora deve ficar assim:

```
############### This section is just for location-hidden
services ###
## Once you have configured a hidden service, you can look at
the
## contents of the file ".../hidden_service/hostname" for the
address
## to tell people.
##
## HiddenServicePort x y:z says to redirect requests on port x
to the
## address y:z.

HiddenServiceDir /var/lib/tor/hidden_service/
HiddenServicePort 80 127.0.0.1:80

#HiddenServiceDir /var/lib/tor/other_hidden_service/
#HiddenServicePort 80 127.0.0.1:80
#HiddenServicePort 22 127.0.0.1:22
```

Reiniciar Tor:

```
sudo service tor restart
```

Libere a pasta do Tor para ser acessada:

```
sudo chmod 700 -R /var/lib/tor/
sudo service tor restart
```

Alguns arquivos devem ter sido gerados pelo Tor. O primeiro é um arquivo de nome de host(seu site tor). Abra-o para obter seu endereço .onion:

```
sudo nano /var/lib/tor/hidden_service/hostname
```

Meu arquivo continha “daeadccneppthiadedizgn.onion”. Seu arquivo deve conter algo semelhante. O outro arquivo é uma chave privada. Abra e dê uma olhada:

```
sudo su

cd /var/lib/tor/hidden_service/

Agora de um sudo nano no arquivo secret_key

sudo nano secret_key
```

Deve ser semelhante a este:

```
-----BEGIN RSA PRIVATE KEY-----
MIICXgIBAAKBgQCnNsOc9iODyPGeLFvkTcgENzZ/c1aKAwslQ/WwLjd9rRh4rf
K7
4887uS+Thb3ggnVDc+GKHwkBlJY5Zvo95atYIHigGHR1QCbZ1GCBt4YebLcCBr
NG
1zsDoDEbxu4MqVB+0dntEJ2CDciHz6lnSvz9VJoWA8m5PNlC4ITZ+v1prQIDAQ
AB
AoGBAKCCPCFmUE8HS492qzqqwy3wxfpvf4l5RHCgHK3in1efGZd1+kQLeHiu2Z
F1
```

```
Vv+0mtWF3eDUy7g0oDluck1337Haxor1FcoKGEgpCXtVnOuEnEJEn/K+dFsxFY
Bd
AUuZ61yOC7cWySAJA1pi5CtJQm1aH10IxyNYg9kjOPbEiIjBAkEA3UtXwwTxHW
LZ
hvcBLzM3uQ31CK93HKar40DyYmlOHZfHPhzgwjr3gwbAjqKnx0AXcnBuhy1gww
W8
U4V6yDSNyrqfiYcMPCYVEKZV/ebmBLW0BWOw+kimukGhGQ==
-----END RSA PRIVATE KEY-----
```

Com esses dois arquivos você pode mover seu servidor para uma nova máquina caso seja necessário. Copie esses arquivos e mantenha-os seguros.

Nginx

Nginx é um bom servidor web para este projeto. Instale o Nginx

```
sudo apt-get install nginx
```

Seu servidor deve estar executando um firewall. Eu recomendo o Firewall Descomplicado (UFW). Se precisar de ajuda com o UFW, confira A Guide to the Uncomplicated Firewall (UFW) for Linux . O comando a seguir permitirá o tráfego HTTP.

```
sudo ufw allow 'Nginx HTTP'
```

Visite o endereço IP do seu servidor para verificar se o servidor web está operacional. Se as coisas estiverem funcionando corretamente, remova esta regra. Em seguida, recarregue o firewall. (demora um tempo para o reload funcionar)

```
sudo ufw deny 'Nginx HTTP'
sudo ufw reload
```

```
Resultado: Firewall not enabled
```

nginx.conf

Edite o arquivo de configuração principal do Nginx para desabilitar o compartilhamento de informações indesejáveis.

```
sudo nano /etc/nginx/nginx.conf
```

Dentro do http bloco adicione o seguinte:

```
server_name_in_redirect off;
server_tokens off;
port_in_redirect off;
```

Salve o arquivo.

Em seguida, reinicie o servidor Nginx:

```
sudo systemctl restart nginx
```

Web Server Root Directory

Crie um diretório para armazenar nossos arquivos para o servidor web.

```
sudo mkdir /var/www/dark_web
```

Crie e edite um arquivo index.html para seu site:

```
sudo nano /var/www/dark_web/index.html
```

Dentro basta colocar qualquer coisa. Nós não precisamos de html real, apenas algo meio único para agora:

```
Bem-vindo à minha página da Dark Web
```

Defina as permissões para que o Nginx possa acessar os arquivos.

```
sudo chmod 755 /var/www/dark_web
```

Remover o padrão do Nginx:

```
sudo rm /etc/nginx/sites-enabled/default
sudo rm /etc/nginx/sites-available/default
```

Adicionar site disponível:

```
sudo nano /etc/nginx/sites-available/dark_web
```

Dentro, adicione o seguinte substituindo os valores root e server_name para sua instância (server_name será seu site onion adquirido anteriormente e o root pode ser o padrão abaixo ou outra porta de sua preferência);

```
server {
     listen 127.0.0.1:80;
     root /var/www/dark_web/;
     index index.html;
     server_name n5622uuovjmgmk24omkugh4ny745bjxbtxkxyd.onion;
}
```

Adicione este site o site_enabled:

```
sudo ln -s /etc/nginx/sites-available/dark_web
/etc/nginx/sites-enabled/
```

Em seguida, reinicie o servidor Nginx.

```
sudo systemctl restart nginx
```

Navegador Tor

Abra seu navegador Tor e visite seu endereço .onion que foi gerado anteriormente. Se o sistema estiver funcionando corretamente, você verá a index.html página fictícia que criamos anteriormente.

Conclusão

Então agora você tem um site na Dark Web. Qualquer arquivo no `/var/www/dark_web` estará disponível online. Se você usar um gerador de site estático, essa será a pasta para a qual a saída será.

XIV

Criando sua ferramenta com Python para a Dark Web

1. **Instale o Tor**

Instale o Tor aqui ou via linha de comando como ensinando no tópico anterior:

```
sudo apt-get install tor
```

Iniciando o Tor:

```
sudo service tor start
```

Verifique se funcionou, basta executar o seguinte comando de um terminal:

```
curl --socks5 localhost:9050 --socks5-hostname localhost:9050 -s https://check.torproject.org/ | cat | grep -m 1
Congratulations | xargs
```

2. **Instale a biblioteca necessária**

Lembre-se de usar algum tipo de sistema de ambiente Python isolado. Eu gosto de virtualenvwrapper, mas muitos outros preferem pipenv.

```
pip install requests
```

3. **Depois importa**

```
import requests
```

4. **Usando Session**

Estaremos usando o objeto Session da biblioteca Requests. Este objeto permitirá que determinado parâmetro seja persistente. Vamos criar um objeto Session vazio.

```
session = request.session()
session.proxies = {}
```

Normalmente fazemos solicitações com a biblioteca Request assim:

```
r = requests.get('https://beacons.ai/ackercode')
```

Mas o uso do objeto Session é um pouco diferente:

```
r = session.get('https://beacons.ai/ackercode')
```

5. **Verificando nosso IP atual**

Não mostrarei meu endereço IP real. Em vez disso, eu estarei usando o endereço do seu roteador 192.168.0.1.

Vamos verificar o endereço IP pedindo usando o httpbin.org.

```
r = session.get('http://httpbin.org/ip')
print(r.text)
```

Nos dá como resultado:

```
{
    "origin": "192.168.0.1"
}
```

6. **Usando Proxies**

Agora vamos criar um novo objeto Session e então adicionar nossos proxies.

```
session = requests.session()
session.proxies = {}
session.proxies['http'] = 'socks5h://localhost:9050'
session.proxies['https'] = 'socks5h://localhost:9050'
```

7. **Verificando nosso novo IP**

Agora verificamos o endereço IP novamente:

```
r = session.get('http://httpbin.org/ip')
print(r.text)
```

Nos dá como resultado:

```
{
    "origin": "185.220.101.26"
}
```

Este IP parece ser da África Oriental, mas estou no Brasil. A coisa parece estar funcionando.

Dark Web Requests Python

Essa configuração também nos permitirá solicitar serviços ocultos do Tor, também conhecidos como dark web. Vamos visitar um site bastante notório neste exemplo. Um site que tem sido usado para revoluções violentas, drogas, e para interferir nas eleições democráticas. Eu só quero avisá-lo. Esses caras ganham dinheiro vendendo informações pessoais e eles literalmente vendem para qualquer pessoa. Estamos indo para o Facebook. Eles executam um serviço oculto no facebookcorewwwi.onion. Se você tentar visitar este endereço em um padrão sem o Tor, não receberá nada. Mas vamos tentar com nosso objeto Session.

```
r = session.get('https://www.facebookcorewwwi.onion/')
print(r.headers)
```

E nós vamos obter o resultado:

```
{
   'Content-Encoding':'gzip',
   'Strict-Transport-Security':'max-age=15552000; preload',
   'X-Frame-Options':'DENY',
   'X-Content-Type-Options':'nosniff',
   'Connection':'keep-alive',
   'Date':'Tue, 06 Feb 2018 23:41:05 GMT',
   'Transfer-Encoding':'chunked',
   'Set-
Cookie':'fr=0ibUkv48vNYqUtRGO..Baej0R.a4.AAA.0.0.Baej0R.AWXOsJtM;
expires=Mon, 07-Aug-2022 23:41:05 GMT; Max-Age=7776000; path=/;
domain=.facebookcorewwwi.onion; secure;
httponly,sb=ET16Wt8nU0VqZwyI2JREUG7L; expires=Thu, 06-Feb-2020
23:41:05 GMT; Max-Age=63072000; path=/;
domain=.facebookcorewwwi.onion; secure; httponly',
   'Content-Type':'text/html; charset=UTF-8',
   'Cache-Control':'private, no-cache, no-store, must-revalidate',
   'Vary':'Accept-Encoding',
   'Expires':'Sat, 01 Jan 2000 00:00:00 GMT',
   'X-XSS-Protection':'0',
   'X-FB-Debug':'rPWGof2T7AWYKmygk/NHSKiD73OmtkI579bnw
/2FQxmgmIKmB92dRJYTjXLr13Fj79PNaBYfp4N5/F2dzcNbSg==',
   'Pragma':'no-cache'
}
```

Agora temos acesso à dark web por meio de nossos scripts Python. Agora é hora de ficar paranóico.

1. **User-agent**

Estamos enviando algumas informações de nossos pedidos:

```
r = session.get('https://httpbin.orguser-agent')
print(r.text)
```

O que nos retorna:

```
{
    "user-agent”: “python-requests/3.7.4"
}
```

Bem, eles saberiam que somos um script Python, qual biblioteca estamos usando e algumas informações de versão. Nós podemos mudar isso.

Vamos criar alguns cabeçalhos de solicitação e alterar o User-agent:

```
headers = {}
headers['User-agent'] = “HotJava/1.1.2 FCS”
```

Alguém se lembra do HotJava? Você sabe que é antiquado quando a página de download avisa que o software não é seguro para Y2K.

Em seguida, incluímos os cabeçalhos na solicitação:

```
r = session.get('https://httpbin.org/user-agent',
headers=headers)
print(r.text)
```

O que nos retorna:

```
{
    "user-agent": "HotJava/1.1.2 FCS"
}
```

2. Cookies

Usar o objeto Session significa que temos cookies. Usaremos httpbin para definir um cookie com o valor “Hello”:

```
session.get('http://httpbin.org/cookies/set/sessioncookie/Hello')
```

Agora verificamos se esse cookie está funcionando:

```
r = session.get('http://httpbin.org/cookies')
print(r.text)
```

O que nos retorna:

```
{
    "cookies": {
        "sessioncookie": "Hello"
    }
}
```

Podemos eliminar os cookies:

```
session.cookies.clear()
r = session.get('http://httpbin.org/cookies')
print(r.text)
```

Resultado:

Código Final

```
import requests
session = requests.session()
session.proxies = {}

session.proxies['http'] = 'socks5h://localhost:9050'
session.proxies['https'] = 'socks5h://localhost:9050'

#request NORMAL
r = requests.get('http://httpbin.org/ip')
print(r.text)

#request TOR
r = session.get('http://httpbin.org/ip')
print(r.text)
```

Obtendo uma nova identidade

Se você precisar de uma nova identidade e alterar seu endereço IP, precisará instalar o stem:

```
pip install stem
```

O controlador Tor também deve ser configurado para solicitar renovação de identidade:

```
sudo nano /etc/tor/torrc
```

Usamos os parâmetros:

```
ControlPort 9051
CookieAuthentication 1
```

Em seguida, reiniciamos o Tor para levar em consideração essas modificações:

```
sudo service tor restart
```

Com Python, agora usamos o seguinte comando:

```
from stem import Signal
from stem.control import Controller

with Controller.from_port(port = 9051) as c:
    c.authenticate()
    c.signal(Signal.NEWNYM)
```

Para verificar, verificamos se obtemos um novo IP com:

```
requests.get('https://api.ipify.org', proxies=proxies).text
```

Fortaleça o anonimato alterando o User-Agent

Se o anonimato for necessário, pode ser útil alterar o user-agent , que traz nossa identidade para o servidor. Para fazer isso, instale fake_useragent:

```
pip install fake_useragent
```

Podemos então usar, em Python:

```
from fake_useragent import UserAgent
headers = { 'User-Agent': UserAgent().random }
requests.get(url, proxies=proxies,
headers=headers).text
```

Automação com Cron

Se seu script Python for usado regularmente usando um trabalho Cron, pode ser útil adicionar um atraso aleatório para evitar que o tempo de acesso seja muito regular:

```
import random, time
wait = random.uniform(0, 2*60*60)
time.sleep(wait)
```

XV

Ferramentas

1. **Ferramentas para dispositivos Apple:**

Tor.framework - A maneira mais fácil de incorporar o Tor no aplicativo para iOS.

iCepa - Cliente Tor baseado em VPN em todo o sistema Apple iOS.

2. **Ferramentas para dispositivos Android:**

Orbot - Fornece Tor na plataforma Android.

Orfox - Fornece o navegador Tor na plataforma Android.

Biblioteca Tor Onion Proxy - Fornece um JAR e um AAR para incorporar um proxy de serviço Tor Onion em um programa Java ou Android.

3. **Ferramentas de desenvolvimento e pesquisa gerais**

HTTPS Everywhere - HTTPS Everywhere é uma extensão do Firefox e Chrome que criptografa suas comunicações com muitos dos principais sites, tornando sua navegação mais segura.

Nyx - Nyx (anteriormente arm) é um monitor de status de terminal para Tor destinado a aficionados de linha de comando, conexões ssh e qualquer pessoa com um terminal tty. Isso funciona da mesma forma que o top faz para o uso do sistema, fornecendo estatísticas em tempo real para largura de banda, uso de recursos, conexões e muito mais.

Orbot - Fornece Tor na plataforma Android. O projeto está em desenvolvimento ativo, atualizações para as versões mais recentes do Tor e trabalhando para se manter atualizado com todas as mudanças no Android e nas ameaças móveis.

The Amnesic Incognito Live System - O Amnesic Incognito Live System é uma distribuição live CD/USB pré-configurada para que tudo seja roteado com segurança pelo Tor e não deixe rastros no sistema local. Esta é uma fusão dos projetos Amnesia e Incognito, e ainda em desenvolvimento muito ativo.

Tor Messenger - O Tor Messenger é um programa de bate-papo multiplataforma que visa ser seguro por padrão e envia todo o seu tráfego pelo Tor.

Shadow - Shadow é um simulador de rede de eventos discretos que executa o software Tor real como um plug-in. Shadow é um software de código aberto que permite a experimentação Tor precisa, eficiente, controlada e repetível. Para outro simulador, consulte ExperimenTor.

Stem - Biblioteca de controladores Python para scripts e aplicativos controladores usando Tor.

Txtorcon - Implementação do protocolo de controle Tor assíncrono baseado em torção. Inclui testes de unidade, exemplos, código de rastreamento de estado e abstração de configuração. Usado pela OONI e APAF.

Metrics - Processamento e análise de dados de consenso, fornecidos aos usuários por meio do portal de métricas. Isso está em desenvolvimento ativo há vários anos por Karsten Loesing.

Relay Search - Relay Search é um aplicativo da web para descobrir relés e pontes do Tor. Ele fornece informações úteis sobre como os relés são configurados juntamente com gráficos sobre seu uso anterior.

Este é o sucessor espiritual do TorStatus, cuja base de código original foi escrita em PHP e reescrita por estudantes de Wesleyan como Django. Se você se aprofundar nesse espaço, confira também o Globe, outro site semelhante que foi descontinuado.

Onionoo - Onionoo é um protocolo baseado em JSON para aprender informações sobre relés e pontes Tor atualmente em execução.

ExitMap - Scanner para a rede Tor por Philipp Winter para detectar saídas maliciosas e mal configuradas. Para obter mais informações sobre como funciona, consulte seu artigo de pesquisa Spoiled Onions.

Weather - Fornece notificação automática aos operadores de retransmissão inscritos quando sua retransmissão estiver inacessível. Isso passou por uma reescrita pela equipe Wesleyan HFOSS, que foi ao ar no início de 2011.

GetTor - Autoresponder de e-mail fornecendo os pacotes do Tor via SMTP. Isso tem sido relativamente inalterado por um bom tempo.

TorCheck - Site para determinar se o visitante está usando o Tor ou não.

BridgeDB - Distribuidor de ponte de back-end, lidando com os vários pools em que são distribuídos. Isso foi desenvolvido ativamente até o outono de 2010.

Ooni Probe - Scanner de censura, verificando sua conexão local para conteúdo bloqueado ou modificado.

TorFlow - Biblioteca e coleção de serviços para monitorar ativamente a rede Tor. Estes incluem os Bandwidth Scanners (medindo a taxa de transferência de relés) e SoaT (varre por arquivos maliciosos ou mal configurados

4. **Troca de Mensagens**

Briar - Mensagens e fóruns criptografados ponto a ponto em vários transportes, incluindo Bluetooth, Wi-Fi clearnet ou rede Tor.

Ricochet - cliente baseado em Jabber que cria um serviço Onion usado para se encontrar com seus contatos sem revelar sua localização ou endereço IP.

TorChat-Mac - cliente TorChat nativo do Mac OS X.

TorChat - Mensageiro instantâneo anônimo descentralizado em cima dos Serviços Ocultos do Tor.

5. **Ferramentas para offensive security**

ToRat - Ferramenta de administração remota multiplataforma escrita em Go usando Tor como mecanismo de transporte.

dos-over-tor - PoC de negação de serviço sobre a ferramenta de teste de estresse Tor.

oregano - módulo Python que é executado como um machine-in-the-middle (MITM) aceitando solicitações do cliente Tor.

Offensive Tor Toolkit - Série de ferramentas escritas em Go que simplificam o uso do Tor para tarefas típicas de exploração e pós-exploração.

6. **Ferramentas Onion Service**

Enterprise Onion Toolkit - Ferramenta para auxiliar em implantações em larga escala de sites HTTP(S) Onion como uma presença oficial Onionspace para sites clearnet existentes.

OnionBalance - Balanceamento de carga e redundância para serviços ocultos do Tor.

Stormy - Fácil criação de serviços Tor Onion ("Serviços de Localização Oculta"), atualmente em desenvolvimento pesado.

Vanguards - Versão 3 script de mitigação de ataque de descoberta de guarda de serviço Onion (destinado para eventual inclusão no núcleo Tor).

goldy/tor-hidden-service - Contêiner do Docker capaz de fornecer vários serviços Onion simultâneos no formato da Versão 2 ou da Versão 3, juntamente com suporte adicional para Vanguards.

7. **Distros OS**

O Amnesic Incognito Live System (TAILS) - Distribuição Live CD/USB pré-configurada para que tudo seja roteado com segurança pelo Tor e não deixe rastros no sistema local.

Whonix - Sistema operacional de desktop que pode ser executado em várias configurações, que roteia todo o ambiente de desktop e sistema operacional do usuário através do Tor.

tor-ramdisk - distribuição micro Linux baseada em uClibc cujo único propósito é hospedar com segurança um servidor Tor puramente em RAM.

8. Transporte

ScrambleSuit - Módulo Python para Obfsproxy adequado para Tor, VPN, SSH ou qualquer outro aplicativo que suporte SOCKS.

Stegotorus - Máscara o tráfego de um cliente Tor para o ponto de entrada na rede Tor de forma que pareça tráfego HTML comum.

9. Tor controller interfaces

Bine - Biblioteca Go para acessar e incorporar clientes e servidores Tor.
PHP TorControl - biblioteca PHP para controlar um servidor Tor.
Stem - A biblioteca oficial do controlador Python do TorProject para scripts e aplicativos de controlador usando o Tor.
tor.rb - Biblioteca Ruby para interagir com a rede de anonimato Tor.
txtorcon - Implementação oficial do TorProject da especificação de controle para Tor usando a biblioteca de rede Twisted para Python (suporta Py2, PyPy e Py3).

10. Tor protocol implementations

haskell-tor - Implementação Haskell do protocolo Tor.
node-Tor - Implementação Javascript do projeto de anonimizador Tor (ou Tor like).

11. Denúncias

GlobaLeaks - Software gratuito destinado a permitir iniciativas de denúncias seguras e anônimas.

SecureDrop - Sistema de envio de denúncias de código aberto que as organizações de mídia podem usar para aceitar documentos com segurança e se comunicar com fontes anônimas.

12. Compartilhamento de arquivos

OnionShare - Ferramenta de código aberto que permite compartilhar de forma segura e anônima um arquivo de qualquer tamanho.

ZeroNet - Site descentralizado e plataforma de aplicativo da Web baseado no protocolo BitTorrent com blockchain semelhante ao Bitcoin que possui suporte embutido para anonimização através do Tor.

13. Artigos

Anonbib - Lista de trabalhos importantes no campo do anonimato. É também um conjunto de scripts para gerar o site a partir do Latex (bibtex). Se estiver faltando algum documento importante, por favor nos avise!

Conectando-se a um serviço Onion autenticado - Procedimento guiado escrito para leigos descrevendo como configurar um cliente Tor para se conectar a serviços Onion autenticados.

Dimensionamento de serviços ocultos do Tor - Artigo sobre dimensionamento do serviço Onion

XVI

O que esperar da Dark Web?

Não há uma resposta para essa pergunta, porque a dark web é um lugar com conteúdos diversificados, sendo uns bons e outros nem tanto. Porém, queremos dar uma ideia dos temas que você pode encontrar lá.

Além do conteúdo ilegal que é frequentemente associado à dark web, também é possível encontrar:

- Fóruns sobre diferentes tópicos (drogas, armas, hacking etc)
- Marketplaces para compra e venda de bens (incluindo itens ilícitos)
- Redes de mídia social ocultas
- Wikis que listam vários links .onion para explorar mais
- Blogs e artigos sobre diversos assuntos

Uma coisa a lembrar é que os serviços ocultos do Tor são como sites, eles vêm em todas as formas e tamanhos com níveis variados de segurança. Por isso, é importante que você tome cuidado antes de acessar qualquer site e esteja sempre atento aos riscos potenciais envolvidos. Além disso, como mencionado anteriormente, os sites onion às vezes podem ter versões móveis, então você deve tentar trocar de dispositivo se sua conexão estiver lenta.

Um ótimo conselho para estar na dark web é não se envolver com conteúdos ilegais. A dark web é uma rede oculta de sites criptografados que só podem ser acessados através do uso de software especial. Algumas organizações criminosas usam isso para se comunicar.

As mercadorias vendidas, também estão sob vigilância de agências de aplicação da lei que podem acabar marcando compradores desavisados nesses sites. Portanto, feche a guia e não gaste mais tempo do que o necessário nos sites desonestos.

XVII

Pensamentos finais

A dark web é um lugar assustador, mas existem maneiras de visitá-la com segurança e encontrar coisas legais. Neste livro, discutimos o que é a dark web e como você pode acessá-la de forma segura, para que sua experiência seja a mais divertida e gratificante possível. Então vá em frente, explore esses cantos do ciberespaço, onde nem todo mundo foi antes lembre-se de ficar seguro e se divertir!

XVIII

Aviso

Como na surface web ainda existem **sites maliciosos** na Dark Web existe mais ainda, coloque sua conta em risco ao acessar os sites e lembre-se sempre de usar o Tor browser para navegar, VPN e seguir todos os itens de segurança citados neste livro.

XIX

Hidden Links

Como na surface web ainda existem muitos **sites maliciosos,** na Dark Web existe o dobro, coloque sua conta em risco ao acessar os sites e lembre-se de usar o Tor browser para navegar, uma VPN e seguir todas as dicas de segurança citadas neste livro.

Vale lembrar que, o maior objetivo deste livro é tratar sobre anonimato e como funciona a Dark Web. Os sites wiki com diversos links, no geral vão demonstrar alguns temas que não apoiamos nesse livro, então, fica a critério do usuário navegar por estes tópicos ou não, mas claro, lembrando que ***a navegacão não é crime***, contudo o consumo de qualquer tipo de pornografia infantil e

também compra e venda de drogas e demais temas ilegais citados como proibidos no nosso pais, são crimes e sofrem as mais diversas penalidades já atribuidas na lei.

Caso algum site esteja indexado no wiki com muitos links, sempre lembre-se de pensar antes de navegar por aquele site, pois, a maioria traz o link com uma informação relevante sobre o que se trata o site ao lado.

Se você possui mais de **18 anos**, siga para os sites abaixo, se não, recomendo não fazer isso. Existem sites bem legais, mas como qualquer lugar cheio anonimato vamos encontrar coisas bizarras também.

Observação importante: se encontrar algum marketplace na dark web desconfie!!! A grande maioria apenas vai querer te roubar. E, se caso algum site não funcionar, possivelmente foi tirado do ar e mudou de link, isso acontece muito na Dark Web.

http://donionsixbjtiohce24abfgsffo2l4tk26qx464zylumgejukfq2vead.onion/onions.php **- Ferramenta para encontrar dominios**

https://blackhost7pws76u6vohksdahnm6adf7riukgcmahrwt43wv2drvyxid.onion/ **- BlackHost blog de technology and security**

http://lpiyu33yusoalp5kh3f4hak2so2sjjvjw5ykyvu2dulzosgvuffq6sad.onion/ **- Technology education**

https://duckduckgogg42xjoc72x3sjasowoarfbgcmvfimaftt6twagswzczad.onion/ **- DuckDuckGo**

https://dark.fail/ **- Muitos sites da Dark Web**

http://juhanurmihxlp77nkq76byazcldy2hlmovfu2epvl5ankdibsot4csyd.onion/ **- Ahmia**

http://spore64i5sofqlfz5gq2ju4msgzojjwifls7rok2cti624zyq3fcelad.onion/ **- Host para sites na dark web**

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/?_fb_noscript=1 **- Facebook**

https://twitter3e4tixl4xyajtrzo62zg5vztmjuricljdp2c5kshju4avyoid.onion/ **- Twitter**

http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion/ **Daniel é um excelente recurso para ajudá-lo a explorar diferentes links ocultos da web e no navegador Tor em geral. O site Daniel lista 7.000 onion links.**

http://fhostingineiwjg6cppciac2bemu42nwsupvvisihnczinok362qfrqd.onion/ **- Hospedagem gratuita anônima com suporte PHP/MySQL**

http://jamie3vkiwibfiwucd6vxijskbhpjdyajmzeor4mc4i7yopvpo4p7cyd.onion/ - Jamie Web

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/ - Dread Forum

https://www.4chan.org/ - 4chan Forum

https://www.nulled.to/ - Nulled Forum

https://xss.is/ - Forum Russo

http://bcloudwenjxgcxjh6uheyt72a5isimzgg4kv5u74jb2s22y3hzpwh6id.onion/ - Black Cloud - Image upload

http://strongerw2ise74v3duebgsvug4mehyhlpa7f6kfwnas7zofs3kov7yd.onion/ - Pastebin simples

http://uoxqi4lrfqztugili7zzgygibs4xstehf5hohtkpyqcoyryweypzkwid.onion/ - Image Hosting

http://dic5v3rpphxnlvtudevxnodwz3hlr2xulddymfzehknju4s66qxpsrid.onion/ - Image upload

http://xh6liiypqffzwnu5734ucwps37tn2g6npthvugz3gdoqpikujju525yd.onion/ - Respostas Ocultas (br)

http://anonyradixhkgh5myfrkarggfnmdzzhhcgoy2v66uf7sml27to5n2tid.onion/ - Deep Web Radio

http://lgmtjgfpqk6hpik7yygkhavqivn6wsmfa7s7vszmcxwqkpwodinbhnad.onion/ - No Tone

http://lkqx6qn7whctpdjhcoohpoyi6ahtrveuii7kq2m647ssvo5skqp7ioad.onion/ - Um divertido jogo online de preenchimento automático do Google

https://27m3p2uv7igmj6kvd4ql3cct5h3sdwrsajovkkndeufumzyfhlfev4qd.onion/ - Jornal The Intercept

http://xjfbpuj56rdazx4iolylxplbvyft2onuerjeimlcqwaihp3s6r4xebqd.onion/ - S-Config Blog de tecnologia

http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion DanWin's Email - Free tor email provider

http://f2vfjp3jc37gxgn4hum4uf2bhi2w3kp4jbzdwegrn6bvtezbhminobid.onion/ - Notícias e análises sobre imigração e demografia nos Estados Unidos da América, 'A voz da imigração da América'.

https://www.thedarkweblinks.com/ - Diversos sites da Dark Web

http://bvten5svsltfpxrxl72ukqxixwo2m5ek5svmcxgrmkta4tbmiemuibid.onion/ - Explorando os túneis de vapor da Virginia Tech e além.

https://darkwebwiki.org/ - Muitos sites da Dark Web

http://ovgl57qc3a5abwqgdhdtssvmydr6f6mjz6ey23thwy63pmbxqmi45iid.onion/ - Flash Light Deep Web News

http://digdeep4orxw6psc33yxa2dgmuycj74zi6334xhxjlgppw6odvkzkiad.onion/ - Conselhos de segurança.

http://cgjzkysxa4ru5rhrtr6rafckhexbisbtxwg2fg743cjumioysmirhdad.onion/ - A Privacy and Cybersecurity Blog.

http://p53lf57qovyuvwsc6xnrppyply3vtqm7l6pcobkmyqsiofyeznfu5uqd.onion/ - Investigative Journalism and News.

http://kx5thpx2olielkihfyo4jgjqfb7zx7wxr3sd4xzt26ochei4m6f7tayd.onion/ - Imperial Book - Livros Gratis

http://libraryfyuybp7oyidyya3ah5xvwgyx6weauoini7zyz555litmmumad.onion/ - Another Library

https://www.bbcnewsd73hkzno2ini43t4gblxvycyac5aw4gnv7t2rccijh7745uqd.onion/ - BBC Jornal

https://protonmailrmez3lotccipshtkleegetolb73fuirgj7r4o4vfu7ozyd.onion/ - Proton Mail

http://qubesosfasa4zl44o4tws22di6kepyzfeqv3tg4e3ztknltfxqrymdad.onion/ - Qube OS - Sistema operacional privado e seguro

http://ncidetfs7banpz2d7vpndev5somwoki5vwdpfty2k7javniujekit6ad.onion/ - The Northern California Illicit Digital Economy (NCIDE) Task Force

http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/index.html - CIA Central Intelligence Agency

http://www.dds6qkxpwdeubwucdiaord2xgbbeyds25rbsgr73tbfpqpt4a6vjwsyd.onion/ - The most watertight privacy operating system in the world.

http://blkhatjxlrvc5aevqzz5t6kxldayog6jlx5h7glnu44euzongl4fh5ad.onion/ - Black Hat Chat

http://4usoivrpy52lmc4mgn2h34cmfiltslesthr56yttv2pxudd3dapqciyd.onion/ - 8chan community forum

http://eux4gt4qcaiesps5w5rppxcenoe5shapwycums5yuiikmc4mpc74gpyd.onion/ - AnonGTS Forum

http://suprbaydvdcaynfo4dgdzgxb4zuso7rftlil5yg5kqjefnw4wq4ulcad.onion/ - Pirate Bay Forum

http://nehdddktmhvqklsnkjqcbpmb63htee2iznpcbs5tgzctipxykpj6yrid.onion/ - Monero

http://ylmjp76zk4ndvgpncbtgzrfsrzpblvlzgtuoduqgygwdlexou64iwfqd.onion/?ref=guanxi - Mega Tor Chat

http://crqkllx7afomrokwx6f2sjcnl2do2i3i77hjjb4eqetlgq3cths3o6ad.onion/ - Mega Files TOR

http://4drjmo7z2dld4mci2limogypdibxxpg7dad6g2snnrdufw6lcradc2qd.onion/ - Paradise Chat Bot

http://xp44cagis447k3lpb4wwhcqukix6cgqokbuys24vmxmbzmaq2gjvc2yd.onion/ - The Gardian Jornal

http://g7ejphhubv5idbbu3hb3wawrs5adw7tkx7yjabnf65xtzztgg4hcsqqd.onion/ - DefCon

http://danielas3rtn54uwmofdo3x2bsdifr47huasnmbgqzfrec5ubupvtpid.onion/ - Daniela um conglomerado de sites onion

http://xde6utx5ljbhrjbkkufzkuubexbyftyxrxrh74cqjky3x547gjygy3qd.onion/ - Coin Master

http://kevsec74wbstoa5l7sezjsiyzi4gouvyn32wjso5a27ndmmfmwntj4yd.onion/ - Kevin Sec

http://darkhuo35yiohrsdlbdhhrtl5ds7jtv5x2cjusqqebalj5vtrdqgqoid.onion/ - Dark Tools

http://2mqeepkwhpadzjd6o3iktot4loebjzmbffbvkuq3huiunay7co7vorad.onion/ - Umbrella Escrow

http://lzogc3coyafxtfir3u6w7cms6t3zgyldgvwtw7lmq6e5pdfy5vqu57id.onion/vendors/king-of-money-transfers/ - King of Money

http://crqkllx7afomrokwx6f2sjcnl2do2i3i77hjjb4eqetlgq3cths3o6ad.onion/ - Mega Tor

http://sdolvtfhatvsysc6l34d65ymdwxcujausv7k5jk4cy5ttzhjoi6fzvyd.onion/ - Secure Drop

http://pvhwsb7a3d2oq73xtr3pzvmrruvswyqgkyahcb7dmbbfftr4qtsmvjid.onion/ - Onion Scanner

https://torgateway.com/ - Tor2Web: Tor Hidden Services Gateway

https://pgpsuite.com/ - A simple and easy-to-use client-side PGP tool

https://calyxinstitute.org/ -

https://www.lettersanonymous.com/ - Letters Anonymous

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion/ - Forum Dread

https://oniontv.org/ - Video Search Engine

https://majestictfvnfjgo5hqvmuzynak4kjl5tjs3j5zdabawe6n2aaebldad.onion/welcome - Majestic Bank

http://nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion/ - Comic Book Library

http://notbumpz34bgbz4yfdigxvd6vzwtxc3zpt5imukgl6bvip2nikdmdaad.onion/ - Chat

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/?_fb_noscript=1 - Facebook

http://hzwjmjimhr7bdmfv2doll4upibt5ojjmpo3pbp5ctwcg37n3hyk7qzid.onion/ - Ablative.Hosting

http://asapmsp2nsqiyufpnw5bziguahdpxbpyc6jbiss35wgca6ka434w27ad.onion/ - ASAPMail

http://qubesosfasa4zl44o4tws22di6kepyzfeqv3tg4e3ztknltfxqrymdad.onion/ - Qubes OS

http://ovgl57qc3a5abwqgdhdtssvmydr6f6mjz6ey23thwy63pmbxqmi45iid.onion/ - Flash Light Info Dark Web

http://lzogc3coyafxtfir3u6w7cms6t3zgyldgvwtw7lmq6e5pdfy5vqu57id.onion/ - DeepSy

http://zqktlwiuavvvqqt4ybvgvi7tyo4hjl5xgfuvpdf6otjiycgwqbym2qad.onion/wiki/Main_Page - The Hidden Wiki

http://63jhzz5w3flwbcstmt6grrgmm2qembekcj4yugyyktlxnispcfw7guyd.onion/ - Team Premium

http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion/ - DarkNetlive

http://duckwm3krjkdpb7wbkgbra5bu7ilwr2wj5zjp6pym7clfprumwdluhid.onion/ - Duck Duck Go Wiki

http://uquroyobsaquslaunwkz6bmc3wutpzvwe7mv62xeq64645a57bugnsyd.onion/ - Tor Wiki

http://wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion/ - Hidden Links

http://torbotzotnpygayi724oewxnynjp4pwumgmpiy3hljwuou3enxiyq3qd.onion/ - Tor Bot

http://ucapoywa7wsbzlf5umrrdi2otooa5napma3r5s5ojysts46l5bic4gid.onion/ Freedom Forum

http://k5aintllrufq23khjnmmfli6uxioboe3ylcao7k72mk2bgvwqb5ek4ad.onion/ - TruthBoard

http://hgzqgqunlejgxruvcthlpk3pywgkci3kkubhnvlv2rgveusz3n6qarad.onion/ - Onion Links

http://22tojepqmpah32fkeuurutki7o5bmb45uhmgzdg4l2tk34fkdafgt7id.onion/ - Tasty Onion

http://wclekwrf2aclunlmuikf2bopusjfv66jlhwtgbiycy5nw524r6ngioid.onion/ - Hidden Links

http://darkhuo35yiohrsdlbdhhrtl5ds7jtv5x2cjusqqebalj5vtrdqgqoid.onion/ - Dark Tools

http://btcw3wabdz3zmt7f6k37k7km5ll6gom2kwf5hxpzd7djuqrhsdhtodqd.onion/ - Bitcoin

http://torlinkv7cft5zhegrokjrxj2st4hcimgidaxdmcmdpcrnwfxrr2zxqd.onion/ - Tor Links

http://asapmsp2nsqiyufpnw5bziguahdpxbpyc6jbiss35wgca6ka434w27ad.onion/ - ASAP Mail

http://no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad.onion/ - Submarine

http://hsquad7ikj4ejivl7e52rdfcvtgpqueqzu27wq273noeoi27y6kglxad.onion/ - Hack_Squad

http://pwndb2am4tzkvold.onion/ - pwndb

http://guardday6e5nxblpojbhmx5ws2avautr7eswu3qg7gynh52rh744anyd.onion/ - DarkGuard

http://dreadytofatroptsdj6io7l3xptbet6onoyno2yv7jicoxknyazubrad.onion Forum dread - Reddit for the darknet

http://enxx3byspwsdo446jujc52ucy2pf5urdbhqw3kbsfhlfjwmbpj5smdad.onion Forum EndChan - 4chan-style discussion board

http://ow5svfag54s2txymiwgl6do6dvgddbcxjrdraykox26pkwdwbpkhnfqd.onion/index.php?forums/main-forum.2/ - Xen Forum

http://bestteermb42clir6ux7xm76d4jjodh3fpahjqgbddbmfrgp4skg2wqd.onion/ - Best Carding World Forum

http://mlyusr6htlxsyc7t2f4z53wdxh3win7q3qpxcrbam6jf3dmua7tnzuyd.onion Kilos - Search engine and a bunch of other stuff

http://torbox36ijlcevujx7mjb4oiusvwgvmue7jfn2cvutwa6kl6to3uyqad.onion/ - TORBOX

http://secmail63sex4dfw6h2nsrbmfz2z6alwxe4e3adtkpd4pcvkhht4jdad.onion/src/login.php - secMail - Darknet email

http://oq7t5ihk4qew5t5s4zghicigokh2ktt575amirsbnilmyawpme6xmyyd.onion/ - Elude

http://darkzzx4avcsuofgfez5zq75cqc4mprjvfqywo45dfcaxrwqg6qrlfid.onion/ - Darknetlive

https://protonirockerxow.onion/ - Protonmail (Onion)

http://continewsnv5otx5kaoje7krkto2qbu3gtqef22mnr7eaxw3y6ncz3ad.onion/ - Conti-2

https://continews.best/ - Conti (Clear web)

http://fylszpcqfel7joif.onion/ - Conti-News (Ryuk)

http://ekbgzchl6x2ias37.onion/ - Clops

http://e6wzjohnxejirqa2sgridvymv2jxhrqdfuyxvoxp3xpqh7kr4kbwpwad.onion/ - Tornode

https://rtuyjoxwxxfdzhtrignwbr7acdlnu5m4gwfqvhkywmnflkajcpjwnhyd.onion/About/HeartsCenterForum/tabid/499/Default.aspx#.Ym4hj9_LdIG - Hearts Center Forum

http://no6m4wzdexe3auiupv2zwif7rm6qwxcyhslkcnzisxgeiw6pvjsgafad.onion/ - Submarine (Hidden Services)

https://bible4u2lvhacg4b3to2e2veqpwmrc2c3tjf2wuuqiz332vlwmr4xbad.onion/ - Biblia Online

http://pt.zlibrary24tuxziyiyfr7zd46ytefdqbqd2axkmxm4o5374ptpc52fad.onion/ - Z-Library

http://nv3x2jozywh63fkohn5mwp2d73vasusjixn3im3ueof52fmbjsigw6ad.onion/ - Comic Book Library

http://libraryqxxiqakubqv3dc2bend2koqsndbwox2johfywcatxie26bsad.onion/special/index - The Anarchist Library

http://te5djpo3shwwz6dgkhg6yvwc4skego6jzojo5khrs2uqsmvhbtgujnid.onion/ - Furry Comic Book

http://forums.dds6qkxpwdeubwucdiaord2xgbbeyds25rbsgr73tbfpqpt4a6vjwsyd.onion/ - Whonix Forum

http://tssa3yo5xfkcn4razcnmdhw5uxshx6zwzngwizpyf7phvea3gccrqbad.onion/public/forum/simpleforum.cgi - Arquivos secretos de historia

http://marxists3va6eopxoeiegih3iyex2zg3tmace7afbxjqlabmranzjjad.onion/archive/lenin/index.htm - Lenin Internet Arquivo

http://i45r477vjegjep6x7cqlgt7lihkzyeaqq5nzpt5spa3fgqbbg27zw6qd.onion/ - Just Another Library

http://bhf2b5nb3lb2kxpaoyqz7cuk2dkgej5n2refuffxzyhldwt4d7de4zqd.onion/ - BHF.IM

http://gdarku42fzpyrfra.onion/gdark/search.php - GDark

http://phobosxilamwcg75xt22id7aywkzol6q6rfl2flipcqoc4e4ahima5id.onion/ - Phobos

http://dnmugu4755642434.onion/search - Kilos - Darknet Market Search Engine

http://xssforumv3isucukbxhdhwz67hoa5e2voakcfkuieq4ch257vsburuid.onion/ - XSS

http://ezdhgsy2aw7zg54z6dqsutrduhl22moami5zv2zt6urr6vub7gs6wfad.onion/ - Def Con Forums

https://www.facebookwkhpilnemxj7asaniu7vnjjbiltxjqhye3mhbshg7kx5tfyd.onion/ - Facebook

http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/ - CIA

http://32ici55gwqdxhvvohwzrxyxdhw6x3t4s4g4bzczclrluewx7mhu6g7ad.onion/ - BitCoin Game

http://danschat356lctri3zavzh6fbxg2a7lo6z3etgkctzzpspewu7zdsaqd.onion/ - Daniels Chat

http://yblgsv67jnuzryt74i5xf76tzf2mf3qfcky2l6tndgjm42sj54k2s3qd.onion/ - Daniel Host

http://gerkipwhfuqeeizl.onion/ - Gerki_TOR

http://dyetjpdb24gam3siszbpoehvauunvovpeaozxgv24sqe7bkn74blw7qd.onion/ - Light Money

http://bcbm4y7yusdxthg3.onion/ - SkyFraud

http://l5b5ugkok5owt5w7xz7fvrvd75io2hvnao4c4gonidjmkqsyifwkdryd.onion/ DarkNetStreets

http://wqmfzni2nvbbpk25.onion/partners.html - Pysa

http://rnfdsgm6wb6j6su5txkekw4u4y47kp2eatvu7d6xhyn5cs4lt4pdrqqd.onion/blog - Netwalker

http://hxt254aygrsziejn.onion/ - Nefilim (Corporate Leaks)

https://mazenews.online/ - Maze-News

http://xfr3txoorcyy7tikjgj5dk3rvo3vsrpyaxnclyohkbfp3h277ap4tiad.onion/ - Maze

http://egregoranrmzapcv.onion/ - Egregor

http://hpoo4dosa3x4ognfxpqcrjwnsigvslm7kv6hvmhh2yqczaxy3j6qnwad.onion/ - Dopple Paymer

http://darksidedxcftmqa.onion/ - Darkside

http://avaddongun7rngel.onion/ - Avaddon

http://37rckgo66iydpvgpwve7b2el5q2zhjw4tv4lmyewufnpx4lhkekxkoqd.onion/ - Ako (Ranzy)

http://htcltkjqoitnez5slo7fvhiou5lbno5bwczu7il2hmfpkowwdpj3q2yd.onion/ - Conti

http://marketojbwagqnwx.onion/ - Marketo

http://cuba4mp6ximo2zlo.onion/ - Cuba

http://gtmx56k4hutn3ikv.onion/ - Babuk Locker

http://ixltdyumdlthrtgx.onion/ - Hades

http://ransomocmou6mnbquqz44ewosbkjk3o5qjsl3orawojexfook2j7esad.onion/ - Everest

http://lockbit-blog.com/ - Lockbit

http://mountnewsokhwilx.onion/ - Mount Locker

http://wj3b2wtj7u2bzup75tzhnso56bin6bnvsxcbwbfcuvzpc4vcixbywlid.onion/ - Xinof - Raas (Login Required)

http://msaoyrayohnp32tcgwcanhjouetb5k54aekgnwg7dcvtgtecpumrxpqd.onion/ - Prolock

http://nbzzb6sa6xuura2z.onion/ - Suncrypt

http://sekhmetleaks.top/ - Sekhmet

http://dnpscnbaix6nkwvystl3yxglz7nteicqrou3t75tpcc5532cztc46qyd.onion/ - Revil

http://rnsm777cdsjrsdlbs4v5qoeppu3px6sb2igmh53jzrx7ipcrbjz5b2ad.onion/ - Ransomexx (Defray777)

http://rgleaktxuey67yrgspmhvtnrqtgogur35lwdrup4d3igtbm3pupc4lyd.onion/ - **Ragnar Locker**