Universidade Federal do Estado do Rio de Janeiro

Centro de Ciências Exatas e Tecnologia

Escola de Informática Aplicada

A Rede Tor: No Limiar Entre A Desobediência Civil E A Delinquência

Daniel Ruiz Teixeira

Orientador

Sidney Cunha de Lucena

Rio de Janeiro, RJ – Brasil

Dezembro de 2016

A Rede TOR: No Limiar Entre A Desobediência Civil E A Delinquência

Daniel Ruiz Teixeira

Projeto de Graduação apresentado à Escola de Informática Aplicada da Universidade Federal do Estado do Rio de Janeiro (UNIRIO) para obtenção do título de Bacharel em Sistemas de Informação.

Aprovada por:

_____

Sidney Cunha de Lucena

Rio de Janeiro, RJ – Brasil

Dezembro de 2016

Agradecimentos

Agradeço aos meus pais, por tudo. Agradeço à minha família, por trilharem o caminho comigo. Agradeço aos meus amigos, por fazerem parte de mim. Agradeço à UNIRIO e seus mestres, por todo conhecimento adquirido. E agradeço ao meu amor, por ser a luz que me guia.

RESUMO

A Rede TOR é utilizada por milhares de pessoas ao redor do mundo não apenas para se obter uma maior privacidade em seu uso de Internet, mas especificamente para buscar o anonimato, seja para boas ou más intenções. O conjunto do uso do véu do anonimato com o advento tecnológico da Internet possibilita uma observação mais prática do comportamento humano, seja através de ferramentas de monitoração, seja através de métricas ou rastros virtuais.

A proposta deste trabalho é a descrever o funcionamento da Rede TOR e, a partir desta ótica, levantar questões e analisá-las quanto ao aspecto moral no uso desta ferramenta tecnológica que promove um maior controle da privacidade individual do usuário da Internet e até mesmo seu anonimato. Quais visões podem ser tiradas do uso criminoso da Rede TOR, quais usos legalizados a rede pode proporcionar, até onde seu uso fora da lei é válido e outras questões.

Palavras-chave: Rede TOR, privacidade, anonimato, roteamento cebola, *deep web*, *dark web*.

ABSTRACT

The TOR Network is used by thousands of people around the world not only to gain greater privacy in their use of the Internet, but also to specifically seek anonymity for either good or bad intentions. The use of the veil of anonymity with the technological advent of the Internet allows a more practical observation of human behavior, either through monitoring tools, virtual metrics or virtual traces.

The purpose of this work is to technically describe how the TOR Network works and, with this understanding, raise questions and analyze them regarding moral aspects in the use of this technological tool that promotes greater control of the individual privacy of Internet users and even their anonymity. What visions can be drawn from the criminal use of the TOR Network, what legalized uses the network can provide, to what extent its lawful use is valid, and other issues.

Keywords: TOR network, privacy, anonymity, onion routing, deep web, dark web.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABELAS

GLOSSÁRIO

1. DARPA: Defense Advanced Research Projects Agency.
2. GCHQ: Government Communications Headquarters.
3. ISP: Internet Service Provider.
4. MIT: Massachusetts Institute of Technology.
5. NSA: National Security Agency.
6. PIPA: PROTECT IP Act.
7. SOPA: Stop Online Piracy Act.
8. SSL/TLS: Secure Sockets Layer / Transport Layer Security.
9. IP: Internet Protocol.
10. FBI: Federal Bureau of Investigation.
11. TCP: Transmission Control Protocol.
12. AES: Advanced Encryption Standard.
13. SOCKS: Socket Secure.
14. SSH: Secure Shell.
15. HTTP: Hypertext Transfer Protocol.
16. HTTPS: Hypertext Transfer Protocol Secure.
17. TLD: Top Level Domain.

1. Introdução

1.1 Motivação

A Internet é hoje parte inerente no lar de um cidadão. Com ela, há a introdução de uma janela virtual dentro da casa do internauta, uma janela que não apenas traz um visual para o mundo como também pode trazer a possibilidade de que pessoas de fora observem o interior da casa de terceiros.

A privacidade está cada dia mais frágil, principalmente a virtual, já que o usuário comum não costuma se precaver para cuidar de sua segurança computacional na Internet. Com isso, cria-se uma grande abertura para que pessoas e serviços externos tenham contato com informações privadas dos usuários.

Com essa sensibilidade da privacidade no meio virtual, surgiu uma necessidade de maior proteção da identidade do usuário na rede, já que por padrão a Internet não é segura nem confiável. Inúmeras ferramentas e técnicas surgiram para suprir essa necessidade, uma delas foi a Rede TOR.

O objetivo deste trabalho não é, porém, tratar sobre o desenvolvimento da Rede TOR, mas sim questionar e refletir a respeito da privacidade na Internet a partir da ótica de funcionamento da Rede TOR. Levantar questões do uso correto ou incorreto do anonimato, do potencial revolucionário que uma rede anônima como a Rede TOR pode proporcionar e, ao mesmo tempo, do potencial destrutivo que a mesma rede pode disponibilizar.

1.2 Questionamentos

A rede TOR pode proporcionar anonimato e privacidade a um usuário e, de uso desta condição, um cidadão pode ter total liberdade para praticar crimes, realizar negociações escusas, contratar serviços ilegais etc. Por outro lado, uma outra abordagem do uso da rede seria o de lutar por causas sociais a partir de territórios dominados por censura à liberdade de expressão, também como para própria proteção contra *hackers* e até mesmo compartilhamento de material jornalístico.

A Rede TOR é, enfim, válida como uma ferramenta para canalizar e destacar uma atitude ou comportamento do ser humano que acaba sendo coibida e censurada, inibida e apequenada pela sociedade? Existe limite moral para o uso da Internet?

1.3 Organização do Trabalho

O presente trabalho está estruturado em 8 capítulos que, a partir desta introdução, estão distribuídos da seguinte forma:

O Capítulo 2 terá como assunto a fundamentação teórica, ou seja, os conceitos que serão utilizados neste trabalho para chegar ao seu objetivo final: compreender o funcionamento da Rede TOR e traçar uma análise dos efeitos práticos do anonimato e da privacidade por ela provida, assim como seu impacto na sociedade.

O Capítulo 3 tratará sobre o histórico da Rede TOR. Sua criação, desenvolvimento, popularização, expansão pelo mercado negro e, por fim, analisará

as variações de popularidade.

O Capítulo 4 fará uma breve exposição sobre o Bitcoin, uma criptomoeda virtual usada como moeda de troca para as transações na Rede TOR. Trata-se de um capítulo para fundamentar alguns conhecimentos sobre sua história, funcionamento e, também, sobre a legalidade ou ilegalidade de seu uso através dos países.

O Capítulo 5 fala, enfim, sobre o funcionamento técnico da Rede TOR, abordando endereços .onion, nós e pontes

O Capítulo 6 analista a questão da moralidade no uso da Rede e traz estatísticas quanto ao uso do TOR quanto a legalidade e/ou moralidade..

O Capítulo 7 descreve uma experiência prática com o uso da Rede TOR. Inicialmente com uma demonstração dos endereços .onion – endereços exclusivos para uso através da Rede Onion – seguida por buscas tanto por conteúdo de desobediência civil e delinquência. Posteriormente, explica-se como se dá a criação de um endereço .onion.

O Capítulo 8 trará reflexões sob o aspecto social do TOR e, também, reflexões sobre a moralidade na Rede. Questionará sobre o anonimato na sociedade, o combate à censura e a validade da ferramenta no que tange a desobediência civil. O oitavo capítulo volta às questões abertas na Introdução e ao longo do documento.

O Capítulo 9 traz a conclusão do trabalho com as considerações finais.

2. Fundamentação Teórica

Este capítulo aborda algumas explicações acerca de tecnologias envolvidas na Rede TOR e no contexto geral tratado no texto, essenciais para a compreensão do trabalho.

2.1. Proxy

Um *proxy* é uma unidade computacional que atua como um portão de entrada/saída ou *gateway* entre duas redes, normalmente entre uma rede local e a Internet. Funciona interceptando conexões entre remetente e receptor, e vice-versa, onde todos os dados trafegados entram através de uma porta e são encaminhados para a rede de destino através de outra.

Alguns servidores *proxy* são grupos de aplicativos ou servidores que bloqueiam serviços comuns na Internet. Por exemplo, um proxy HTTP intercepta o acesso à Internet e um proxy SMTP intercepta tráfego de e-mails.

Um servidor *proxy* usa um endereçamento de rede para apresentar um endereço IP de toda a organização para a Internet. O servidor encaminha todas as solicitações de usuários para a Internet e retorna respostas aos usuários específicos. Além de restringir o acesso externo, esse mecanismo pode impedir que usuários internos acessem recursos específicos da Internet.

A Rede TOR funciona como uma espécie de *proxy*, encaminhando todo o tráfego de dados através de um circuito virtual constituído por nós da rede TOR até o destino final da mensagem, circuito este que a própria aplicação no computador de

origem define na hora da transmissão das mensagens.

2.2. DNS

O Domain Name System (ou Sistema de Nomes de Domínio) é um sistema de banco de dados, hierárquico e distribuído pela Internet, que converte o nome de domínio de uma unidade computacional em um endereço de IP.

Computadores em rede usam endereços IP para localizar e conectar uns aos outros, mas os endereços IP podem ser complexos e difíceis de memorizar, no que tange à comunicação entre usuários. O DNS permite que o usuário se conecte a outro computador usando seu nome de domínio, tornando o processo mais transparente e simples.

A Rede TOR utiliza o serviço de DNS para disponibilizar acesso a *websites* da Surface Web (Internet comum, “visível” a todos) para os usuários. Já na Dark Web (porção da Internet “escondida” pela Rede TOR), com seus endereços .onion, os DNS não são necessários, já que o próprio TOR indexa e mantém gravada a lista de endereços onion ativos em sua rede.

2.3. Criptografia

Criptografia é a transformação de dados em uma forma ilegível para qualquer pessoa que não tenha a chave de criptografia. Seu propósito é o de assegurar a privacidade, ao fazer com que as informações criptografadas se mantenham incompreensíveis para qualquer pessoa, ou sistema, que não seja o seu destino

intencional.

A criptografia da Rede TOR funciona através de camadas. A ferramenta, ao enviar uma mensagem e após escolher o caminho de seu circuito virtual, encripta a mensagem em camadas, como se fossem “cascas de uma cebola”. A cada etapa do trajeto, ao passar por um nó da Rede TOR (TOR Relay), a mensagem encriptada terá uma camada “descascada”, ou seja, descriptografada, revelando assim o próximo TOR relay que conduzirá a mensagem pelo circuito até seu destino final.

2.4. Criptografia por Chave Pública

Existem dois tipos de criptografia: a simétrica e a assimétrica. Na criptografia simétrica, uma mesma chave criptográfica é usada para criptografar uma mensagem e descriptografá-la. Já na criptografia assimétrica, uma chave é usada para criptografar e outra, gerada em conjunto com a primeira, é usada para descriptografar.

Na criptografia por chave pública, duas chaves são geradas para cada extremidade (elemento que deseja se comunicar) da rede: uma pública e uma privada. Como os próprios nomes sugerem, a chave pública é de conhecimento público e a chave privada é de conhecimento apenas daquele elemento da rede. A forma de geração deste par de chaves permite que, ao se criptografar uma mensagem com uma chave, seja possível descriptografá-la com a outra, qualquer que seja a ordem. O processo de envio de mensagens com privacidade se inicia com o transmissor usando a chave pública do receptor para criptografar a mensagem, que por sua vez será descriptografada pelo receptor com sua chave privada.

Vale ressaltar que esta forma de criptografia e descriptografia usando chaves públicas e privadas é bastante custosa em termos de tempo e processamento, sendo evitada para dados muito extensos. Geralmente, nestes casos, usa-se a criptografia por chaves públicas para o envio sigiloso de uma chave simétrica que será usada na criptografia do conteúdo.

Na Rede TOR, cada *relay* no circuito virtual possui sua chave pública e, consequentemente, sua chave privada. Elas são usadas para negociar uma chave simétrica entre o nó de origem e cada nó *relay* do circuito de modo que, através desta chave, seja possível "descascar" uma camada específica de encriptação e nada mais, dando continuidade à transmissão da mensagem pelo circuito. Apenas o destino final da mensagem terá a chave criptográfica necessária para desencriptar a mensagem por completo.

3. Histórico da Rede TOR

Neste capítulo serão mostrados parágrafos acerca do trajeto da Rede TOR na história, desde sua criação até os dias atuais, com análises sobre a popularização da ferramenta.

3.1. Criação e Origens Militares

O conceito inicial de roteamento cebola foi criado em 1995 pelo Office of Naval Research (Escritório de Pesquisa Naval) dos EUA, com a intenção de proteger a comunicação militar. Posteriormente, em 1997, seu desenvolvimento passou a ser patrocinado pela DARPA (Defense Advanced Research Projects Agency), também dos Estados Unidos.

Em 1999 o desenvolvimento do roteamento cebola é suspenso por falta de investimentos, apesar de sua pesquisa e análise continuar. Já em 2001 seu desenvolvimento é retomado, novamente patrocinado pela DARPA.

Em 2002 o desenvolvimento do roteamento cebola, pelo menos sua primeira versão, foi finalmente abandonado por estar obsoleto. Começa então o desenvolvimento do código da geração 2 do roteamento cebola, ou seja, o TOR. O código original foi inicialmente produzido por Matej Pfajfar, da Universidade de Cambridge, para seu projeto de graduação – porém é bom salientar que, em meados de 2004, já não constava nenhuma parte do código original na base de códigos do TOR.

Ainda em 2002, em setembro, a versão alfa do TOR foi desenvolvida pelos

cientistas computacionais Syverson, Dingledine e Mathewson. No ano seguinte, em 2003, é realizado o primeiro *release* público sob uma licença livre e gratuita do MIT (Massachusetts Institute of Technology) [DINGLEDINE, 2004].

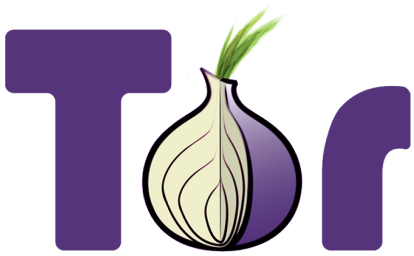

Figura 1 – Logomarca do TOR Project Fonte: torproject.org

Em 2006 foi fundado o The Tor Project, uma organização sem fins lucrativos orientada para pesquisa e educação responsável pela manutenção do TOR. A Figura 1 traz a logomarca deste projeto.

É interessante notar que todo o desenvolvimento da tecnologia foi patrocinada por órgãos militares norte-americanos. É curioso também observar que os próprios militares americanos alteraram o rumo do desenvolvimento da tecnologia, trazendo o TOR para os olhos civis e disponibilizando-o para a sociedade geral.

Uma explicação simples para o motivo desse rumo tomado é que a comunicação só é tão segura e anônima quanto a relevância do tamanho da rede que compõe a Rede TOR.

3.2. Popularidade

Uma breve análise da popularidade pode ser feita a partir de um gráfico gerado pelo site de métricas do próprio projeto TOR, como mostrado na Figura 2. Porém, a própria organização mantenedora do projeto não dispõe de explicações das variações da popularidade do serviço, cabendo na sua observação apenas conjecturas sobre os períodos.

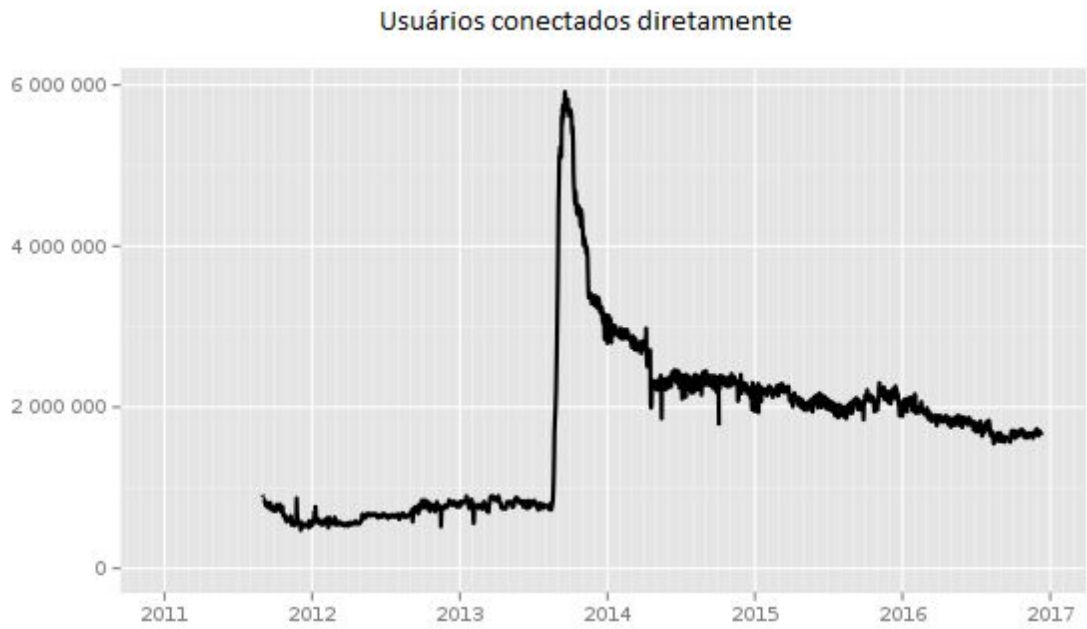

Figura 2 – Métricas de acesso entre 2011 e 2016. Fonte: metrics.torproject.org

Pode-se notar, na Figura 2, dois eventos interessantes ao longo dos anos. Em 2013 houve tanto um aumento impressionante do uso da Rede quanto uma queda drástica neste uso. Uma possível explicação para o aumento súbito seria as revelações de Edward Snowden sobre GCHQ, coletando dados de usuários de Internet na Inglaterra. Também pode ser relacionado à preocupação americana da espionagem realizada pela NSA, uma agência governamental. Também pode-se supôr que seja reflexo da lei anti-pirataria russa recém-criada, similar às americanas

SOPA e PIPA. Ou, por fim, pode ser relacionado a um novo *browser* provido pelo site agregador de *torrents* ThePirateBay. Talvez pode ter sido todos os motivos juntos, não há dados conclusivos a respeito desse evento.

Já a queda no gráfico é relativamente mais difícil de se conjecturar. Não houve nenhum tipo de ataque à Rede TOR na época, tampouco revelações de vulnerabilidade. A opinião mais difundida é a de que, na época em questão, a pouca velocidade da Rede TOR, somada à reduzida oferta de *sites* e serviços disponíveis para o público comum, tenham afastado a maioria dos usuários que haviam inicialmente fugido para este arcabouço em busca de privacidade.

4. O Bitcoin

Este capítulo expõe informações a respeito do Bitcoin, uma popular moeda criptográfica usada internacionalmente e principalmente na Deep Web (porção da Internet não indexada pelos mecanismos de busca), já que ela é originalmente não-rastreável, o que a torna perfeita para o uso anônimo na Rede TOR, por exemplo [NOVAES, 2014].

4.1. Histórico

Figura 3 – Logomarca do Bitcoin. Fonte: forum.bitcoin.org

O Bitcoin foi criado por Satoshi Nakamoto, em 2008, em forma de um trabalho disponibilizado em uma lista de e-mail denominado “Bitcoin: A Peer-to-Peer Eletronic Cash System” (Bitcoin: um sistema de dinheiro eletrônico peer-to-peer). Foi implementado e distribuído em 2009 sob um código *open source*. O Bitcoin foi a primeira moeda digital descentralizada. A Figura 3 traz a logomarca do Bitcoin.

Em 2012 foi criada a Bitcoin Foundation, organização estadunidense sem fins lucrativos criada com o objetivo de padronizar, proteger e promover o uso de Bitcoins. Seus membros originais foram Gavin Andresen, Charlie Shrem, Mark Karpeles, Peter Vessenes, Roger Ver e Patrick Murck.

Um ponto curioso a se observar é que o criador, Satoshi Nakamoto, nunca foi reconhecido. Não se sabe se é uma única pessoa ou um grupo de pessoas. Atualmente ele – ou eles – encontra-se ausente do cenário virtual e de Bitcoins.

4.2. Popularidade

O Bitcoin sempre esteve em uma crescente de popularidade, desde sua criação. Mesmo tendo passado por períodos em que sua imagem foi afetada, como quando o FBI invadiu empresas que acumulavam Bitcoins de clientes, ou quando *sites* da Dark Web (porção da Deep Web acessível apenas por mecanismos como os disponibilizados pela Rede TOR) foram desbaratados e, então, verificados que seu principal meio de comercialização era através de Bitcoins. É simples de se observar a popularidade dos Bitcoins através de gráficos ao longo dos anos, conforme mostrado na Figura 4.

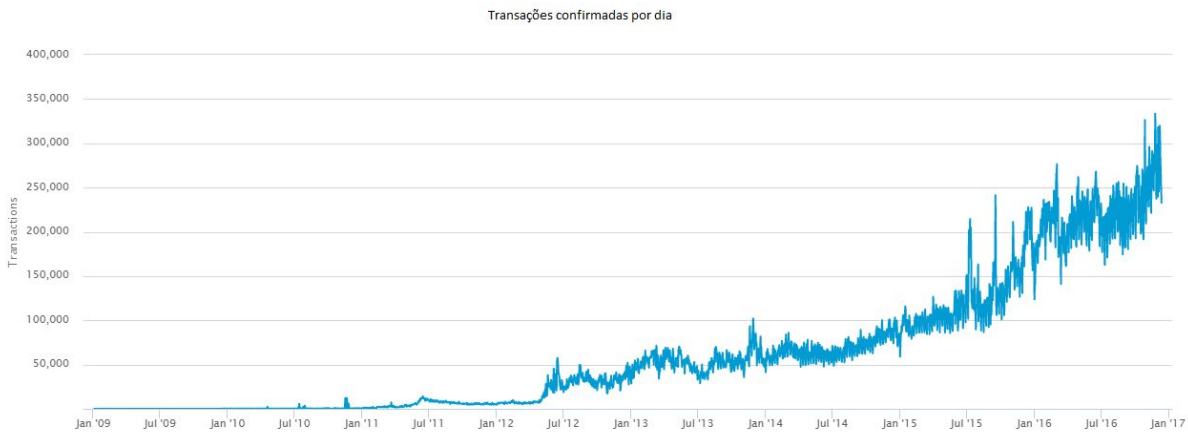

Figura 4 – Transações confirmadas por dia, desde 2009. Fonte: blockchain.info

Na Figura 4, pode-se notar que o número de transações usando Bitcoins tem

aumentado de forma aparentemente exponencial. É fácil compreender este aumento ao notar que, hoje em dia, grandes empresas aceitam Bitcoins como forma de pagamento. Desde lojas físicas de bairro até gigantes como Paypal.

4.3. Funcionamento

Bitcoin é, em essência, um controle de transações de moedas virtuais. Esse controle acontece através de um registro virtual que é mantido, compartilhado e conhecido por todos que estão envolvidos com Bitcoin. Este registro virtual se dá num banco de dados distribuído chamado *Blockchain* que é sincronizado através de todos os clientes *online* de Bitcoin, fazendo com que o registro seja conhecido por todos os usuários. Todas as transações confirmadas são lá registradas e têm, como garantia de integridade e de cronologia, uma proteção feita por criptografia.

Cada transação é executada entre um usuário de origem do dinheiro virtual e um de destino. Apesar da transação ser feita entre dois usuários, todos da rede têm conhecimento da transação e de seus detalhes. Esses detalhes são as contas de origem, de destino e a assinatura da transação, assinatura essa realizada através de criptografia usando as chaves privadas dos dois usuários envolvidos na transação, o que confere garantia de autenticidade de cada ponta. Para estimular a manutenção das transações no *Blockchain*, usuários voluntários – chamados mineradores – recebem pequenas quantidades de Bitcoin como recompensa. Esta recompensa se dá conforme a execução dos cálculos matemáticos responsáveis pela criptografia que mantém a proteção de atualização e gerenciamento do *Blockchain*, tornando a participação nas minerações algo lucrativo. Estes cálculos são computacionalmente intensos, o que leva muitos usuários a investirem nos componentes de seus computadores para aumentar a capacidade de processamento e, assim, poderem minerar mais Bitcoins.

Apesar das Bitcoins serem moedas virtuais, há vários órgãos e empresas que oferecem serviços de compra e venda da moeda, um câmbio entre virtual e físico.

4.4. Bitcoin e a Rede TOR

A relevância de Bitcoins com a Rede TOR se dá pelo fato de ambos terem um forte apelo no anonimato. Grande parte das transações ocorridas na Deep Web são através de Bitcoins, já que a origem e o destino do dinheiro não são rastreáveis, o que retira a possibilidade de uma vulnerabilidade em uma transação anônima.

5. Funcionamento da Rede TOR

Este capítulo retrata o funcionamento da Rede TOR, uma visão técnica dos mecanismos que fazem o roteamento *onion* e a Rede TOR ser o que é. As informações contidas neste capítulo são, em sua maioria, livres traduções das informações obtidas em [DINGLEDINE, 2015].

5.1. Explicação Técnica

5.1.1. Em Resumo

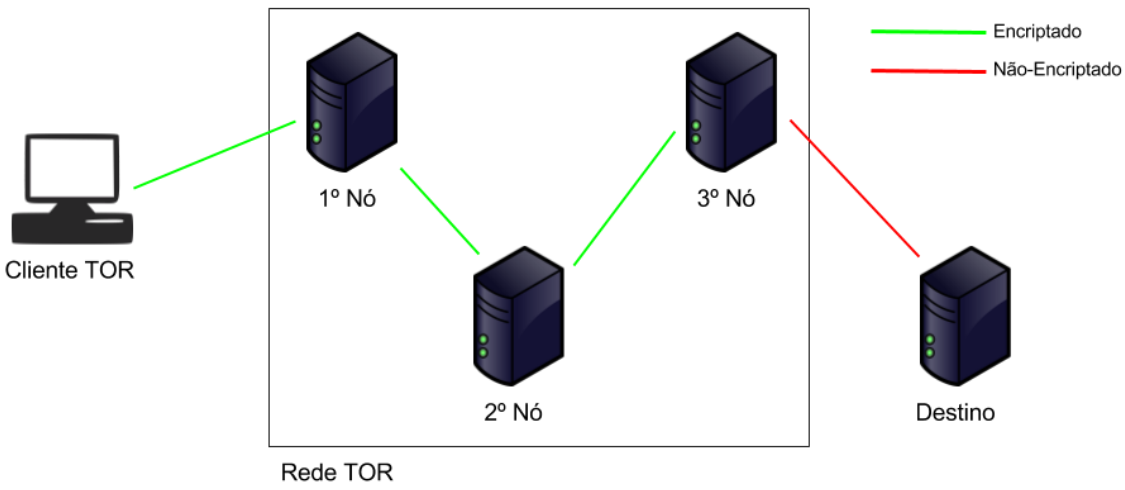

Figura 5 – A Rede TOR - Visão Básica dos Nós

Temos na Figura 5 uma ilustração simples de como funciona a Rede TOR. O cliente TOR instalado no computador do usuário estabelece um caminho virtual até um dado destino – chamado de circuito virtual. Este circuito é gerado aleatoriamente a partir de uma lista de nós conhecidos e usa, por padrão, sempre três nós: o de entrada, o de *relay* e o de saída. No exemplo, três nós já conhecidos e indexados -

dentre as dezenas de milhares de nós já existentes - são selecionados e encadeados para compor o circuito virtual entre o cliente TOR e seu destino final. Este caminho (circuito) será percorrido pelas mensagens enviadas pelo cliente TOR para o destino final, onde tanto o conteúdo da mensagem como também os endereços de origem e destino são encriptados. Além disso, o cliente TOR adiciona às mensagens as respectivas chaves criptográficas que serão usadas ao longo do caminho. A cada nó que a mensagem percorre, uma camada de criptografia é descascada, revelando o próximo nó do circuito a ser percorrido. Ao chegar no último nó, o destino final da mensagem é revelado e, enfim, a mensagem é entregue [JANSEN, 2008].

A Figura 6 ilustra as camadas de criptografia “cebola” do roteamento *onion*:

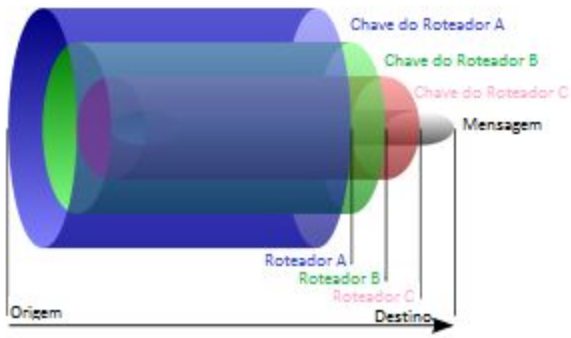

Figura 6 – Roteamento cebola. Fonte: wikipedia.org

5.1.2. O Design

TOR é uma rede distribuída de sobreposição projetada para anonimizar aplicações baseadas em TCP, como a navegação na *web*, *shells* e mensagens instantâneas. Os clientes escolhem um caminho através da rede e determinam um circuito virtual no qual cada nó (ou ‘onion router’, ou ‘OR’) no caminho conhece

apenas o seu antecessor e sucessor, mas não conhece nenhum outro nó do circuito. O tráfego de dados segue pelo circuito e, a cada nó, uma camada de criptografia é descascada através de uma chave simétrica – como camadas de cebola – seguindo em frente para continuar o processo de descamação até o destino final. Cada roteador cebola, na verdade, trata-se de um processo normal sendo executado no nível de usuário, muitas vezes em um computador comum, sem qualquer privilégio. Do ponto de vista desta comunicação entre ORs, assim como entre o cliente TOR e o primeiro OR, ou como no último salto até o destino, a arquitetura corresponde ao de uma rede peer-to-peer usando criptografia. Portanto, cada roteador mantém uma conexão TLS a qualquer outro roteador da Rede TOR.

Cada usuário executa um *software* local chamado ‘onion proxy’ (OP) para buscar diretórios, estabelecer os circuitos pela rede e lidar com conexões de aplicações de usuários. Esses OPs aceitam fluxos TCP e os multiplexam através dos circuitos. O roteador cebola do outro lado conecta-se então ao próximo “salto” requerido e transmite os dados.

Cada roteador cebola mantém uma chave de identidade de longo prazo e uma chave de cebola de curto prazo. A chave de identidade é usada para assinar certificados TLS. A chave de cebola é usada para decifrar solicitações de usuários para configurar um circuito e negociar chaves efêmeras. O protocolo TLS também estabelece uma chave de curto prazo para quando há comunicação entre os roteadores cebola, chave essa que é rotacionada periodicamente e de forma independente, com o objetivo de limitar o impacto em caso de comprometimento de chaves.

5.1.3. Comunicação entre Nós

Os roteadores cebola comunicam-se uns com os outros, e também com os OPs, através de conexões TLS com chaves efêmeras. Usando TLS, esconde-se os dados com sigilo e se impede que um invasor modifique esses dados ao longo do seu trajeto físico, se passando por um roteador cebola. O tráfego que passa por essas conexões é formado por células (pacotes de dados) de tamanho fixo. Cada célula tem 512 bytes e consiste em um cabeçalho e sua carga (*payload*). O cabeçalho inclui um identificador de circuito (circID), que especifica a qual circuito a célula pertence (muitos circuitos podem ser multiplexados sobre uma única conexão TLS), e um *comando* para descrever o que fazer com a carga da célula. Os identificadores de circuito são específicos para cada conexão, ou seja, cada circuito tem um circID para cada conexão OP/OR (entre *onion proxy* e *onion router*) ou OR/OR que ele atravessa. Com base no seu *comando*, as células podem ser consideradas como células de controle, que são sempre interpretadas pelo nó que as recebem, ou células de distribuição, que carregam parte do fluxo de dados entre origem e destino. As células de controle podem ter as seguintes funções: preenchimento – normalmente usadas como *keepalive* (indicando que o circuito deve permanecer ativo); criação – usadas para configurar um novo circuito; e destruição – usadas para derrubar um circuito. As células de distribuição têm um cabeçalho adicional em frente à carga contendo um streamID (identificador de fluxo, já que vários fluxos podem ser multiplexados em um circuito), um *checksum* de fim a fim para verificação de integridade, o comprimento da carga de distribuição e um comando de distribuição. O conteúdo completo do cabeçalho e da célula de carga de distribuição é encriptado e decriptado junto a medida que a célula atravessa os nós do circuito, usando o algoritmo de criptografia de chave simétrica AES, com chave criptográfica de 128 bits.

Na Figura 7 há a demonstração de uma célula de tamanho fixo utilizada como

unidade de comunicação na Rede TOR.

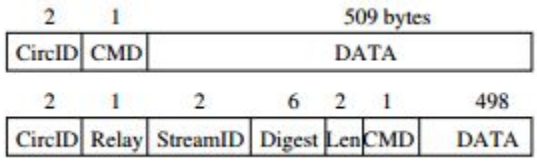

Figura 7 – Célula de tamanho fixo. Fonte: Tor: The Second-Generation Onion Router (2004) de Dingledine, Roger ; Mathewson, Nick ; Syverson, Paul

5.1.4. Circuitos e Fluxos

No TOR, cada circuito pode ser compartilhado por muitos fluxos TCP. Para evitar atrasos, os usuários constroem circuitos de forma preventiva. Os OPs dos usuários criam um novo circuito periodicamente se o anterior já estiver sendo usado assim como derrubam um circuito antigo que já tenha expirado, para o qual não exista mais nenhum fluxo aberto. Como circuitos são criados previamente em “plano de fundo”, os OPs podem se recuperar da criação de circuitos falhados sem prejudicar a experiência do usuário.

5.1.5. Construindo um Circuito

O Onion Proxy (OP) de um usuário constrói cada circuito de forma incremental, negociando uma chave simétrica diferente para cada OR ao longo do circuito, um salto por vez. Para começar a criar um circuito, o OP envia uma célula com comando de criação de circuito para o primeiro nó do caminho escolhido. A partir desta célula de criação, OP e OR negociam uma chave simétrica entre eles. Em seguida, para estender o circuito ao próximo OR do caminho virtual, o OP envia

para o primeiro OR uma célula com o comando *relay extend*, especificando o endereço deste próximo OR (segundo OR). O primeiro OR e o segundo OR criam então um circID entre eles, permitindo estender o circuito do OP até este segundo OR. A partir desta extensão, o OP e o segundo OR negociam então uma chave simétrica entre eles, conforme previsto no roteamento em cebola. Este procedimento é então repetido para cada salto ao longo do circuito virtual, até se chegar ao destino.

Assim que o circuito é estabelecido, tem-se um cenário em que o OP possui um conjunto de chaves simétricas compartilhadas com cada nó ao longo do circuito virtual, permitindo-se então o envio de células de distribuição. Assim que recebe uma célula de distribuição, o OR busca o circuito correspondente e desencripta o cabeçalho de distribuição e sua carga com a respectiva chave para aquele circuito.

5.1.6. Abrindo e Fechando Sessões entre Nós Finais

Quando uma aplicação de um usuário quer abrir uma conexão TCP para um determinado endereço e porta na Rede TOR, ela pede ao OP para fazer a conexão com este destino final na respectiva porta. O OP escolhe o mais novo circuito aberto – ou cria um se necessário – a partir da seleção de um OR adequado para ser o nó de saída daquele circuito para este destino final, ou seja, o último OR do circuito. O OP então pede abertura de sessão enviando uma célula com o comando *relay begin* para o OR de saída, usando um novo e aleatório streamID. O OR de saída então solicita abertura de sessão com o destino final e, uma vez confirmada, o OR de saída responde para o OP com uma célula de *relay connected*. Após recebimento desta célula, o OP notifica a aplicação do sucesso no estabelecimento da sessão com a aplicação no destino final. O OP passa então a aceitar dados do fluxo TCP da aplicação, empacotando-os em células de distribuição de dados e as enviando através do circuito para o OR de saída escolhido.

Há um detalhe que deve ser apontado: algumas aplicações passam o *hostname* alfanumérico para o cliente TOR, enquanto outras o resolvem em um endereço IP primeiro, para depois passar o endereço IP para o cliente TOR. Se a aplicação faz resolução DNS primeiro, o usuário então revela seu destino através da Rede TOR. Algumas aplicações populares como Mozilla e SSH possuem essa falha [JANSEN, 2012] [LOESING,2008].

5.2. Ocultação da Identidade

As figuras 8, 9, 10 e 11 e suas respectivas análises tratam a respeito da diferença do uso de tecnologias no caminho entre origem e destino de uma mensagem através da Internet, apontando quem é capaz de espionar os dados trafegados e em quais momentos [EFF, 2012].

5.2.1. Acesso à Internet sem Proteção:

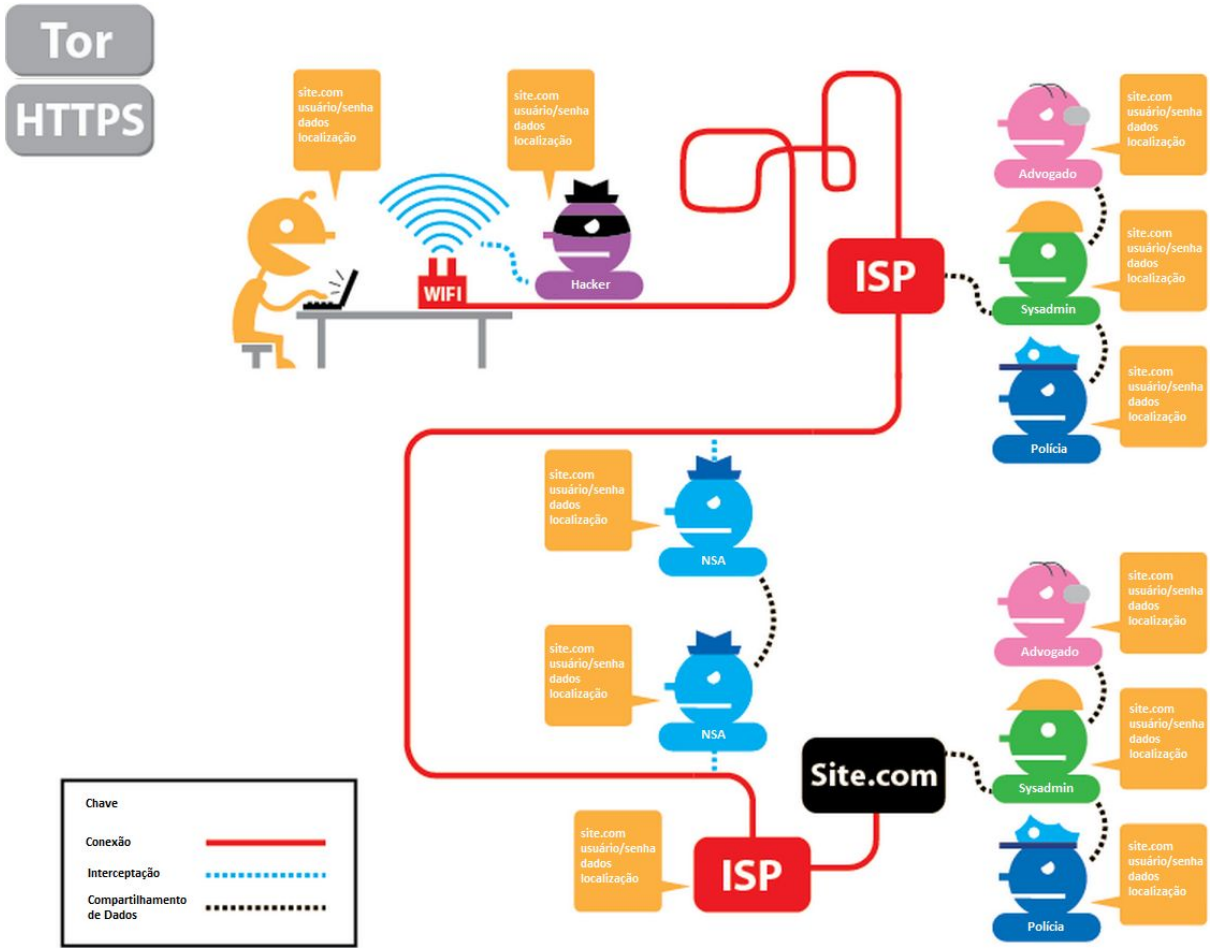

Figura 8 – Sem HTTPS e sem TOR. Fonte: eff.org

A Figura 8 demonstra que, sem proteção, todos os pontos entre o usuário e o site final estão desprotegidos. Todas as informações são visíveis, sem restrições.

5.2.2. Acesso à Internet com uso de HTTPS:

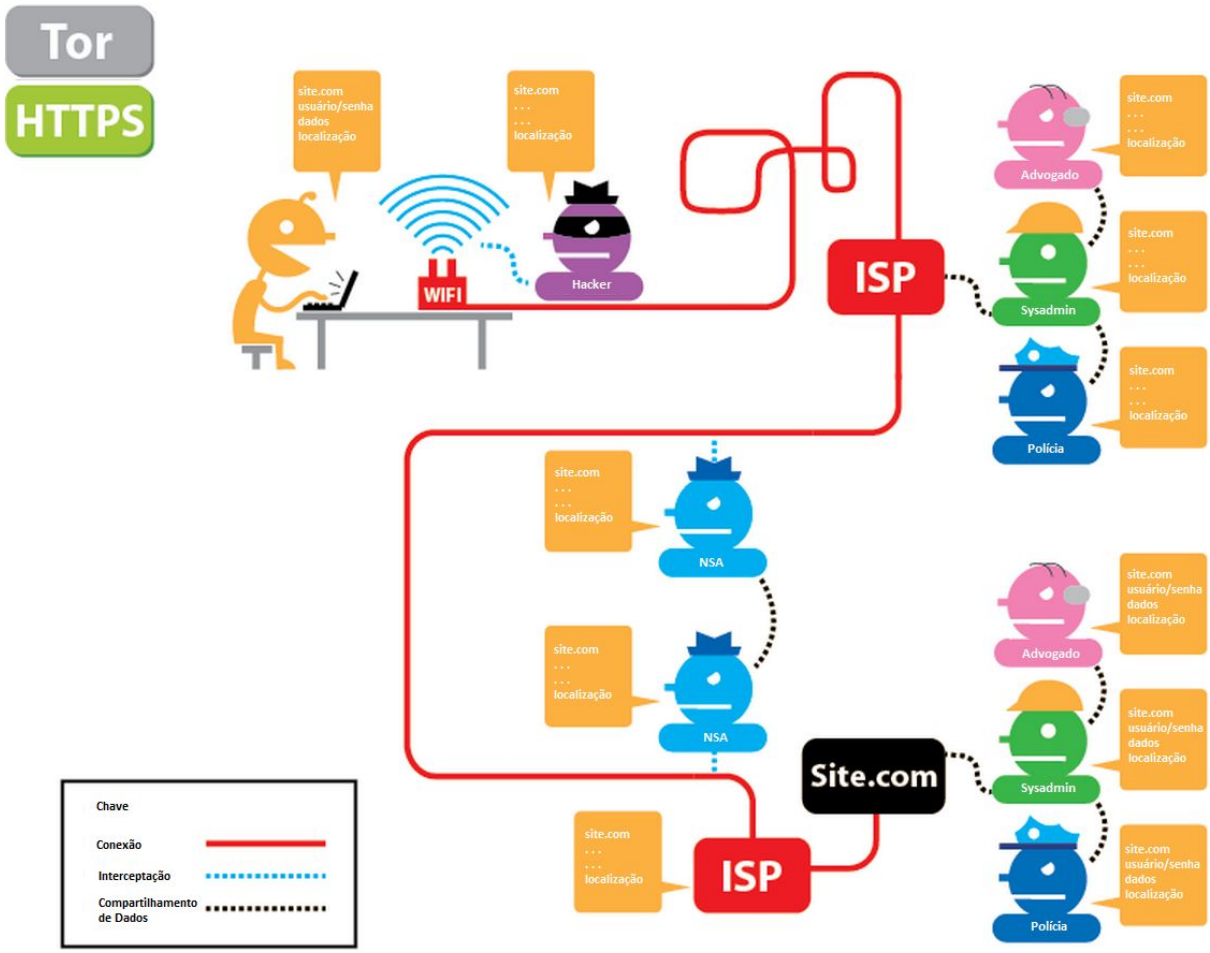

Figura 9 – Com HTTPS e sem TOR. Fonte: eff.org

A Figura 9 demonstra que, com o uso de uma primeira camada de segurança, o HTTPS, algumas informações ficam ocultas por boa parte do trajeto. As credenciais e os dados em si são ocultos para todos, exceto para os que se encontram na última milha.

5.2.3. Acesso à Internet com o uso do TOR

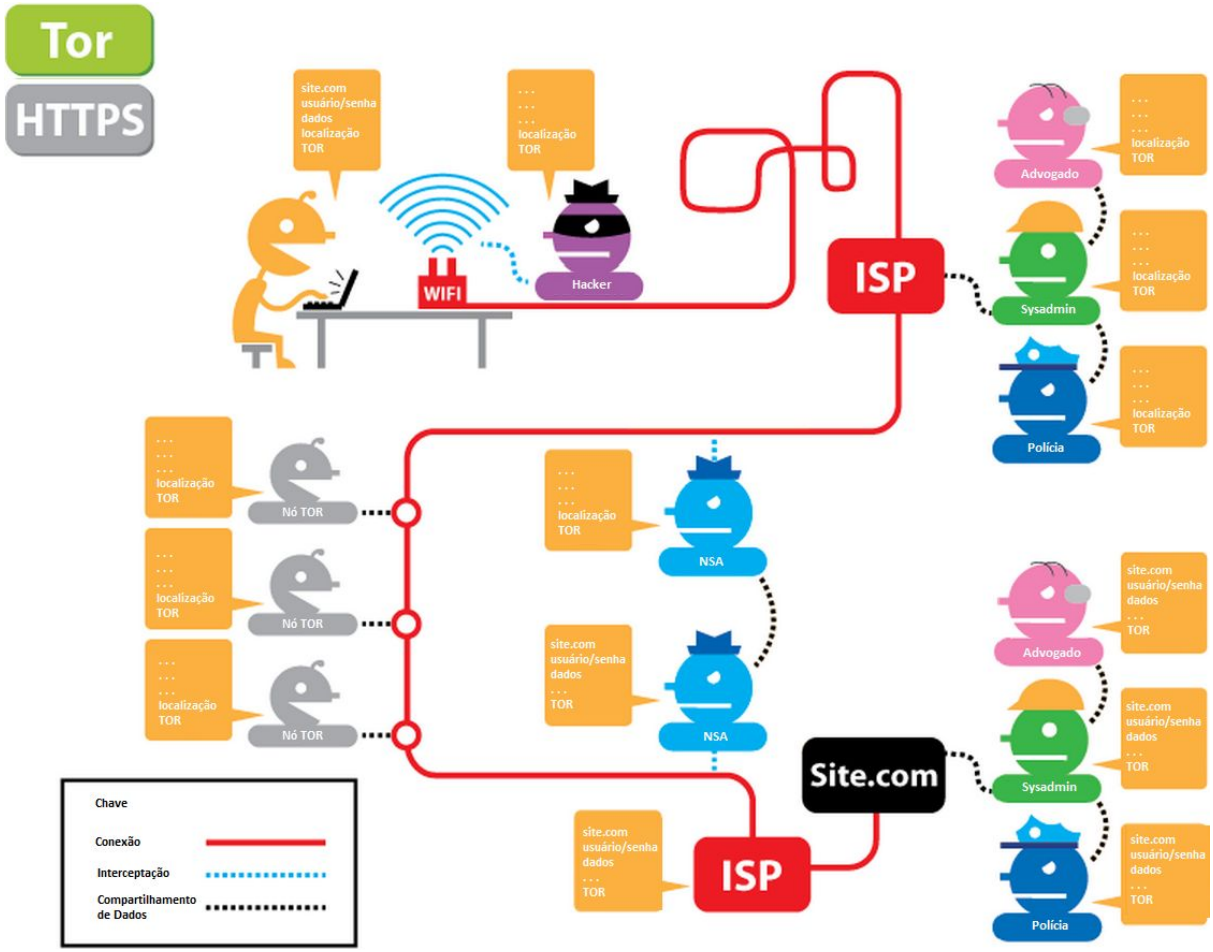

Figura 10 – Sem HTTPS e com TOR. Fonte: eff.org

A Figura 10 demonstra que com apenas o uso da Rede TOR o usuário tem parte de seus dados ocultos – especificamente as credenciais e dados – por quase todo o trajeto, exceto na última milha e após o último nó TOR.

5.2.4. Acesso à Internet com o uso do TOR e HTTPS

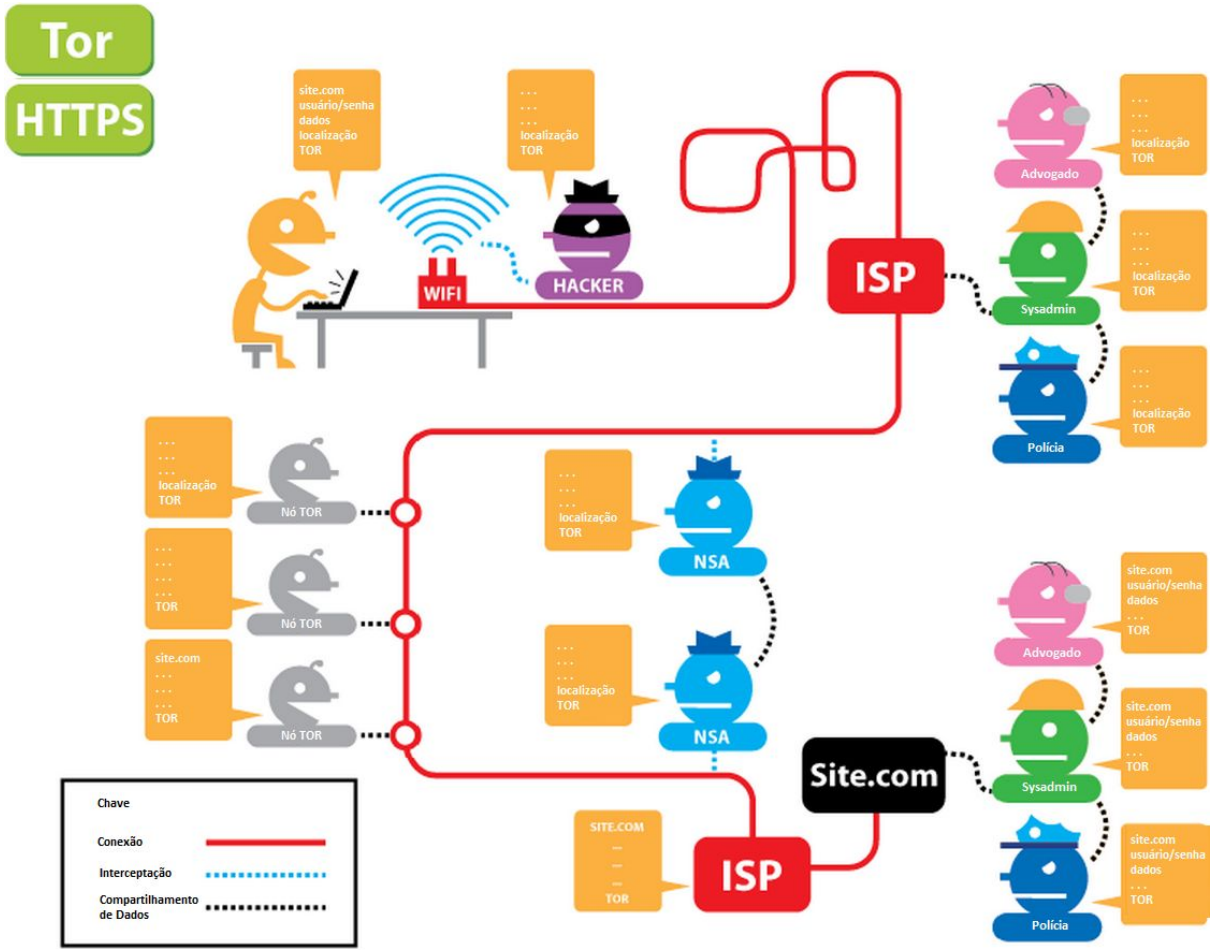

Figura 11 – Com HTTPS e com TOR. Fonte: eff.org

Por fim, a Figura 11 demonstra o uso conjunto de TOR e HTTPS, que oculta praticamente todos os dados por todo o trajeto. Inclusive na última milha, a localização do usuário é oculta.

5.3. Bridges / Pontes

Além dos nós comuns, os conhecidos *relays*, existe na Rede TOR o que se chama de ponte ou *bridge*. Pontes nada mais são do que nós que ainda não foram indexados no diretório principal do TOR. A vantagem disso é que, caso um ISP de algum país resolva bloquear todos os endereços conhecidos de relays TOR, as pontes têm grande chance de não serem bloqueadas, já que não se encontram listadas.

Podemos observar na Figura 12 o crescimento tanto de nós quanto de pontes ao longo dos anos.

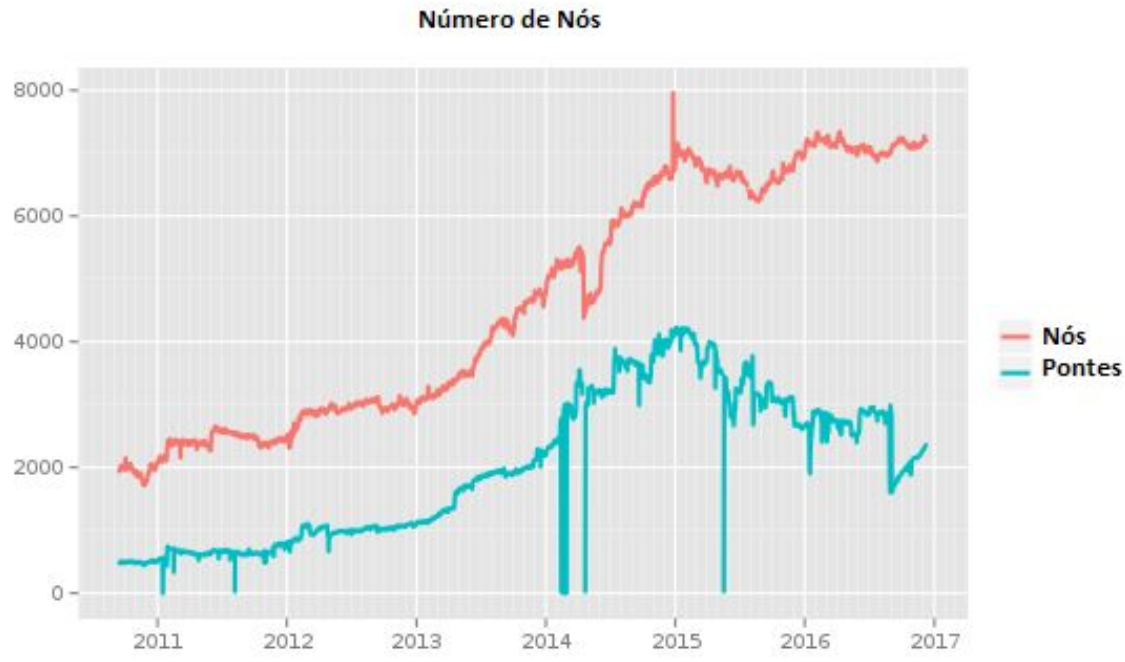

Figura 12 – Nós e Pontes ao longo dos anos. Fonte: metrics.torproject.org

5.4. Endereços .onion

O .onion é um sufixo de domínio de nível de topo no DNS, sendo de uso especial e que designa um serviço acessível apenas através da Rede TOR. Esses endereços não são nomes DNS reais e o TLD (Top Level Domain) .onion não está na raiz DNS da Internet. Porém, com o Onion Proxy – parte inerente do TOR – o acesso à resolução de nomes abaixo do TLD .onion é possível.

Como são criados dentro da própria Rede TOR e utilizando as mesmas tecnologias de criptografia para buscar o anonimato, os endereços .onion possuem maior segurança de identidade. A Figura 13 mostra a expansão dos endereços .onion nos últimos dois anos.

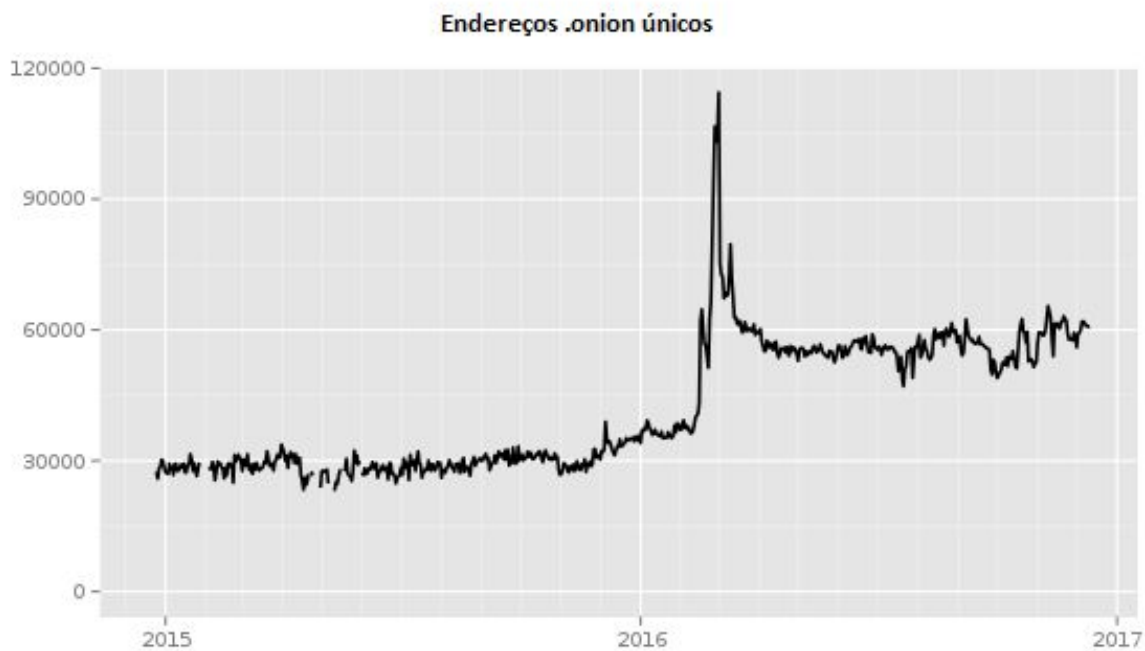

Figura 13 – Endereços .onion únicos. Fonte: metrics.torproject.org

6. O Anonimato e a Moralidade na Rede

Este capítulo apresenta diferentes conceitos e estatísticas relacionadas ao tipo de uso da Rede TOR. O uso moral e imoral em relação ao anonimato e a dificuldade de se obter dados confiáveis a respeito das finalidades do uso da Rede.

6.1. Surface Web, Deep Web e Dark Web

É essencial fazer a diferenciação dos termos que são tão citados quando se trata da Rede TOR. A começar pela *Surface Web*, que nada mais é que a Internet normal, onde qualquer usuário pode acessar digitando seu endereço em seu navegador. É composta por *websites* que são indexados por serviços de busca, não necessita de nenhum tipo de técnica ou procedimento especial para serem acessados.

Em seguida temos a *Deep Web*, que é a parte da Internet que não é indexada mas ainda assim é acessível se o usuário tiver conhecimento da sua forma de acesso. *Sites* de banco, internamente, são assim, por exemplo

Por último temos a *Dark Web*, que além de não ser indexada só é acessível de formas especiais, seja por meio de *software* específico ou algum tipo de credencial de segurança que limita o acesso. Os sites .onion são exemplo desse tipo de *Web*. Na Figura 14 há uma demonstração visual das diferentes camadas.

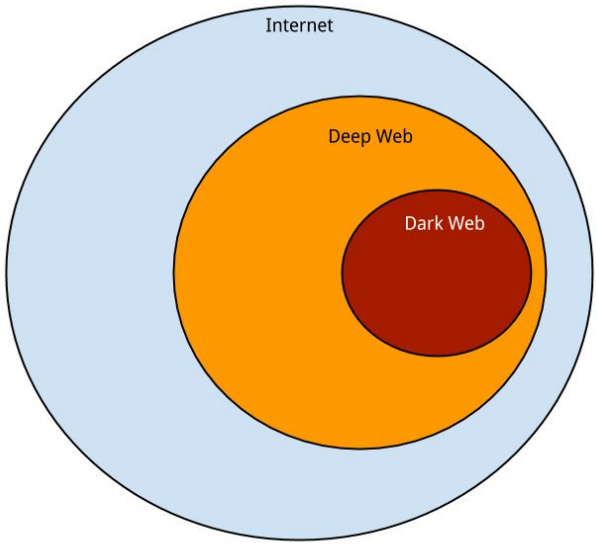

Figura 14 – Surface, Deep e Dark Web. Fonte: danielmiessler.com

6.2. Moralidade na Rede TOR

Quanto à legalidade do anonimato na Rede TOR, há de se observar a legislação local do usuário. No caso do Brasil, a Constituição de 1988 dita que a manifestação do pensamento é livre, porém o anonimato é vedado. Já nos Estados Unidos, a Primeira Emenda garante o direito ao anonimato para seus cidadãos. Mas, e quanto à moralidade do anonimato?

O conceito de moralidade também é subjetivo. As culturas individuais dos países a definem para suas próprias realidades. Portanto, a forma mais universal de se analisar a moralidade do anonimato seria através do posicionamento de órgãos internacionais e neutros. A seção de direitos humanos das Nações Unidas se posiciona a favor do anonimato e da criptografia de dados pois, através destes, o indivíduo pode exercer seu direito de liberdade de opinião e expressão na era digital e, dessa forma, tal direito merece proteção.

Este é, portanto, o julgamento mais universal e neutro que temos em nosso mundo globalizado, no momento. É o posicionamento que grande parte dos países tende a seguir, em concordância com as Nações Unidas [KAYE, 2015].

6.3. Dados sobre o Uso do Anonimato na Rede TOR

Mesmo com o advento do anonimato, pode-se notar que o uso da navegação pela Internet através da Rede TOR não implica em uma mudança drástica do comportamento do usuário. Pelo contrário, só demonstra um comportamento comum, sem tendências surpreendentes para a criminalidade ou imoralidade. Conforme [CHAABANE, 2010], mais de 65% dos *sites* acessados se agrupam em 10 categorias que podem ser vistas na Tabela 1.

Categoria	Porcentagem de Acessos
Mecanismos de Busca/Portais	14,45
Pornografia	11,50
Computadores/Internet	11,45
Redes Sociais	9,52
Blogs/Comunicação Web	2,26
Streaming de Mídia/MP3	1,82
Downloads de Software	1,66
Hacking	0,3
Política	0,18
Ilegal/Questionável	0,15
Ilegal/Drogas	0,06

Tabela 1: Estatística de Uso de Navegação na Rede TOR

Já na Tabela 2, pode-se ver um TOP 10 de países que acessam a Rede TOR

utilizando pontes, ou seja, que evitam o uso dos nós já conhecidos pela Rede e se utilizam das pontes para o uso mais incomum possível de sua rota, de maneira que possam evitar qualquer tipo de rastreamento [TOR Metrics, 2017].

País	Média de Usuários por Dia
Emirados Árabes Unidos	25655 (33,30%)
Estados Unidos da América	7011 (9,10%)
Russia	7011 (9,10%)
Turquia	4281 (5,56%)
Brasil	2657 (3,45%)
Irã	2615 (3,39%)
Reino Unido	2185 (2,84%)
Belarus	2116 (2,75%)
Alemanha	2090 (2,71%)
India	1583 (2,05%)

Tabela 2 - TOP 10 Países por Conexões por Ponte entre 12/2016 e 03/2017

A Tabela 2 [TOR Metrics, 2017] mostra uma mistura de países que possuem algum tipo de censura e outros que não. Pelos percentuais mostrados, verifica-se que a maior parte dos usuários são provenientes de países sem censura, levando-se a crer que a maioria dos usuários acessam a Rede TOR através de pontes apenas com o intuito de blindar suas identidades, sem o objetivo conjunto de se esquivar de censuras e bloqueios.

7. Hands on com a Rede TOR

Este capítulo tem a intenção de demonstrar o contato com a Rede TOR na prática. Realizações de acesso, instalações e demonstração de como criar um website .onion

7.1. Instalação e Utilização Inicial do TOR Bundle

O TOR Bundle é o conjunto de instalações recomendado pelo TOR Project para o usuário comum iniciar seu acesso e uso na Rede TOR. Para instalá-lo, basta ir até seu *website* principal em torporject.org e baixá-lo para a versão certa do Sistema Operacional do usuário. A instalação em si é simples e rápida, não demandando nenhum conhecimento especial do usuário.

7.1.1. Baixando o TOR Bundle

Para baixar o TOR Bundle para o computador, basta acessar o endereço do *website* www.torproject.org e selecionar o botão de *download*, que pode ser visto na Figura 15.

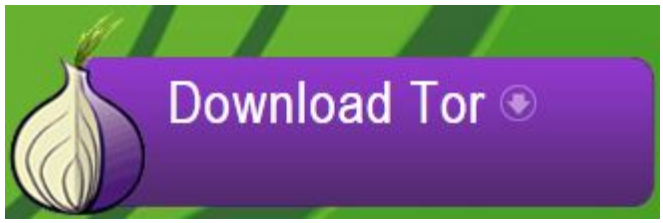

Figura 15 – Primeiro botão de *download* do TOR Bundle. Fonte: torproject.org

Na página seguinte, surge um novo botão de *download* e algumas opções para o sistema operacional e idioma do usuário e de seu computador. Ao selecionar as opções em questão, se assim desejar, prossegue-se para o botão de *download*, visto na Figura 16, para, enfim, baixar o aplicativo TOR Bundle.

Figura 16 – Segundo botão de *download* do TOR Bundle e opções de download. Fonte: torproject.org

Enfim o TOR Bundle está no computador do usuário, pronto para sua instalação. Seu executável tem uma representação gráfica através do ícone da Figura 17.

Figura 17 – Ícone do aplicativo de instalação do TOR Bundle

7.1.2. Instalação do TOR Bundle

Inicialmente o instalador demonstra as opções de idiomas de instalação, seguido de uma tela requisitando o caminho para a instalação. A finalização da instalação provê opção de inserir ícones na área de trabalho e de executar o TOR Browser imediatamente após o fechamento da janela da instalação. A Figura 18 demonstra os ícones criados automaticamente após a instalação bem-sucedida.

Figura 18 – Atalho e pasta criados após a instalação

7.1.3. Configuração do TOR

Ao iniciar o TOR pela primeira vez o usuário é questionado se o uso vai ser tradicional ou se a Internet é censurada, o que poderá requerer a configuração de um *proxy* ou o uso de *bridges* para o acesso.

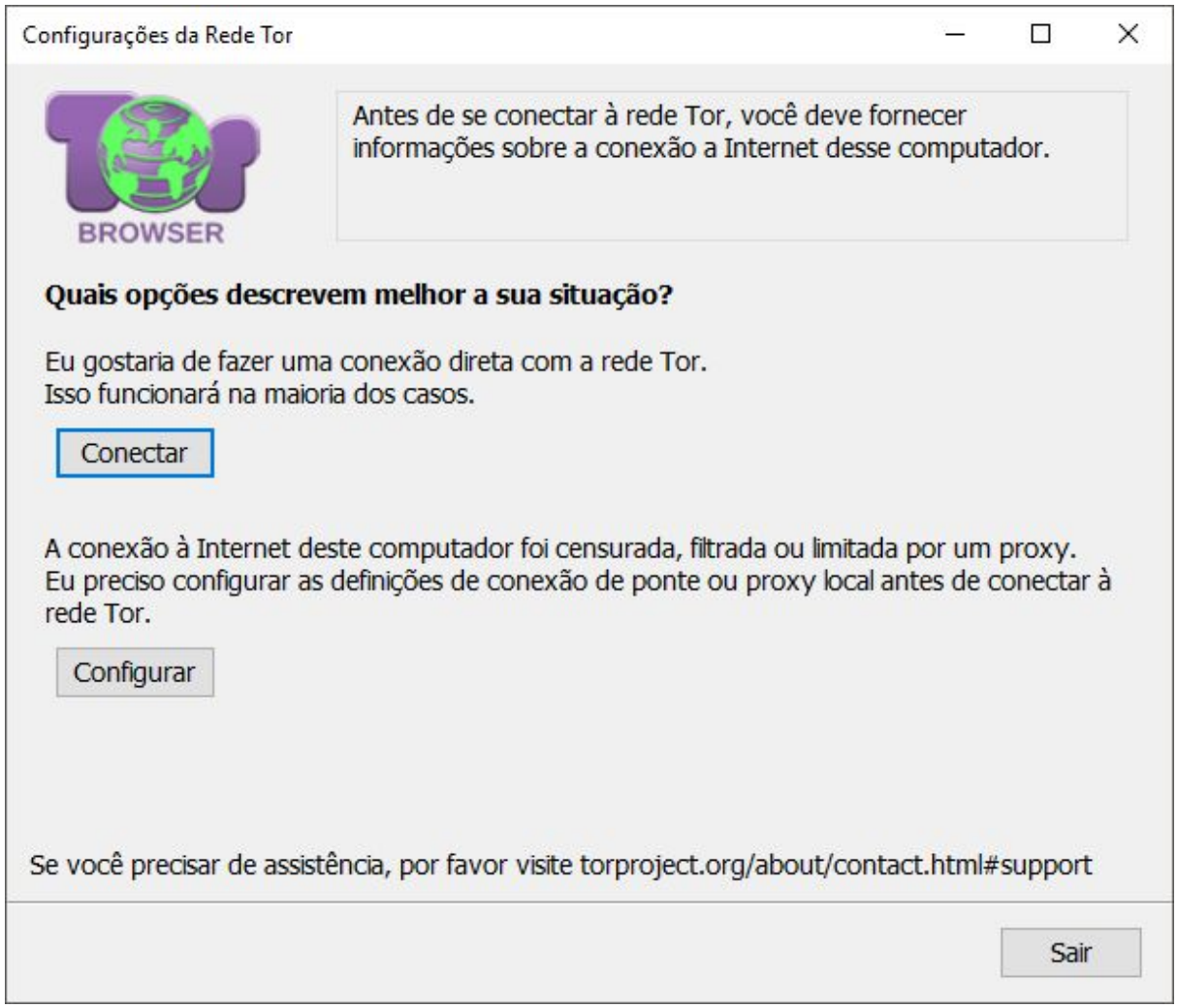

Figura 19 – Primeira tela de configuração do TOR

Ao selecionar a primeira opção – ‘Conectar’ – que pode ser vista na Figura 19, a rede TOR é iniciada normalmente, criando um circuito virtual padrão. Este circuito utiliza três nós aleatoriamente escolhidos para funcionarem como nó de entrada, nó *relay* e nó de saída. Qualquer tráfego originado pela aplicação, para qualquer destino, passará por este circuito. O que mudará será apenas o caminho tomado a partir do nó de saída até o destino final da mensagem.

Ao selecionar a segunda opção – ‘Configurar’ – também vista na Figura 19, o TOR questiona se o provedor de Internet (ISP) bloqueia ou censura o acesso do

usuário a redes TOR. Em caso positivo, a próxima tela, que pode ser vista representada na Figura 20, é para a configuração de pontes (*bridges*).

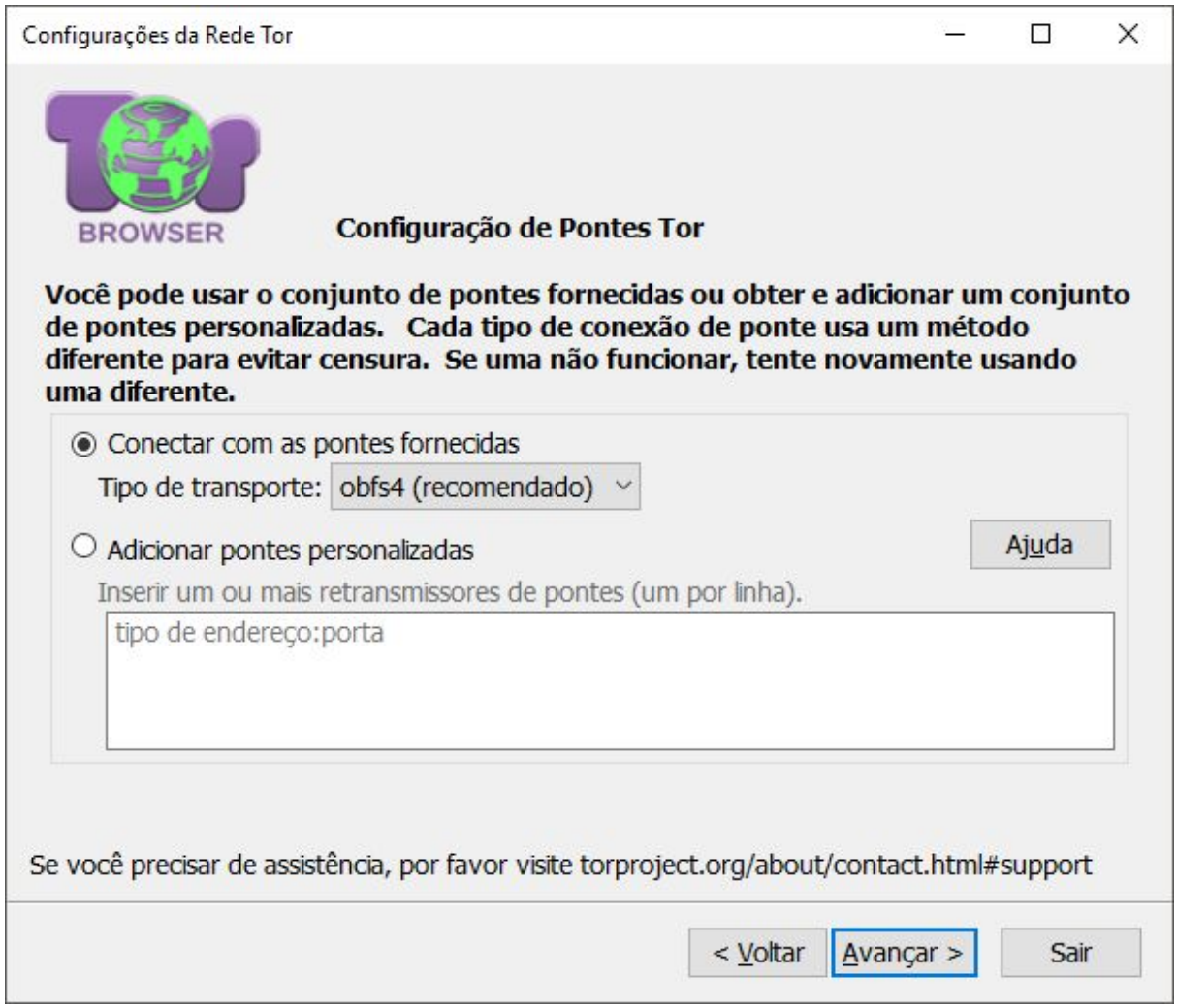

Figura 20 – Segunda tela de configuração do TOR

Como os provedores de Internet brasileiros não censuram ou bloqueiam a Rede TOR de qualquer forma, os próximos passos são demonstrados utilizando a conexão padrão do TOR. Terminando a configuração, o TOR Browser é iniciado logo após o circuito virtual na rede TOR ser estabelecido.

7.1.4. Executando o TOR Browser

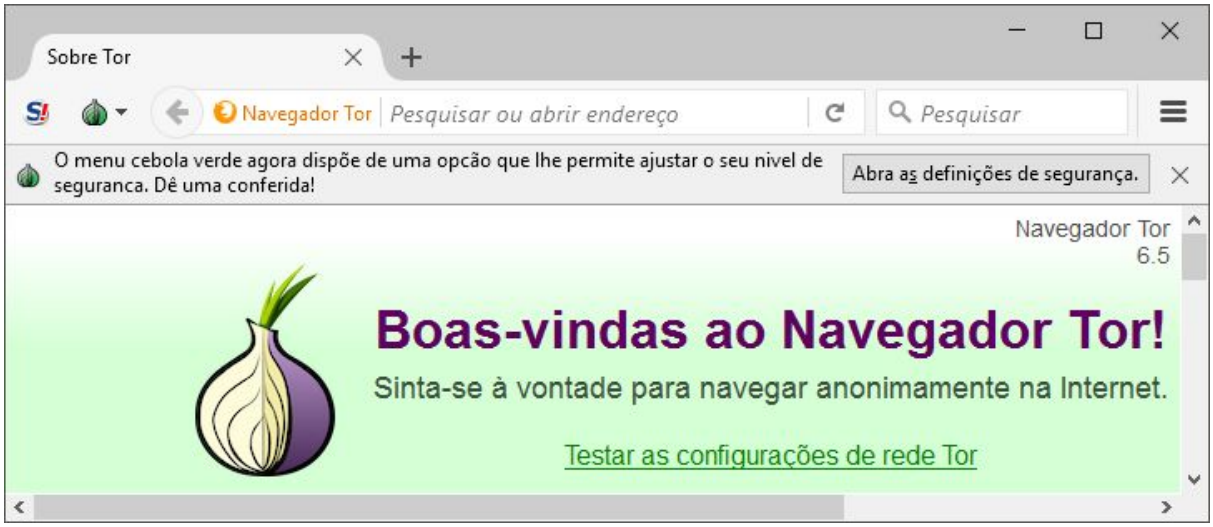

Figura 21 – Tela de boas-vindas do TOR

Na primeira tela, vista na Figura 21, pode-se notar uma extensão de *browser* para bloquear javascript, por questão de segurança, e ao seu lado uma extensão indicando o estado de conexão com a Rede TOR. A partir daí, todo tráfego irá passar pelo circuito virtual estabelecido na Rede.

7.2. Demonstração dos Endereços .onion

Para começar a acessar os endereços ocultos, segue uma demonstração de um acesso a um dos endereços .onion mais populares da Rede TOR, a Hidden Wiki, acessível na Surface Web pelo nome de domínio thehiddenwiki.org, ou através do domínio .onion zqktlwi4fecvo6ri.onion, pela Rede TOR:

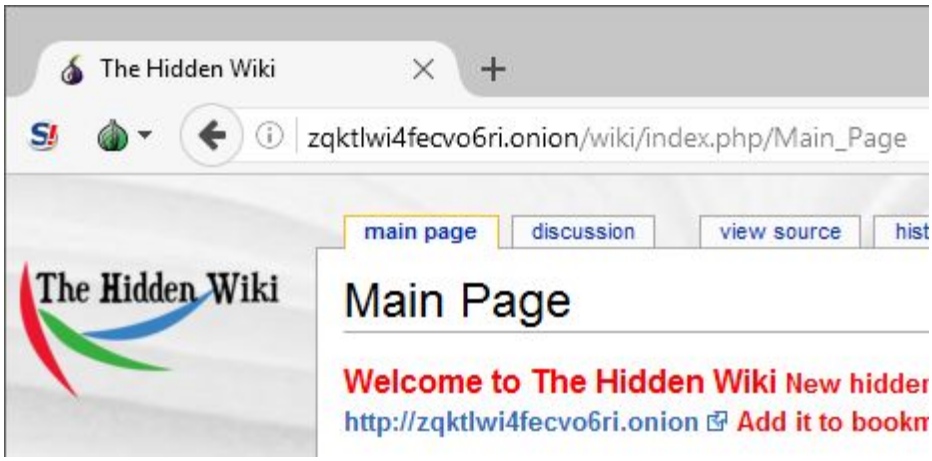

Figura 22 – The Hidden Wiki. Wiki que agrega uma série de informações úteis sobre a dark web.

7.3. Busca por Conteúdo de Desobediência Civil

A Rede TOR pode ser usada para diversos fins. Um deles é a desobediência civil - maneira de protestar contra um governo ou instituição opressora [THOREAU, 2012] - com a luta contra a censura ou vazamento de dados secretos sobre genocídios, por exemplo. Os conteúdos podem vir tanto da Surface Web quanto da Dark Web. Como a navegação é feita através da Rede TOR, a origem é irrelevante, já que o usuário estará anônimo e irrastreável.

Há diversos *sites* de busca da Surface Web com um paralelo na Rede TOR, como por exemplo o DuckDuckGo, cujo endereço comum é duckduckgo.com e seu endereço oculto é 3g2upl4pq6kufc4m.onion.

Outros *sites*, como o NotEvil (hss3uro2hsxfogfq.onion), indexam apenas *sites* .onion. Uma busca rápida por “turkey censorship” retorna mais de mil *links* a respeito da censura do governo Turco com relação ao acesso a informações na Internet, incluindo endereços .onion lutando ativamente contra essa censura.

7.4. Busca por Conteúdo Ilícito

Outro uso relativamente comum da Rede TOR é a busca e transação de conteúdo e serviços ilegais. Venda de drogas ilícitas localmente, prestação de serviços de crimes, como assassinato, sequestros, venda de senhas e fotos vazadas, venda de receitas médicas, etc. Para estes fins, os *sites* de busca na Dark Net também funcionam. E há ainda *sites* especializados em certos tipos de conteúdo ilícito, como o já fechado Silk Road e o BitPharma, que vende diversas drogas ilegais.

É bom lembrar que a grande maioria desses *sites* utiliza como única moeda o Bitcoin, justamente por sua irrastreabilidade nas transações.

7.5. Criação de Website .onion

A criação de um *website* onion é bem simples. Após ter um *webserver* instalado e rodando, basta editar o arquivo *torrc*, instalado junto com o TOR, adicionando o diretório local do serviço, o número da porta e o IP do *website*. O aplicativo TOR, por si só, já indexa o *website* para que ele seja acessível pela Rede TOR e provê seu endereço onion com sua chave privada gerada automaticamente. Com isso, é possível gerar qualquer tipo de *website*, seja com conteúdo de desobediência civil ou de delinquência, e disponibilizá-lo ao mundo.

8. Reflexões Sobre o Impacto Social da Rede TOR

Este capítulo tece considerações sobre os benefícios e malefícios da Rede TOR e do anonimato na sociedade moderna, buscando, por fim, refletir sobre as questões levantadas na Introdução.

8.1. Validade da Rede TOR.

No capítulo de introdução foi levantada a questão “A Rede TOR é, enfim, válida como uma ferramenta para canalizar e destacar uma atitude ou comportamento do ser humano que acaba sendo coibida e censurada, inibida e apequenada pela sociedade?” Questão essa que não pode ser propriamente respondida, e sim vivida, experienciada pela sociedade. O anonimato ainda não é totalmente bem visto pela sociedade moderna.

Um bom caso de análise sobre isso é o WikiLeaks, um *website* que disponibiliza documentos sigilosos vazados de diversos países em sua página. Estes documentos envolvem desde acordos comerciais, passando por trâmites diplomáticos e chegando a provas de crimes internacionais. Porém, a reação inicial e generalizada dos governos quanto ao WikiLeaks foi de repulsa e agressão. Em sua maioria, esses governos são os mesmos que apresentam projetos de lei que de alguma forma limitam e fragilizam a privacidade individual do cidadão.

A Rede TOR talvez seja válida para a voz que quer ser ouvida em um país ditatorial e censurador, como Turquia ou China. Talvez seja válida para expor abusos de guerras civis na África e no Afeganistão. Todas as situações sob o manto do anonimato, em prol da segurança do usuário. Talvez só o tempo julgue, enfim, o potencial da ajuda que a Rede TOR terá no desenvolvimento da liberdade individual,

seja de expressão ou de privacidade, do cidadão e usuário da Rede.

Mas há um outro ponto a ser observado, quando se trata de canalizar algo do ser humano. E é justamente a canalização de uma atitude danosa para sociedade. Da mesma forma que pessoas usam o anonimato para lutar por direitos humanos, outras o usam para a criminalidade. A Rede TOR é popularmente conhecida por cobrir diversos criminosos e crimes em suas páginas ocultas. O potencial humano canalizado, neste caso, é de criar a contravenção. Serviços de tráfego de drogas ilícitas, de prostituição infantil, de venda de dados ilegais, etc. Tudo sob um manto de anonimato e segurança. Mas será que a presença deste tipo de público contamina a Rede TOR? Ou talvez esse tipo de atitude se apresente não importa o meio, seja físico ou virtual, e que a humanidade sempre terá esse tipo de atitude delinquente, independente dos métodos, tecnologias e meios?

O ser humano sempre praticou o crime e sempre buscou o proibido. Será que a ferramenta TOR, por si só, incentiva este comportamento ou quiçá o cria? Alternativamente, pode-se entender que ela é apenas mais um meio desenvolvido pelo ser humano que foi explorado de diversas formas distintas, boas e ruins.

8.2. Limite Moral na Internet

Foi perguntado também na Introdução se “Existe limite moral para o uso da Internet?”. Mas, qual a diferença entre as variações do comportamento moral na Internet e aquelas observadas no mundo físico, desde milhares de anos de humanidade e sociedade? É senso comum assumir que o imoral, o amoral e o moral existem em todos os meios. Sendo assim, a Rede TOR apenas funcionaria como uma máscara virtual para seu usuário, em uma sociedade que usa outras formas de mascaramento desde seus primórdios. Pode-se entender, portanto, que o virtual não

muda o homem, é apenas uma de suas ferramentas que é usada a seu bel prazer. Caberia então a reflexão se existe limite da moral na própria humanidade.

Pode-se concluir, portanto, que a Rede TOR é apenas uma ferramenta que preza pela identidade de seu usuário. Deixa-o anônimo se assim ele desejar. E a ética no uso da ferramenta cabe ao próprio usuário. Seriam a sociedade e a Rede TOR aliados ou inimigos? A sociedade deve olhar para si própria na busca por esta resposta.

9. Conclusão

A busca do anonimato sempre esteve presente ao longo da história da humanidade. Como uma ferramenta, foi usada para diversos fins, positivos ou não. Nos dias de hoje há um consenso da maioria das nações em proteger o anonimato em prol do indivíduo que busca se proteger ou proteger sua opinião e voz. Mas nem sempre foi assim, e talvez algum dia essa realidade mude novamente.

Este trabalho pôde apresentar a fundo o histórico e o funcionamento da Rede TOR, suas possibilidades e usos. Pôde-se ver que apesar do uso do anonimato, a finalidade do tráfego do usuário final não difere muito da de um usuário que não busca a máscara do anonimato para ocultar sua identidade e rastros. Estatísticas demonstram que o conteúdo ilegal e/ou questionável, por mais subjetivo que este assunto seja, é um conteúdo acessado por uma minoria.

Por fim, o que limita o uso da ferramenta TOR e, acima dela, o anonimato, é o usuário por trás da tela. O anonimato irá se desdobrar para o uso legal e moral ou ilegal e imoral, dependendo da intenção do indivíduo que dele usufrui. Se não fosse a Rede TOR, possivelmente seria algum outro método similar.

10. Referências Bibliográficas

1. CHAABANE, Abdelberi; MANILS, Pere; KAAFAR, Mohamed Ali. *Digging into Anonymous Traffic: A deep analysis of the Tor anonymizing network*. 4th IEEE International Conference on Network and System Security (NSS), 2010. Melbourne, Austrália.
2. DINGLEDINE, Roger; MATHEWSON, Nick; SYVERSON, Paul. *Tor: The Second-Generation Onion Router*. Proceedings of the 13th conference on USENIX Security Symposium (SSYM), 2004. San Diego, Estados Unidos.
3. THOREAU, Henry David. *A Desobediência Civil,* 2012. Brasil: Editora Companhia das Letras.
4. JANSEN, Rob et al. *Methodically Modeling the Tor Network*. 5th Workshop on Cyber Security Experimentation and Test (CSET), 2012. Bellevue, Estados Unidos.
5. LOESING, Karsten, et al. *Performance measurements and statistics of Tor hidden services*. IEEE International Symposium on Applications and the Internet (SAINT), 2008. Turku, Finlândia.
6. NOVAES, Rafael. *Saiba o que é criptomoeda, para que ela serve e como utilizá-la*. Psafe.com, 2014. Disponível em: <http://www.psafe.com/blog/o-que-criptomoeda/>.
7. EFF. *TOR and HTTPS*. 2012. Disponível em: <https://www.eff.org/pages/tor-and-https>.
8. KAYE, David. *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*. 17ª Sessão do Conselho de Direitos Humanos das Nações Unidas, 2015.
9. TOR Metrics. *Top-10 countries by bridge users*. Disponível em: <https://metrics.torproject.org/userstats-bridge-table.html>.