FIAP ON

BIOHACKING, DEEP WEB E CRIPTOGRAFIA

DEEP WEB – APLICAÇÃO PRÁTICA

OSMANY D. R. DE ARRUDA

4

LISTA DE FIGURAS

Figura 4.1 – *Onion services* – Fase 1.....7
Figura 4.2 – *Onion services* – Fase 2.....8
Figura 4.3 – *Onion services* – Fase 3.....9
Figura 4.4 – *Onion services* – Fase 4.....10
Figura 4.5 – *Onion services* – Fase 5.....11
Figura 4.6 – *Onion services* – Fase 6.....12
Figura 4.7 – Tor e HTTPS.....15
Figura 4.8 – Download do Tor *browser* 64 bits para Linux, idioma inglês.....17
Figura 4.9 – Página de configuração inicial do Tor *browser*.....19
Figura 4.10 – Lançador do Tor *browser*.....20
Figura 4.11 – Utilização do Tor *browser*.....20
Figura 4.12 – Menu de configurações do Tor *browser*.....21
Figura 4.13 – Menu de informações do Tor *browser*.....21
Figura 4.14 – Menu do HTTPS *Everywhere* no Tor *browser*.....22
Figura 4.15 – Menu alternativo no botão do HTTPS *Everywhere*.....22
Figura 4.16 – Biblioteca on-line na *deep web*.....23
Figura 4.17 – Análise de arquivo pelo VirusTotal.....24

LISTA DE TABELA

Tabela 4.1 – Especificações de referência para a máquina virtual 17

LISTAGEM DE COMANDOS

Listagem 4.1 – Instalação do Tor *browser* em linha de comando 18
Listagem 4.2 – Script de configuração do Tor *browser* 19

SUMÁRIO

4 DEEP WEB – APLICAÇÃO PRÁTICA 6
4.1 O Tor na prática 6
4.2 Onion services e o protocolo rendezvous.....7
4.3 Tor *versus proxies* tradicionais.....12
4.4 O navegador Tor 13
4.5 Instalando o Tor 17
4.6 Utilizando o Tor *browser*.....20
REFERÊNCIAS.....25
GLOSSÁRIO 26

4 DEEP WEB – APLICAÇÃO PRÁTICA

4.1 O Tor na prática

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 de 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.

Nessa linha, o Tor se apresenta ainda como uma ferramenta eficaz para que o usuário possa se esquivar também de algum tipo de censura, conseguindo, então, 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. 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.

4.2 Onion services e o protocolo rendezvous

Como já sabido, o Tor possibilita aos usuários ocultarem suas localizações ao disponibilizar diferentes tipos de serviços, tais como publicações web e servidores de mensagens instantâneas. Por meio dos *rendezvous points*, outros usuários do Tor poderão se conectar a esses serviços (*onion services*) mesmo sem conhecer a identidade de rede uns dos outros. Um *onion service* precisa anunciar sua existência na rede Tor antes que os clientes possam contatá-lo. Portanto, o serviço seleciona aleatoriamente alguns relés, constrói circuitos para eles e pede que atuem como pontos de inserção, informando sua chave pública.

Usando um circuito Tor completo, é difícil para qualquer um associar um ponto de inserção ao endereço IP do servidor *onion*. Os pontos de inserção e demais são informados a respeito da identidade do serviço *onion* (chave pública), mas não da localização do servidor *onion* (endereço IP). A fim de estudar o funcionamento dos *onion services*, considere-se a Figura "*Onion services* – Fase 1", em que Bob escolhe alguns pontos de inserção e constrói circuitos para conexão com eles (os *links* verdes são circuitos, e não conexões diretas).

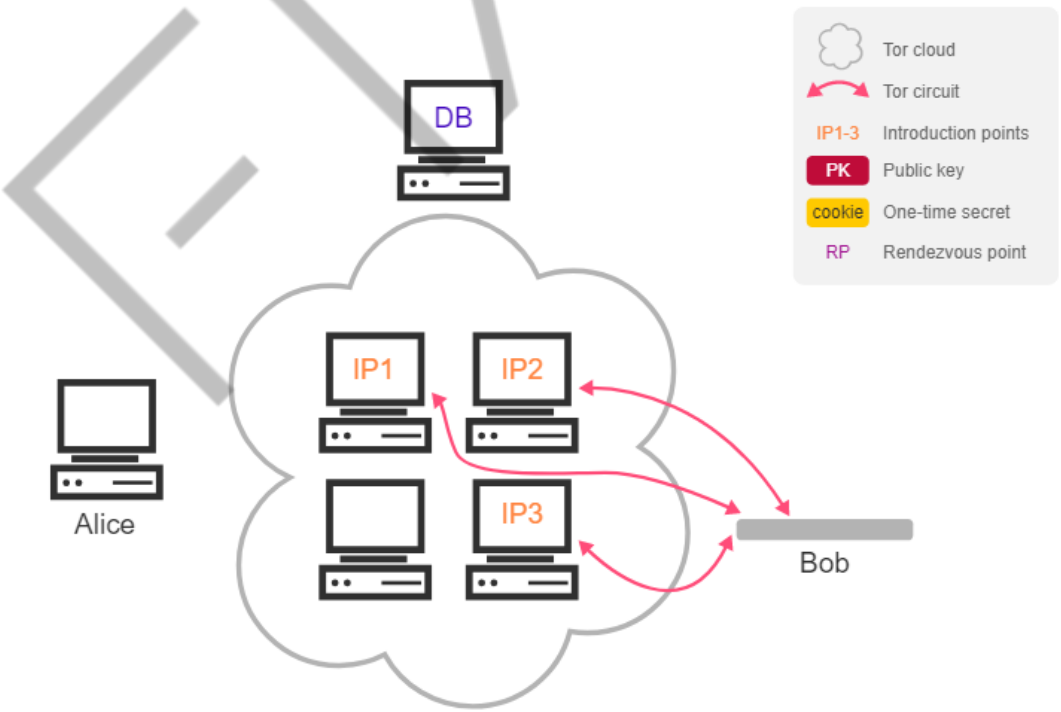

Figura 4.1 – *Onion services* – Fase 1
Fonte: Tor Project (2020)

Na sequência, o *onion service* cria um descritor contendo sua chave pública e um resumo de cada ponto de inserção e assina esse descritor com sua chave privada, fazendo o *upload* desse descritor para uma tabela *hash* distribuída. O descritor será encontrado pelos clientes que solicitarem XYZ.onion, em que XYZ é um nome com 16 caracteres derivado da chave pública do serviço. Após essa etapa, o *onion service* é configurado.

Embora possa parecer impraticável usar um nome de serviço gerado automaticamente, ele atende a um objetivo importante: todos – incluindo os pontos de inserção, o diretório da tabela *hash* distribuída e clientes – podem verificar se estão transacionando com o *onion service* correto. Observe-se ainda que isso acontece em conformidade com a conjectura (triângulo) de Zooko: seguro, descentralizado e ter significado para humanos, duas das propriedades desejadas para os nomes foram alcançadas na medida em que os nomes utilizados pela rede Tor são seguros e descentralizados. Na Figura "*Onion services* – Fase 2", Bob anuncia seu serviço XYZ.onion na base de dados.

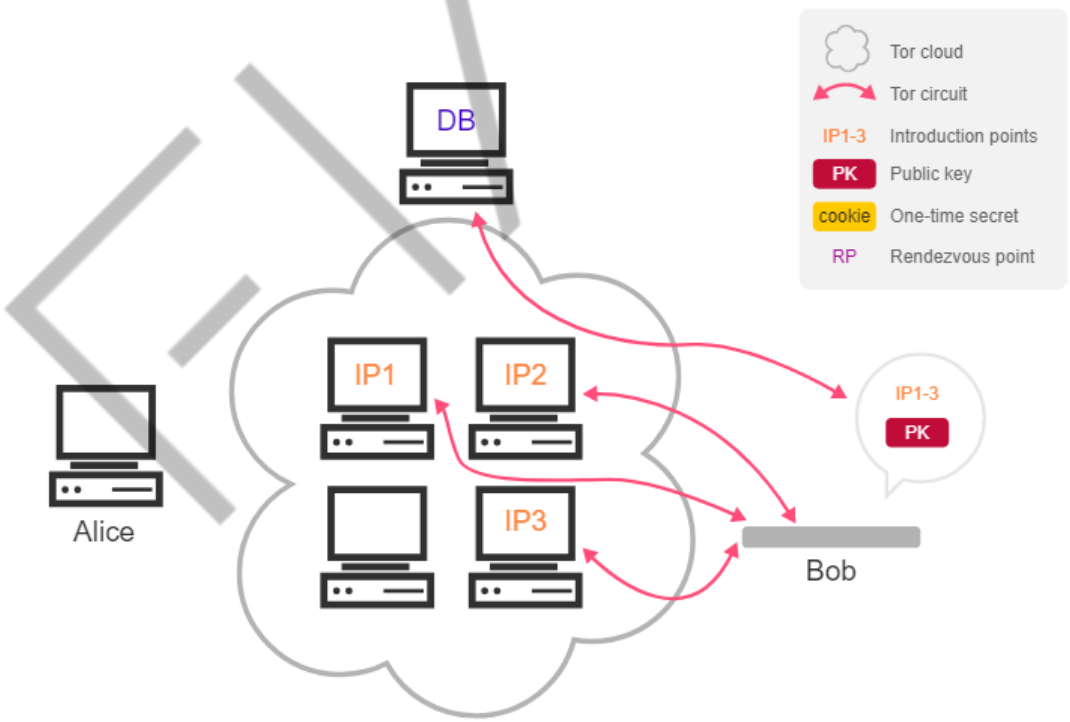

Figura 4.2 – *Onion services* – Fase 2
Fonte: Tor Project (2018)

Logo, para que um cliente possa acessar um *onion service*, ele deverá ter prévio conhecimento do *onion address* do serviço desejado e depois, então, baixar o respectivo descritor a partir da tabela *hash* distribuída para poder iniciar a conexão

com ele. Se houver um descritor para XYZ.onion, o cliente será informado a respeito do conjunto de pontos de inserção, e da chave pública correta, a utilizar. Neste momento, o cliente criará um circuito para outro relé escolhido aleatoriamente, solicitando-lhe que se torne um *rendezvous point* e comunicando-lhe um *one-time secret*.

Na Figura "*Onion services* – Fase 3", Alice descobre o *onion service* XYZ.onion e solicita maiores informações à base de dados, configurando um *rendezvous point*, embora pudesse tê-lo feito anteriormente.

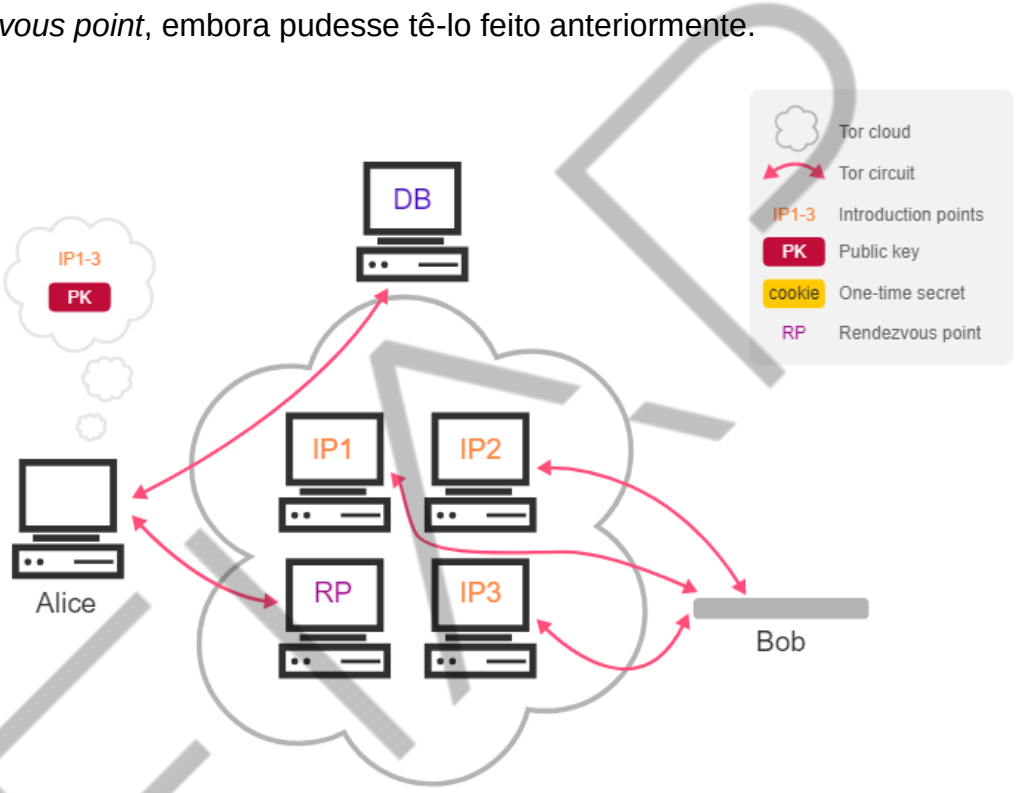

Figura 4.3 – *Onion services* – Fase 3
Fonte: Tor Project (2020)

Quando o descritor for encontrado e o *rendezvous point* estiver pronto, o cliente monta uma mensagem de apresentação (criptografada com a chave pública do *onion service*), incluindo o endereço do *rendezvous point* e o *one-time secret* utilizado, enviando essa mensagem a algum dos pontos de inserção, solicitando que seja entregue ao *onion service*. Novamente, a comunicação é estabelecida por meio dos circuitos do Tor, impedindo que o endereço IP do remetente da mensagem (de apresentação) venha a ser revelado, garantindo seu anonimato (Figura "*Onion services* – Fase 4").

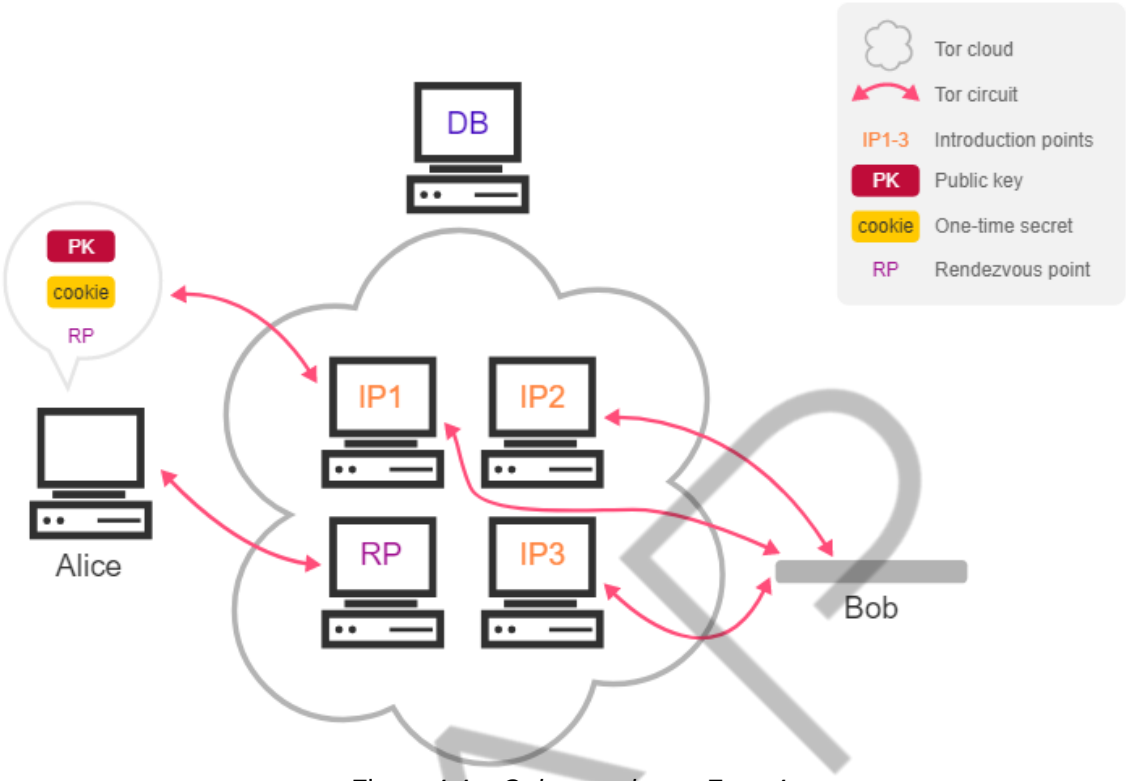

Figura 4.4 – *Onion services* – Fase 4
Fonte: Tor Project (2020)

Na Figura "*Onion services* – Fase 4", Alice envia uma mensagem a Bob (criptografada pela chave pública – PK) listando os *rendezvous points* mais um *one-time secret* e solicita a um ponto de inserção que entregue a Bob. O *onion service* decriptografa a mensagem de apresentação do cliente, na qual encontra o endereço IP do *rendezvous point* (RP) e o *one-time secret* (OTS), criando, então, um circuito para esse RP, por meio do qual lhe envia uma *rendezvous message* com o OTS.

Neste ponto, torna-se altamente relevante que o *onion service* utilize os mesmos *entry guards* ao criar novos circuitos, senão, um atacante poderá executar seu próprio relé e forçar o *onion service* a criar um número arbitrário de circuitos na esperança de que seu relé clandestino seja utilizado como nó de entrada, possibilitando, assim, a descoberta do endereço IP do *onion service* por meio de análise do *timing*. Na Figura "*Onion services* – Fase 5", Bob se conecta ao RP de Alice e resolve o OTS dela.

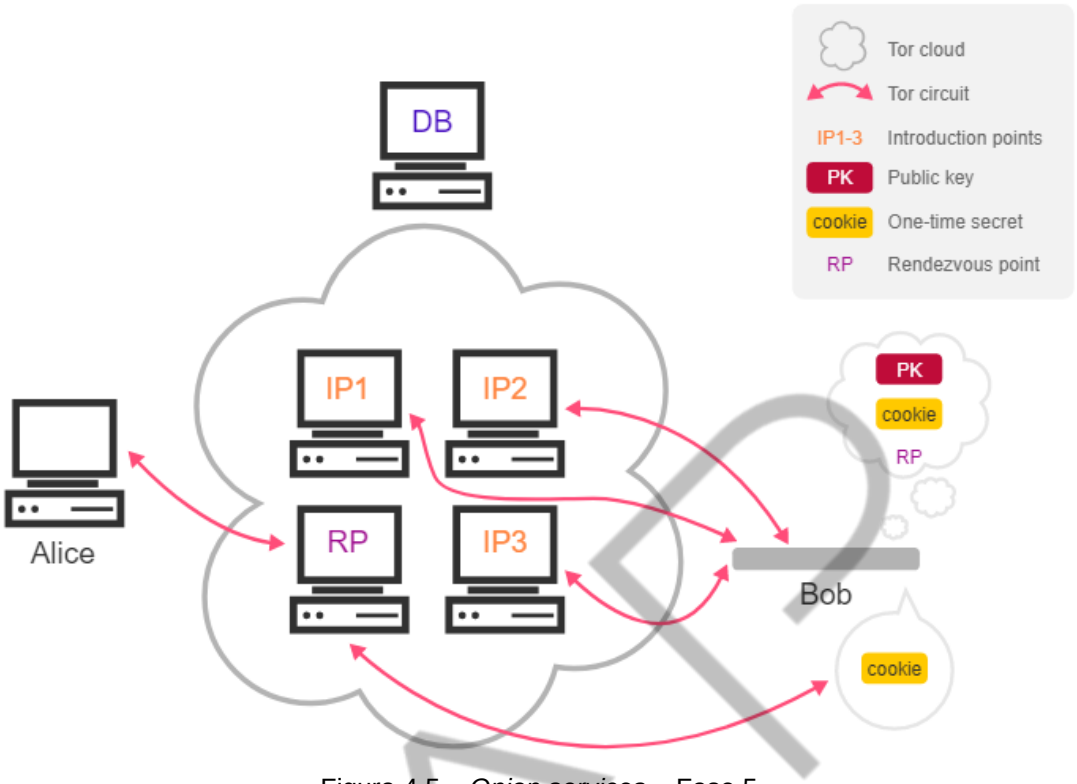

Figura 4.5 – *Onion services* – Fase 5
Fonte: Tor Project (2020)

Na última fase, o RP notifica o cliente de que a conexão foi estabelecida com sucesso. A partir de então, cliente e *onion service* podem usar seus circuitos para o RP a fim de se comunicar. O RP simplesmente se encarrega da retransmissão das mensagens (criptografadas fim a fim) do cliente para o serviço e vice-versa.

Um dos motivos para não se utilizar o circuito de inserção para comunicação real é que nenhum relé único deve aparentar ser o responsável por um dado *onion service* – por isso, o RP nunca aprende a respeito da identidade do *onion service*. Geralmente, o estabelecimento da conexão entre cliente e o *onion service* consiste de seis relés, tendo três deles sido escolhidos pelo cliente – sendo o terceiro, o *rendezvous point* – e os outros três, pelo *onion service*.

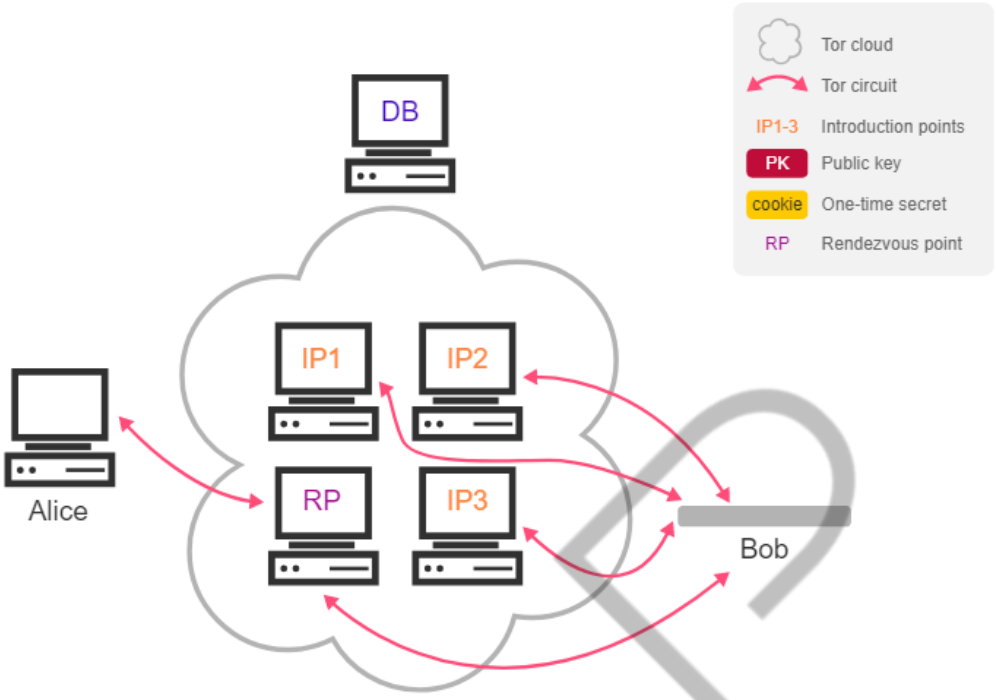

Figura 4.6 – *Onion services* – Fase 6
Fonte: Tor Project (2020)

Na Figura "*Onion services* – Fase 6", Bob e Alice utilizam seus circuitos para a comunicação normal.

4.3 Tor *versus proxies* tradicionais

Um provedor *proxy* típico configura um servidor em algum lugar da Internet e permite aos usuários utilizá-lo para reencaminhamento (*relay*) de seu tráfego, criando, assim, uma arquitetura simples e de fácil manutenção, em que os usuários entram e saem através do mesmo servidor. O provedor pode cobrar pelo uso do *proxy* ou custear suas despesas por intermédio de anúncios.

Configurações mais simples não exigem a instalação de softwares adicionais, bastando que o *browser* seja apontado para o *proxy*. Esses *proxies* podem ser uma boa solução quando o usuário não deseja proteger sua privacidade, e anonimato on-line, e confia no provedor do serviço. Alguns provedores de *proxy* usam SSL para proteger a conexão entre os usuários e seus servidores, o que pode protegê-los também contra bisbilhoteiros locais, como aqueles em estabelecimentos com Internet sem fio gratuita.

Provedores de *proxy* simples criam um ponto único de falha. Eles sabem quem são seus usuários e por onde eles navegam na Internet, podendo monitorar seu tráfego conforme ele atravessa o servidor. Em alguns casos, esses provedores podem até mesmo monitorar o tráfego criptografado enquanto o reencaminha ao site bancário ou de comércio eletrônico solicitado pelo usuário. O usuário deve, então, confiar que o provedor não está monitorando seu tráfego, nem coletando seus dados pessoais, dentre outras atividades indesejadas.

Diferentemente disso, o Tor encaminha o tráfego do usuário por, ao menos, três servidores diferentes antes de enviá-lo ao destino. Como há uma camada separada de criptografia para cada um dos três relés, alguém que esteja monitorando a conexão do usuário com a Internet não será capaz de ler ou modificar o conteúdo trafegado pela rede Tor.

Entretanto, desses três servidores, um primeiro servidor malicioso pode ser capaz de inspecionar o tráfego vindo do computador do usuário, embora não saiba quem é esse usuário, nem o que faz na rede Tor, tomando conhecimento apenas de um endereço IP que está utilizando o Tor. Já um terceiro servidor malicioso dentre esses três poderá visualizar o tráfego enviado pelo Tor, embora não tenha conhecimento sobre quem o enviou. Se esse tráfego estiver criptografado, por exemplo, via HTTPS, o terceiro servidor será capaz de identificar apenas o destino desse tráfego.

4.4 O navegador Tor

De acordo com o projeto, para que a rede Tor seja eficaz, alguns hábitos de navegação do usuário deverão ser mudados:

a. Utilizar o Tor *browser.*

   O Tor não protege todo o tráfego enviado pelo usuário à Internet, e 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.

b. 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).

c. Não instalar ou habilitar *plugins* no navegador.

   O navegador Tor bloqueará plug-ins, 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.

d. Utilizar as versões HTTPS dos sites.

   O Tor criptografará 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.

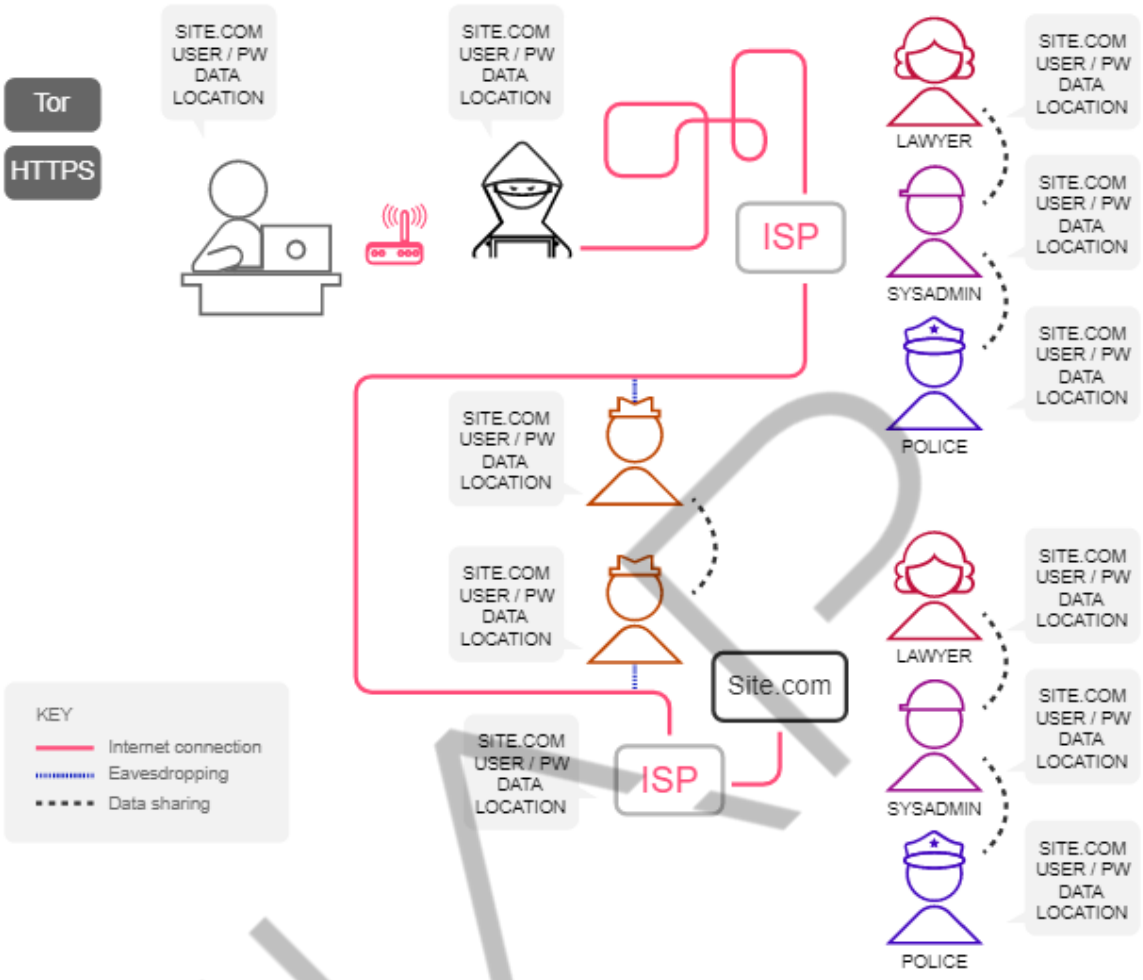

Figura 4.7 – Tor e HTTPS
Fonte: Electronic Frontier Foundation (2020)

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, exibam o nome esperado para o website. Com base na Figura “Tor e HTTPS”, a Electronic Frontier Foundation coloca:

- Clicar no botão “Tor” para verificar quais dados poderão estar visíveis por terceiros quando o Tor estiver em uso. O botão ficará verde, indicando que o Tor está ativo.
- Clique no botão “HTTPS” para verificar quais dados poderão estar visíveis por terceiros quando o HTTPS estiver em uso. O botão ficará verde, apontando que o HTTPS está ativo.

- Quando os dois botões estiverem verdes, o usuário poderá verificar os dados eventualmente visíveis por terceiros quando se utilizar das duas ferramentas.
- Quando os dois botões estiverem cinzas, o usuário poderá verificar os dados eventualmente visíveis por terceiros quando nenhuma das ferramentas estiver em uso.
- Informações potencialmente expostas incluem a URL do site visitado, credenciais (*username* e senha) do usuário, os dados trafegados, o endereço IP do usuário e se ele utiliza ou não o Tor.
- Não abrir documentos baixados por meio do Tor enquanto estava on-line. 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.

e. 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.

4.5 Instalando o Tor

Para instalação e utilização do Tor, sugere-se a criação de uma máquina virtual com as configurações da Tabela “Especificações de referência para a máquina virtual”.

Tabela 4.1 – Especificações de referência para a máquina virtual

Parâmetro	Especificação
Hypervisor	VirtualBox
Sistema operacional	Debian 64bits (versão corrente)
Memória	1GB
Disco	8GB
Rede	NAT
vCPU	1

Fonte: Elaborado pelo autor (2020)

Logado na referida máquina virtual como usuário desprivilegiado, baixar a versão estável mais recente do Tor *browser* a partir de:

<https://www.torproject.org/download/download-easy.html.en>

Vale lembrar que o Tor *browser* está disponível em diversos idiomas e diferentes sistemas operacionais (Figura “Download do Tor *browser* 64 bits para Linux, idioma inglês”).

Figura 4.8 – Download do Tor *browser* 64 bits para Linux, idioma inglês
Fonte: Tor Project (2018)

Finalizado o *download*, a partir de um terminal, entrar no diretório Downloads e descompactar o pacote (Listagem “Instalação do Tor *browser* em linha de comando”).

```
     user1@deb00:~$ cd Downloads/
     user1@deb00:~/Downloads$ ls
     tor-browser-linux64-8.0.3_en-US.tar.xz
     user1@deb00:~/Downloads$ tar xvJf tor-browser-linux64-
9.5_en-US.tar.xz
     !
     <--várias linhas omitidas-->
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/cyaml.py
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/dumper.py
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/emitter.py
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/error.py
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/events.py
     tor-browser_en-
US/Browser/TorBrowser/Tor/PluggableTransports/yaml/loader.py
     <--várias linhas omitidas-->
     !
     user1@deb00:~/Downloads$ ls
     tor-browser_en-US  tor-browser-linux64-9.5_en-US.tar.xz
     user1@deb00:~/Downloads$
```

Listagem 4.1 – Instalação do Tor *browser* em linha de comando
Fonte: Elaborado pelo autor (2020)

Com base na Listagem “Instalação do Tor *browser* em linha de comando”, é possível observar que o pacote do Tor *browser* é um arquivo compactado (tor-browser-linux64-9.5_en-US.tar.xz), o qual foi descompactado pelo comando tar com as opções x (*extract*), v (*verbose*), J (descompactador para arquivos xz) e f (nome do arquivo), criando, assim, o diretório tor-browser_en-US, repositório dos arquivos do pacote. A partir desse diretório, executar o script start-tor-browser.desktop (Listagem “Script de configuração do Tor *browser*”).

```
     user1@deb00:~/Downloads$ cd tor-browser_en-US/
     user1@deb00:~/Downloads/tor-browser_en-US$ ls -l
     total 8
     drwx------ 10 user1 user1 4096 dez 31  1999 Browser
     -rwx------  1 user1 user1 1682 dez 31  1999 start-tor-
browser.desktop
     user1@deb00:~/Downloads/tor-browser_en-US$    ./start-tor-
browser.desktop
```

```
Launching './Browser/start-tor-browser --detach'...
user1@deb00:~/Downloads/tor-browser_en-US$
```

Listagem 4.2 – Script de configuração do Tor *browser*
Fonte: Elaborado pelo autor (2020)

Após alguns instantes, a janela do Tor *browser* surgirá (Figura "Página de configuração inicial do Tor *browser*"), oferecendo opções para conexão à rede Tor e para a configuração do *browser*. Não haverá necessidade de configurar o Tor *browser* se o usuário não utilizar nenhum *proxy* para a navegação, nem estiver em local onde o Tor seja censurado, podendo-se, então, clicar no botão *Connect*.

Figura 4.9 – Página de configuração inicial do Tor *browser*
Fonte: Elaborado pelo autor (2020)

Após o estabelecimento da primeira conexão – que pode demorar um pouco para ser efetivada, o script criará um lançador (ícone) para o Tor *browser*, o qual poderá ser copiado para a área de trabalho (Figura "Lançador do Tor *browser*"). Note que o ícone está dentro do diretório ~/Downloads/tor-browser_en-US

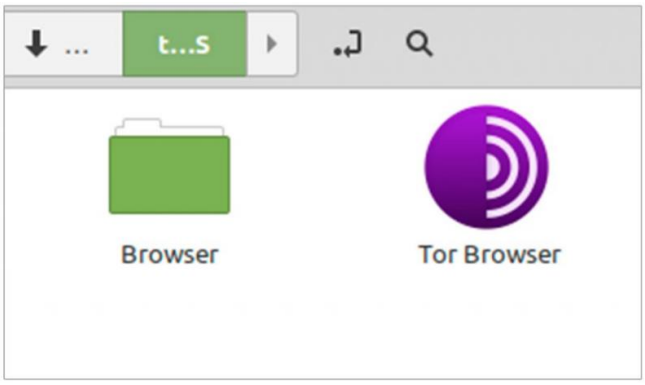

Figura 4.10 – Lançador do Tor *browser*
Fonte: Elaborado pelo autor (2020)

4.6 Utilizando o Tor *browser*

Para essa primeira incursão com o Tor *browser*, será utilizada a URL: <http://torlinkbgs6aabns.onion/> (Figura “Utilização do Tor *browser*”).

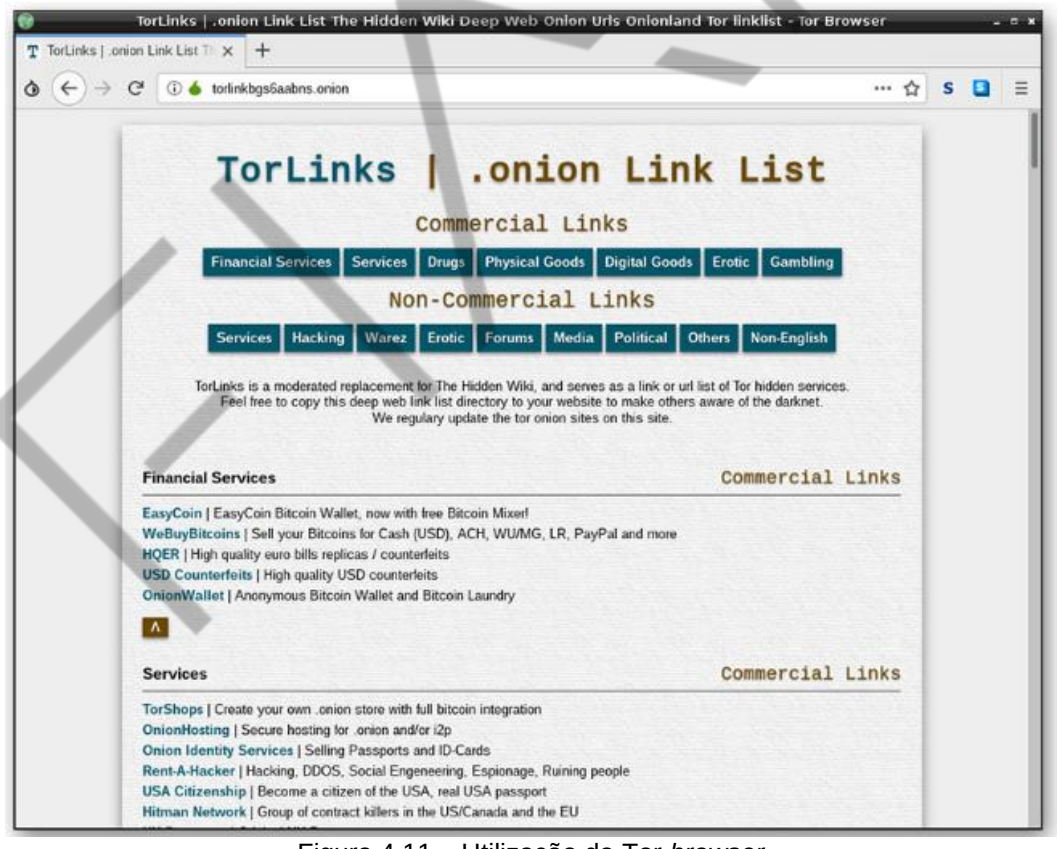

Figura 4.11 – Utilização do Tor *browser*
Fonte: Elaborado pelo autor (2020)

Ela levará o usuário a uma página com *links* para diversos *onion services*, relacionados aos mais diversos assuntos. Observe que, por razões de segurança, a janela do Tor *browser* não foi maximizada, permanecendo no tamanho original

definido pelo próprio navegador. O destaque (Figura “Menu de configurações do Tor *browser*”) ilustra o menu de configurações do Tor *browser*, acessível por meio do botão *onion* (cebola) posicionado no canto superior esquerdo do navegador. Tais configurações são simples e autoexplicativas, não exigindo alterações.

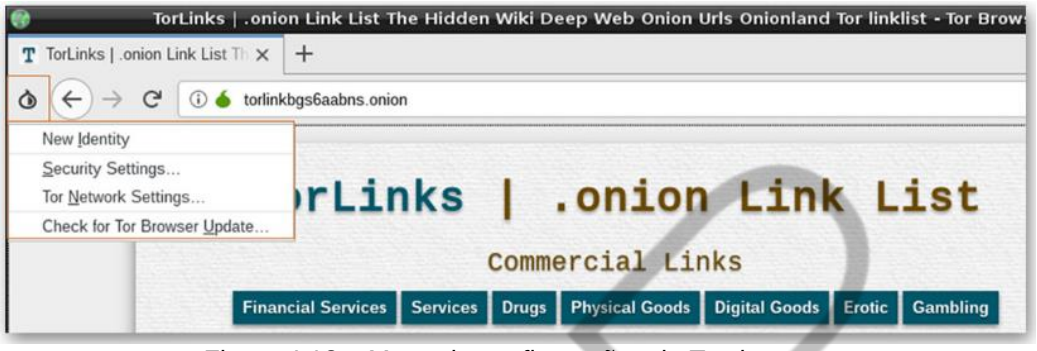

Figura 4.12 – Menu de configurações do Tor *browser*
Fonte: Elaborado pelo autor (2020)

Ao clicar no botão de informações, na barra de URL do navegador, o usuário obterá importantes informações relacionadas ao site e à conexão (Figura “Menu de informações do Tor *browser*”).

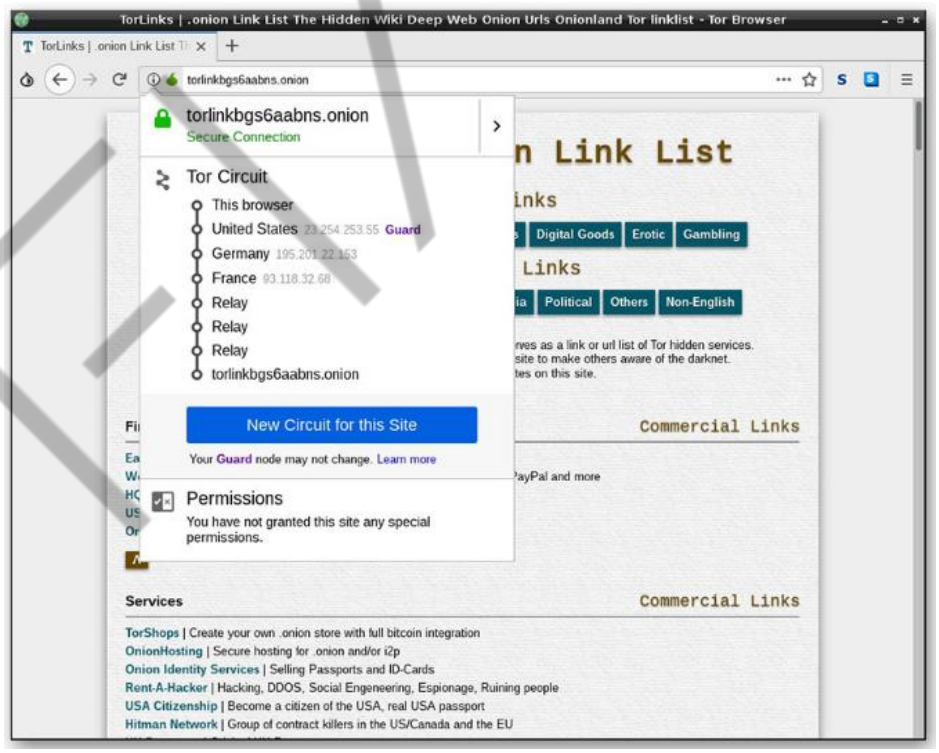

Figura 4.13 – Menu de informações do Tor *browser*
Fonte: Elaborado pelo autor (2020)

No canto superior direito do navegador, encontra-se o painel do HTTPS *Everywhere* (Figura “Menu do HTTPS *Everywhere* no Tor *browser*”). Os menus invocados por esse botão, em destaque na Figura “Menu do HTTPS *Everywhere* no

Tor *browser*", são diferentes em função do botão utilizado no mouse. O menu ilustrado na Figura "Menu do HTTPS *Everywhere* no Tor *browser*" foi invocado pelo botão esquerdo do mouse.

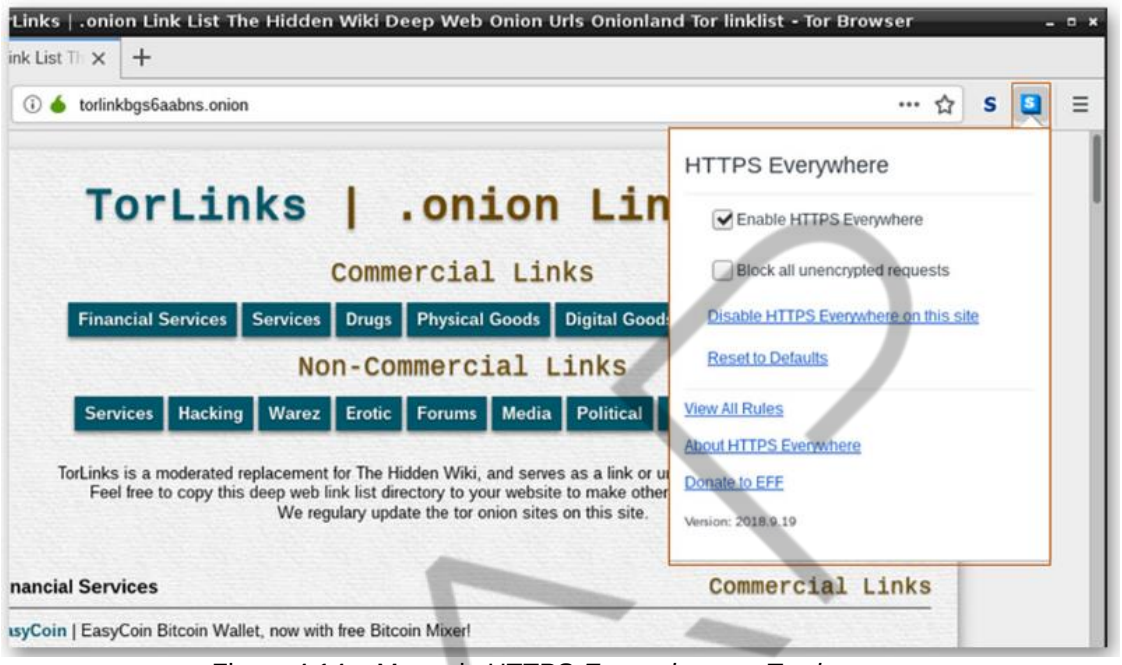

Figura 4.14 – Menu do HTTPS *Everywhere* no Tor *browser*
Fonte: Elaborado pelo autor (2020)

Por exemplo, ao clicar-se com o botão direito do mouse sobre o referido botão do navegador, novas opções serão apresentadas ao usuário, permitindo-lhe, por exemplo, habilitar a barra de menu e de *bookmarks* (Figura "Menu alternativo no botão do HTTPS *Everywhere*").

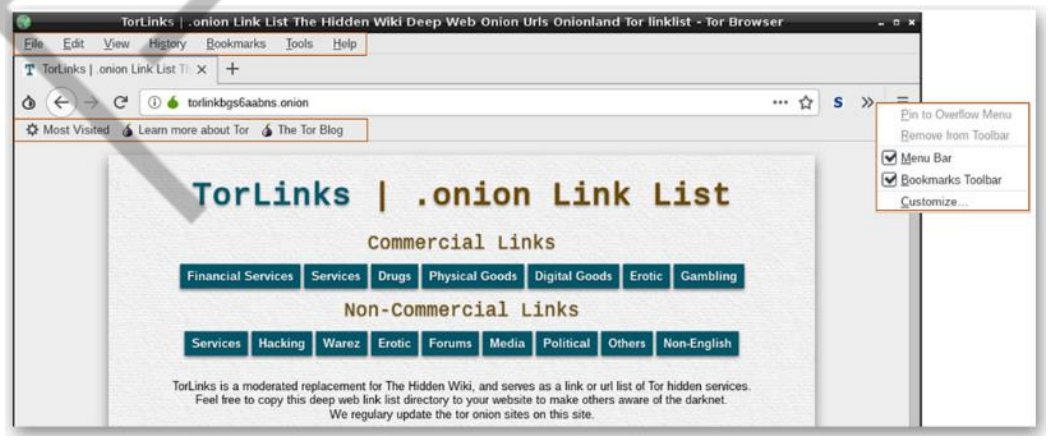

Figura 4.15 – Menu alternativo no botão do HTTPS *Everywhere*
Fonte: Elaborado pelo autor (2020)

Vale a pena para o usuário investir algum tempo conhecendo melhor o Tor *browser* a fim de conseguir usufruir de suas funcionalidades integral e corretamente, enfatizando-se, ainda, ser prática recomendável o uso de VPNs em conjunto com o

Tor *browser* a fim de garantir a segurança e o anonimato do usuário na *deep/dark web*.

O site <http://xfmro77i3lixucja.onion/> é uma biblioteca on-line (*Imperial Library of Trantor*) na *deep web* que contém milhares de títulos (e-books) disponíveis para download.

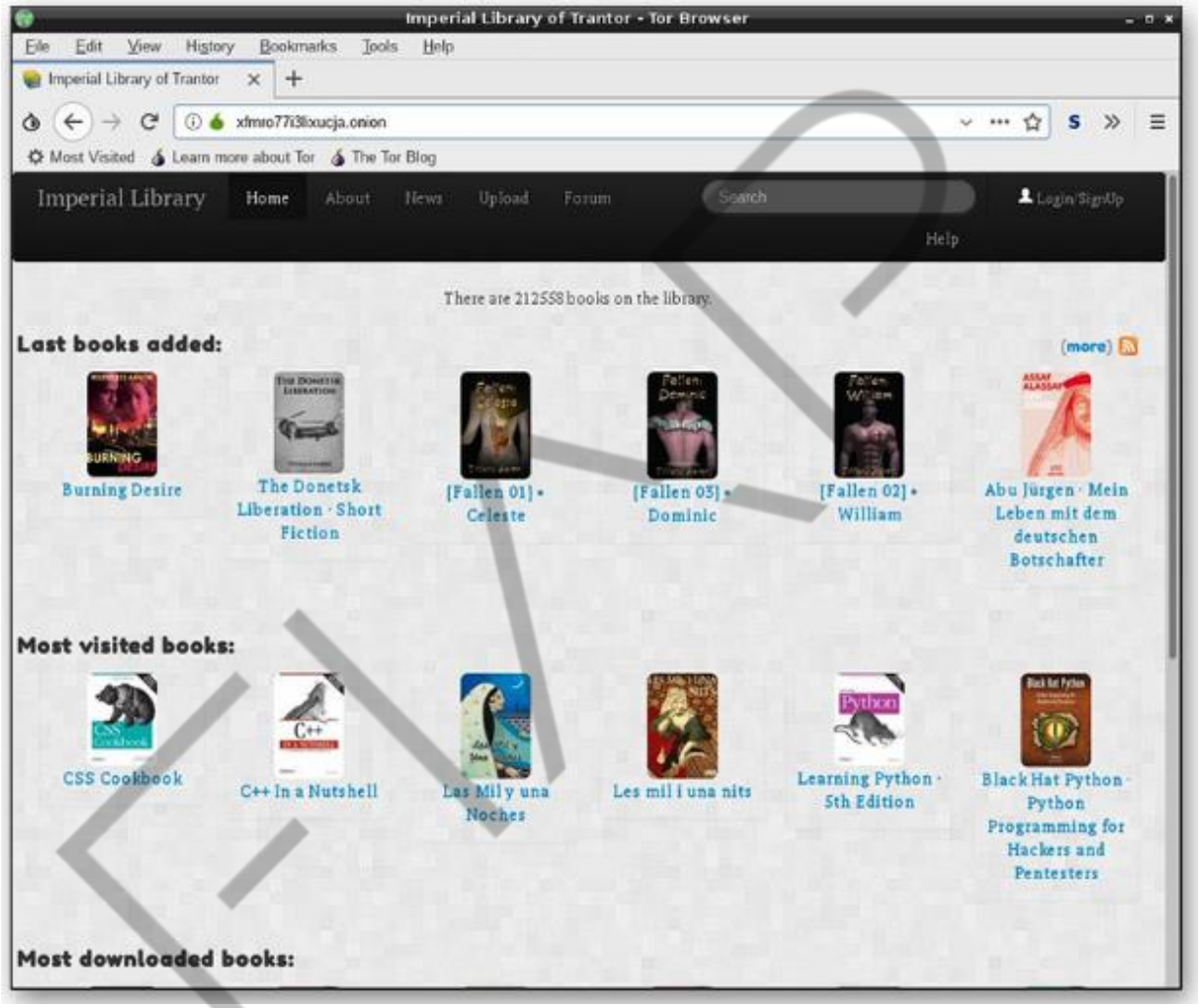

Figura 4.16 – Biblioteca on-line na *deep web*
Fonte: Elaborado pelo autor (2020)

Embora, em geral, seja considerado um *site* seguro (para os padrões da *deep web*), recomenda-se submeter o material baixado ao VirusTotal (https://www.virustotal.com) ou site análogo, para verificação do arquivo antes de retirá-lo da máquina virtual ou carregá-lo para o leitor de e-books. A Figura “Análise de arquivo pelo VirusTotal” ilustra o resultado da análise feita pelo do VirusTotal em um arquivo baixado da *Imperial Library*.

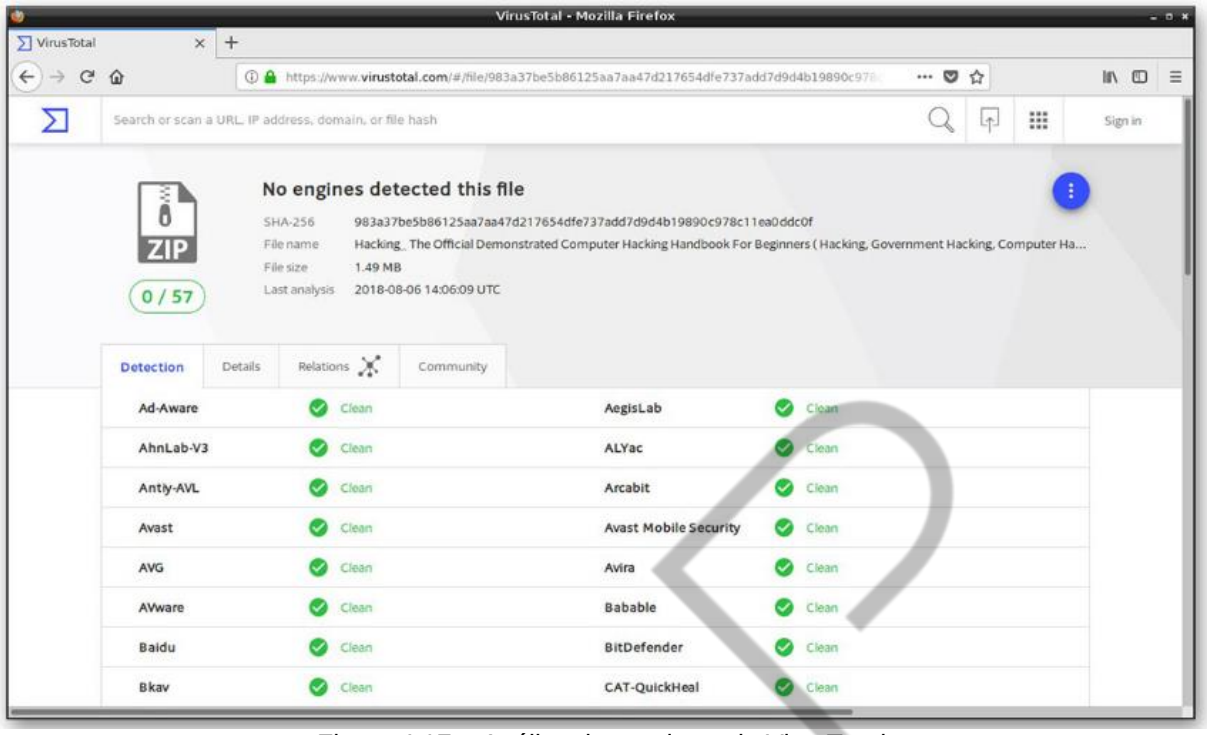

Figura 4.17 – Análise de arquivo pelo VirusTotal
Fonte: Elaborado pelo autor (2018)

Embora o tipo de arquivo baixado (*epub*) não seja suportado pelo Tor *browser*, vale reforçar a orientação do Tor Project e evitar a abertura dos arquivos baixados diretamente nele. Observe, por fim, que a submissão do arquivo a ser analisado também não foi feita por meio do Tor *browser*.

REFERÊNCIAS

ELECTRONIC FRONTIER FOUNDATION. **How HTTPS and Tor work together to protect your anonymity and privacy.** Disponível em: <https://www.eff.org/pages/tor-and-https>. Acesso em: 16 jun. 2020.

ELECTRONIC FRONTIER FOUNDATION. **HTTPS Everywhere.** Disponível em: <https://www.eff.org/https-everywhere>. Acesso em: 16 jun. 2020.

OVERLIER, L.; SYVERSON, P. **Locating hidden servers.** 2006. Disponível em: <https://www.onion-router.net/Publications/locating-hidden-servers.pdf>. Acesso em: 16 jun. 2020.

SIMONSEN, A. W. Privacidade e anonimidade na Internet. **Revista Jus Navigandi**, v. 19, n. 4.192, 23 dez. 2014. Disponível em: <https://jus.com.br/artigos/32143>. Acesso em: 16 jun. 2020.

TOR BLOG. **Bittorrent over Tot isn't a good idea.** 2010. Disponível em: <https://blog.torproject.org/bittorrent-over-tor-isnt-good-idea>. Acesso em: 16 jun. 2020.

TOR PROJECT. **How is Tor different from other proxies?** Disponível em: <https://www.torproject.org/docs/faq#Torisdifferent>. Acesso em: 16 jun. 2020.

TOR PROJECT. **The Onion Service Protocol.** Disponível em: <https://www.torproject.org/docs/onion-services.html.en>. Acesso em: 16 jun. 2020.

TOR PROJECT. **The Tor relay guide.** Disponível em: <https://community.torproject.org/relay/>. Acesso em: 16 jun. 2020.

TOR PROJECT. **Tor Project.** Disponível em: <https://www.torproject.org/index.html.en>. Acesso em: 16 jun. 2020.

GLOSSÁRIO

VPN	Virtual Private Network (VPN), ou rede privada virtual, é uma rede de comunicações privada construída sobre uma rede de comunicações pública (como, por exemplo, a Internet). Simplificadamente, pode ser vista como uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.
AdBlock	Extensão para filtragem de propagandas, instalada em navegadores web.
Entry guards	Relés escolhidos aleatoriamente pelo cliente Tor como ponto de inserção na rede Tor. São utilizados apenas para o primeiro *hop*.
Ghostery	Extensão para navegadores relacionada à privacidade e segurança.
Hypervisor	Software, firmware ou hardware destinado a criação e gerenciamento de máquinas virtuais.
One-time secret	Forma segura para compartilhamento de informações sigilosas que permite acesso a essas informações uma única vez.
Tor bridge	Relé Tor não listado em seu diretório principal.
Torrent tracker	Servidor que auxilia na comunicação entre dois computadores que utilizam o protocolo P2P BitTorrent.