Anonimização e Redes Escuras

José Pedro Silva, José Ricardo Cunha, and Válter Carvalho

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a84577,a84302,a84464}@alunos.uminho.pt

Resumo É dado a conhecer um pouco do que são as redes escuras, em função da sua importância e relevância na Internet, as suas conotações, isto é, o que a sua existência implica assim como a razão de ter sido criada e, também, o contexto atual, ou seja, a forma como se enquadra na sociedada hodierna. É também abordado maneiras de anonimização do tráfego *online*, como a utilização de VPNs e de *Onion Routing*. São abordadas medidas de segurança para utilizadores que pretendem navegar de forma segura e discreta a Internet, assim como práticas que devem tomar para manter a sua privacidade protegida *online*.

1 Introdução

A Internet é algo que já faz parte do dia à dia da maioria das pessoas. Neste momento, mais de quatro mil milhões de pessoas tem acesso à mesma, e esse número continua a aumentar diariamente, pois estima-se que apenas cerca de 40% da população mundial tem acesso à Internet[1]. No entanto, a maioria destas pessoas acedem a apenas uma baixa percentagem da mesma, à *World Wide Web*. Existe uma outra parte, as *Redes Escuras*, que tomam a maior percentagem da Internet (cerca de 500 vezes maior que a anterior), que não são facilmente acessíveis, devido a serem propositadamente escondidas por motivos de segurança ou por motivos de sigilo (explorado em 2.2), cujo propósito possa ser objetivos criminais ou, simplesmente, a garantia da privacidade que é dada.

Há uma crescente preocupação acerca da privacidade dos usuários *online*, devido a diversas ocasiões[2] em que dados de utilizadores são *leaked* sem que estes tenham conhecimento nem forma de o controlar, visto que são, geralmente, brechas na segurança de uma determinada empresa, sejam estas devido a incompetência ou devido a *exploits* nas bases de dados. Há várias formas de um utilizador manter a sua privacidade *online*, dado que partilhar o mínimo de informação pessoal é a base para uma "vida saudável"na Internet, que, aliada a outros métodos, explorados de seguida, levam a um possível anonimato por completo, ou seja, uma utopia alcançável através de métodos modernos de encriptação de conexões, como VPNs ou até mesmo *Onion Routers*[3].

2 Camadas da Internet

A Internet, como a conhecemos, está fragmentada por níveis, em que a dificuldade de obtenção de informação aumenta exponencialmente à medida que "descemos"de camada, cada uma com as suas características. É composta principalmente pela *"Surface Web"* (2.1), *"Deep Web"* (2.2) e *"Dark Web"* (2.3), que representam respetivamente uma divisão lógica por conteúdo que mantêm na sua alçada e com limites bem estabelecidos e controlados.

[1] De acordo com https://www.internetlivestats.com/internet-users/
[2] Facebook *data leaks* (2018), Adobe *data breaches* (2013), entre outros.
[3] O mais conhecido e popular é o Tor.

Divisão por Camadas da Internet[4].

2.1 Surface Web

A primeira camada, comummente referida como "*Surface Web*"é a parte mais acessível da Internet, cuja informação está indexada e, portanto, é reconhecível pelos motores de busca disponíveis (Google, Yahoo, Bing, ...). É estimado que 4% de toda a Internet se encontra nesta camada e, que apesar da sua pequena percentagem, existem mais de 1.5 mil milhões de websites[5] disponíveis e acessíveis através de *browsers* padrão, como o Google Chrome e o Mozilla Firefox.

O indexamento de páginas é possível através de *links*. Através destes, cada página é indexada de acordo com pertinência, títulos, *links*, entre outros. Após o pedido de pesquisa a um motor de busca, este procura por todas as páginas e subsequentes *links* nela embutidos por palavras chave, retornando os resultados para o utilizador conforme a relevância.

2.2 Deep Web

A segunda camada é conhecida por *"Deep Web"*, que aglomera um total aproximado de 90% de toda a Internet. Esta é considerada a sua parte "invisível"porque a maior parte do seu conteúdo não é acessível por motores de busca tradicionais . Isto deve-se ao facto de as páginas nesta camada não estarem indexadas, o que leva a que a que as mesmas não sejam visiveis nas *SERPs*[6]. Por exemplo, grande parte das vezes que se procura algo no catálogo de uma loja *online*, o utilizador acede indiretamente à *"Deep Web"*, visto que é informação armazenada nos servidores da empresa e, consequentemente, não têm *links* indexados aos motores de busca.

Ao contrário do que é a sua reputação, esta camada não possui apenas acesso a atividades ilegais. Inclui, maioritariamente, conteúdo intencionalmente escondido, com o intuito de não divulgar facilmente informação que poderia ser utilizada para propósitos nefastos,

[4] Imagem retirada de https://hackercombat.com/wp-content/uploads/2018/02/Deep-Web-and-Dark-Web-Explained-1.png/

[5] https://www.internetlivestats.com/total-number-of-websites/

tal como informações acerca de contas de e-mail, redes sociais, bancárias, etc dos respetivos utilizadores, assim como bases dados de empresas/organizações, registos médicos, documentos legais, entre muitos outros.

2.3 Dark Web

A terceira camada é frequentemente referida como a *"Dark Web"*. Esta camada é confundida como sendo a *"Deep Web"* e que causa a sua má reputação, quando na verdade é apenas uma fração minúscula dela (cerca de 6% da *"Deep Web"* e 5% de toda a Internet), em que é onde se tem levantado uma crescente preocupação mundial acerca do conteúdo partilhado nesta camada, devido à intensa atividade criminal.

Esta camada é o local cujo conteúdo só pode ser acedido por *browsers* específicos como o *Tor*, visto que é constituído por páginas não indexadas, cuja função é permitir a conexão, de forma anónima, a *URLs* tipicamente terminados em **.onion**. Para além de ser difícil de localizar as páginas, a maior parte estão bloqueadas por algum tipo de autenticação, de modo a manter o sigilo e a discrição destas e, evidentemente, a grande maioria destina-se a usos criminais, como a compra e venda de substâncias ilegais, contrato de *hitmen*, venda de dados pessoais, tráfego humano, entre muitos outros[7].

3 Anonimização

A privacidade *online* é um assunto cada vez mais recorrente. Uma das formas de manter essa privacidade passa por manter o tráfego *online* atrás da linha do anonimato. Existem várias razões para querer manter o anonimato *online*, as quais têm uma ampla variedade de motivos que vão desde objetivos mundanos, como a partilha de conteúdos mais sensíveis, a ilegais, como a venda de armas e drogas, sendo que os últimos são os que trazem mais razões para preocupação. Dito isto, o mercado respondeu a esta crescente necessidade por manter o anomimato *online*. As duas principais maneiras de o fazer são o uso das redes Tor e o uso dos VPN's (Virtual Private Network), às vezes até em conjunto.

3.1 Tor e o Anonimato

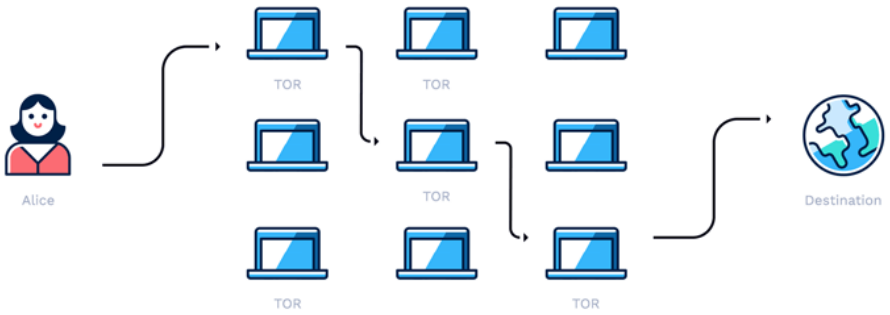
Tal como já foi referido anteriormente, o Tor é uma das maneiras mais comuns de manter o anonimato *online*, sendo que até passa a ser quase obrigatório para poder navegar na Dark Web. Mas como é que o Tor consegue manter o tráfego *online* das pessoas privado e como dificulta o rastreamento?

O Tor, para além de software, é uma rede retransmissão de tráfego administrada por voluntários por todo o mundo. Em primeiro lugar, o Tor tenta manter o anonimato ao passar a informação por várias camadas de encriptação. De seguida faz esta informação encriptada passar por múltiplos nodos de retransmissão que vão "descascando"essas várias camadas aos poucos (tal como uma cebola, daí o famoso símbolo da rede Tor). A única informação que é passada aos nodos é a qual nodo passar a informação a seguir. Desta maneira, não só se esconde a informação através da encriptação, como também torna difícil o rastreamento dos endereços de IP dos usuários, já que essa informação vai passar por vários outros endereços.

---

[6] Search Engine Results Pages

[7] O caso mais notável foi a *"Silk Road"*, que era um mercado para virtualmente qualquer item que fosse ilegal.



Modelo (simples) do funcionamento do Tor[8].

No entanto, no final a informação vai ter de sair da rede Tor para ir para o seu destino através do nodo de saída. A partir desse ponto a informação já não está encriptada, por isso, apesar de ser muito difícil ligar essa informação a alguém, o operador do nodo de saída e o site ao qual se está a conectar consegue ter fácil acesso à informação e a quaisquer dados pessoais nela incluídos.

3.2 Redes privadas virtuais (VPN)

Os VPN's no fundo são uma conexão de um indivíduo a um servidor maior. O que eles fazem é criar um "túnel"através do qual a informação passa. Este cria uma camada de segurança que termina imediatamente o tráfego de dados caso seja detetada uma intrusão, e volta reconectar de volta ao servidor usando um caminho diferente para evitar ponto(s) comprometidos ou até mesmo abortando o caminho anterior na totalidade. Para além da informação vir já encriptada, alguns até usam métodos como o uso de vários caminhos para passar os dados.

Apesar de terem originado para usos empresariais, os VPN's estão a ser cada vez mais usados pela população em geral, já que estes serviços já se encontram ao seu alcance com empresas como "ExpressVPN", "Tunnel Bear"ou "NordVPN"e, pela facilidade de utilização, tornam-se alvo de imensos consumidores, atualmente. É uma forma eficaz de manter o anonimato *online* sem entrar em requisitos técnicos avançados.

3.3 Atividades Ilegais

Apesar da Deep Web ter os seus usos legais, uma boa parte do tráfego é por motivos ilegais. Existe uma grande variedade de oferta neste mercado negro *online*, que vai desde a venda de drogas e armas, à venda de serviços de assassinos a contrato e sequestradores. Já existem vários exemplos deste tipo de sites na Dark Web, alguns deles já extintos. Veja-se o caso do "Silk Road", uma espécie de mercado negro virtual que se especializava na venda de substâncias ilícitas, mas que vendia de tudo desde software pirateado e produtos roubados, a armas e serviços especializados. Este *website* foi encerrado em Setembro de 2013, no entanto, entretanto já foram lançadas várias "sequelas"como "Silk Road 2.0"e "Silk Road 3 Reloaded".

Todos estes mercados precisam de uma maneira segura de transferência de dinheiro, sendo que a maioria deles recorre à *"Bitcoin"* e a outras moedas virtuais encriptadas, pela simples razão de garantir anonimato a tanto o comprador como o vendedor, porque não recorre a identificadores pessoais.

[8] Imagem retirada de https://www.hotspotshield.com/what-is-a-vpn/tor-vs-vpn.

De modo a combater o crescimento de atividades ilegais na *"Dark Web"* por grupos ou organizações, foram criadas *task-forces* a nível mundial, cujo propósito é parar a distribuição e/ou promoção de conteúdos ilícitos. Uma destas operações foi chamada de *Operation Onymous*[9] que, citando a *Europol*, é definida como: "Law enforcement and judicial agencies around the globe undertook a joint action, coordinated by Europol's EC3, the FBI, ICE, HIS and Eurojust, against dark markets running as hidden services on the Tor network. The action aimed to stop the sale, distribution and promotion of illegal and harmful items, which were sold on online dark marketplaces.". Teve como resultados, citando novamente a *Europol*, "10 hidden services taken down. 17 vendors and administrators arrested. USD 1 million worth of Bitcoins, EUR 180,000 in cash, drugs, gold and silver seized."[10]

4 Conclusão

Tendo presente estas distinções entre camadas e sabendo que é muito difícil entrar em contacto com conteúdo ilícito, porque este predomina em locais muito dificilmente acessíveis, é simples manter uma boa prática de navegação *online* sem entrar em especificações demasiado técnicas, nem custos extremos monetários, isto é, basta apenas bom-senso e um sentido crítico na partilha de dados pessoais na Internet.

Para um usuário "normal"[11], manter uma subscrição de VPN (ou utilizar um que tenha planos gratuitos) é essencial na preservação da identidade pessoal, como o mascaramento de IP e, consequentemente, ocultação da localização geográfica. Nesta prática, não é necessário o acesso ao Tor, apesar do enorme anonimato que este fornece, devido ao caráter perigoso inerente. Basta permitir a execução de um mini-programa dentro deste *software* de forma inocente para causar danos irreparáveis, não só à maquina ligada à Internet, como também à privacidade, pelo que o sujeito nesta situação pode ser vítima de roubo de identidade. É um risco desnecessário para atividade em Internet do dia-a-dia (redes sociais, pesquisas, leitura de artigos,...), que não exige um grau de privacidade tão alto como *Onion Routing*.

Por fim, o usuário não deve de forma alguma colocar informação desnecessária *online*. As redes sociais são especialmente culpadas neste aspeto, porque incentivam à partilha de *data* por parte do utilizador e, como tudo fica catalogado e indexado, diminuem exponencialmente o anonimato do indivíduo. Para além disto, as empresas podem ter *data breaches* e quanto mais informação desnecessariamente partilhada for descoberta, pior o estado de anonimato da pessoa enquanto consumidor. Isto leva a que, atualmente, o anonimato não seja uma realidade absoluta, pelo que deve haver uma crescente preocupação do usuário de modo a manter os seus direito e liberdade na Internet.

Em suma, não é necessário recorrer a mecanismos de anonimato tão sofisticados, como o Tor, quando uma "boa higiene"*online* (usar VPN e fazer pouca dispersão de dados pessoais) assegura um nível de privacidade satisfatório, assim como segurança e tranquilidade de que os utilizadores não estão a ser vigiados constantemente, para efeitos de navegação comum na Internet.

Referências

1. Kristin Finklea: Dark Web, *Congressional Research Service* (2017)
2. Ken Yeung: What is Tor and Why Does It Matter?, *Insider* (2013)
3. Computer Hope: What is a Search Engine (2019)
4. Corianna Jacoby, Ming Chow: The Onion Router and the Darkweb (2016)

[9] O nome vem de remover o *An* de *Anonymous*, isto é, remover privilégios de privacidade a grupos com propósitos criminais.

[10] Esta informação foi retirada de: https://www.europol.europa.eu/activities-services/europol-in-action/operations/operation-onymous.

[11] Que utiliza apenas a "Surface Web".

5. Andy Greenberg: Hacker Lexicon: What Is the Dark Web?, *Wired.com* (2014)
6. David Goldschlag, Michael Reed, Paul Syverson: Onion Routing for Anonymous and Private Internet Connections (1999)
7. Roger Dingledine, Nick Mathewson, Paul Syverson: Tor: The Second-Generation Onion Router (2004)