Darknets e Anonimato

Rui Oliveira[a95254], Luís Pereira[a96681], and Guilherme Sampaio[a96766]

Universidade do Minho

Resumo Ensaio sobre as darknets e formas de preservar o anonimato ao navegar na internet

Keywords: Darknets · Anonimato · TOR · VPN

1 Introdução

Com o crescimento da internet ao longo das últimas décadas está também associado o crescimento de redes ocultas, denominadas por *darknets*, não acessíveis por métodos *tradicionais*, como através de motores de busca. A principal preocupação destas redes está em manter o anonimato dos seus utilizadores e dos conteúdos que nelas circulam.

Existem diferentes tipos de *darknets*, por exemplo, redes *Tor* e *Peer to Peer*, que serão exploradas em detalhe neste ensaio. Também iremos explorar formas de um utilizador da rede se manter anónimo, em particular através da utilização de redes privadas virtuais (VPNs).

2 *Darknets*

Todos sabemos que, assim como as montanhas, os icebergues são muito mais extensos abaixo da superfície. A *Internet* tem exatamente as mesmas caraterísticas e pode ser dividida em *Open Web* (no topo), *Deep Web* (a meio) e *Dark Web* (no fundo). Este último nível e parte dos níveis acima são designados por *Darknet* são normalmente apenas acedidos através de ferramentas especializadas e representam cerca de 96% de toda a rede conhecida. Normalmente, este nível mais profundo é usado por utilizadores com intuitos ilegais. [5].

A *Darknet* (também escrita *"Dark Net"*) é um termo que muitas vezes ouvimos falar, porém vagamente definido. Frequentemente, quando falamos neste tipo de rede, referiremo-nos a uma área da *Internet*, acessível, por exemplo, através da utilização de uma ferramenta de encriptação chamada *"The Onion Router"* (TOR). O método de *Onion Routing* é, sem dúvida, o mais conhecido, porém existem outros como, conexões *peer-to-peer* ou *friend-to-friend* (um subtipo de redes *peer-to-peer*). Todos estes métodos de acesso à *Darknet* serão discutidos em detalhe nos próximos capítulos.

A ideia de *Darknet* é muitas vezes suportada sob três princípios [1]:

- Independentemente do objeto (*software*, músicas, filmes, livros, etc.), este está disponível para alguns utilizadores sob uma forma que permita a sua cópia.
- Os utilizadores irão copiar tais objetos se for possível e favorável.
- Os utilizadores estão conectados entre si através de canais de alta largura de banda.

Tendo isto em conta, podemos, de certa forma, definir *Darknet* como uma rede de distribuição que apenas se mantém devido à injeção de objetos e à sua mesma distribuição/partilha.

Convém distinguir o conceito de *Darknet*, que foi acima explicado, com o conceito de *Dark Web*. A *Dark Web* é o conjunto de sites da *Darknet* ligados a atividades criminosas, tais como tráfico de droga ou de armas.

Figura 1. Camadas da *Internet* [4]

3 *Onion Routing*

Uma das formas de manter o anonimato na *Internet* surgiu em meados da década de 1990 e consiste na utilização de roteamento em cebola (em inglês, *onion routing*). Este procedimento consiste em três fases [7]. Inicialmente, a conexão é preparada, isto é, o remetente da mensagem decide um caminho entre várias máquinas que esta vai fazer até chegar ao seu destinatário; contrariamente a uma ligação *tradicional*, onde a mensagem é enviada diretamente do remetente para o destinatário. Este caminho é armazenado numa estrutura de dados recursiva normalmente designada por *onion*, em que cada camada contém informação sobre as propriedades da conexão em cada ponto do caminho.

De seguida, o remetente partilha chaves de encriptação simétricas com cada um dos nodos da rede e encripta a mensagem que pretende enviar sucessivamente com essas chaves. Seguidamente, a mensagem é enviada para o primeiro nodo. Aí, essa máquina desencripta a primeira camada usando a sua chave (sendo a única à qual tem acesso), e revela a informação relativa ao próximo elemento no caminho, ao qual envia a mensagem desencriptada. Este processo repete-se, até a mensagem chegar, desencriptada ao seu destino.

Deste modo, cada elemento da rede nada mais sabe acerca desta senão o nodo imediatamente anterior e seguinte a ele mesmo. Não sabe, inclusive, se é o primeiro ou o último elemento da rede. Isto garante, naturalmente, o anonimato do remetente da mensagem.

3.1 O navegador TOR

A implementação mais famosa deste conceito é o projeto Tor (acrónimo para *The Onion Router*), que teve início em 2006 como uma organização sem fins lucrativos [11]. Os serviços Tor são considerados um dos melhores e mais populares para impor o anonimato do utilizador e, como dito acima, baseia-se em *onion routing*. Isto, porém, não significa que estes sejam infalíveis no que toca ao anonimato, pois, atualmente, existem diversos pesquisadores cujo objetivo é a desanonimização, cerca de 55% do total de pesquisadores

relacionados com o projeto Tor. Para além disso, alguns estudos mostram que quantos mais utilizadores estiverem ativos em simultâneo, menor é a segurança da rede, devido à quantidade de servidores por onde a informação circula ser limitada, assim, a informação não poderá ser encaminhada por tantos pontos.[9].

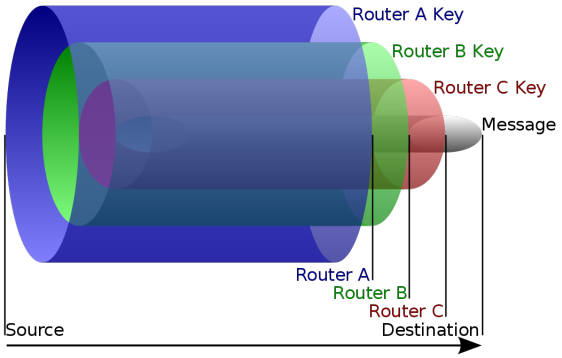

Figura 2. Onion Routing[14]

4 Redes *Peer-to-Peer*

4.1 *Friend-to-Friend*

Outra forma de um utilizador se manter anónimo na *Internet* é através de uma rede *anonymous friend-to-friend*, nesta categoria de rede cada utilizador tem uma lista de "amigos"dos quais recebe informação e aponta quem lhe deu o quê. Posteriormente, repartilha para os seus amigos o que recebeu sem partilhar quem forneceu os dados. Desta forma sempre que alguém faz um pedido este vai percorrer vários nodos até chegar ao destino sendo que como cada utilizador só sabe quem está na sua lista de amigos, os nodos intermédios só sabem o seu antecedente e assim não é partilhada a informação de onde foi feito o pedido.[10]

Como a informação fornecida por um amigo a alguém é repartilhada por todos os seus outros amigos, é possível observar que esta rede cresce muito rapidamente.

Este tipo de conexões, no entanto, tem um problema severo visto que a informação do IP original de quem executa pedidos não existe, logo, é impossível criar uma *blacklist* de IP's para combater ataques do tipo DoS (*Denial of Service*).

4.2 *Tarzan*

Um exemplo de uma rede *Peer-to-Peer* é o *Tarzan* que para garantir o anonimato dos utilizadores tira proveito do uso de caminhos pseudo-aleatório entre nodos, encriptação entre dois nodos, a transmissão de informação inútil para encobrir as verdadeiras transmissões de dados e tradutor de endereços IP para criar uma ligação entre o *Tarzan* e a rede de *Internet* tradicional. [8].

4.3 *Torrenting*

Torrenting refere-se a partilha de ficheiros através de uma conexão *friends-to-friends* descentralizada. Partilha por conexões *friends-to-friends* permite utilizadores a trocarem ficheiros sem os carregarem para servidores sendo estes enviados diretamente para o utilizador final. Este serviço, no entanto, mostra para todos na rede quem está nela tendo assim uma falta de segurança [3].

5 Anonimato

5.1 *Virtual Private Networks*

Uma maneira de anonimizar o tráfego na internet consiste na utilização de uma rede virtual privada (VPN, do inglês, *virtual private network*). Uma VPN consiste numa rede privada construída dentro de uma rede pública, como a internet global [12].

Por outras palavras, para um utilizador se conectar à internet através de uma VPN, liga-se a uma máquina intermediária que se liga pelo utilizador ao *site* pretendido, e devolve os conteúdos. Isto adiciona uma camada de segurança à ligação, visto que a ligação à máquina intermediária é também ela encriptada (resultando em pacotes IP encapsulados noutros pacotes IP), permitindo acesso seguro à internet mesmo em redes não seguras e também o acesso a sites bloqueados.

Além da sua utilização para anonimizar o tráfego, nomeadamente do provedor de serviço (ISP), VPNs também podem ser usadas para permitir um utilizador aceder a uma *intranet* remotamente, o que pode ser utilizados por empresas para que os seus funcionários se conectem à sua rede interna a partir de casa.

Uma outra vantagem de VPNs para um utilizador final está na possibilidade de superar limites geográficas a conteúdos, isto é, quando um serviço Web bloqueia o acesso a certos conteúdos a utilizadores de certas zonas geográficas. Como o endereço de IP que o sítio de destino vê corresponde ao IP da máquina que hospeda a máquina virtual e não a do utilizador da mesma, este consegue acesso aos conteúdos dessa zona geográfica.

5.2 *Fingerprinting*

O conceito *fingerprint* tem um significado similar tanto no mundo real como no mundo digital. Em termos de cibersegurança uma *fingerprint* (também conhecida como *footprint*), é um grupo de informação que pode ser usada para obter diferentes tipos de dados tais como programas a serem utilizados, protocolos de redes (*network protocols*), sistemas operativos ou dispositivos de *hardware* do utilizador.

Fingerprinting é o método cujo objetivo é acumular a maior quantidade de informação possível sobre um alvo. Normalmente este mecanismo é usado quando precisamos de saber tudo (num nível digital) sobre alguém e, após a sua execução, conseguimos utilizar a informação obtida para correlacionar diferentes conjuntos de dados para identificar as especificações de *software* usado pelo utilizador, qual o sistema operativo, etc. Após a identificação, podemos explorar métodos para explorar (*exploit*) ao alvo.

Assim como existem diversas maneiras de extrair informação através da impressão digital de um humano, no mundo digital, existem pelos dois métodos principais de *fingerprinting*, ativo e passivo.

***Fingerprinting* Passivo** [2]: é uma abordagem segura e capaz de evitar deteção, pois, contrariamente à versão ativa, não são enviados pacotes ao sistema do alvo. Em vez disso, esta abordagem age como um *scanner* da rede (*sniffer*), ou seja, não são enviados/alterados nenhuns tipos de dados. Quando o agente

atacante obtém informação suficiente é possível extrair padrões que podem ser úteis na deteção de sistemas operativos ou aplicações.

***Fingerprinting* Ativo** [2]: é a abordagem mais popular e, contrariamente ao passivo, permite a deteção do atacante, pois consiste no envio de pacotes de dados para o alvo de modo a receber uma resposta, cuja análise pode levar a resultados importantes sobre o alvo. É um dos melhores métodos de deteção de sistema operativo, serviços e rede. A razão pela qual os atacantes têm de esconder a sua identidade é devido à existência de sistemas de deteção de intrusão (IDS) e de barreiras de segurança (*firewalls*) que filtram específicos pacotes de dados que levam à sua identificação.

Atualmente, e dada a proliferação da utilização desta técnica, já existem navegadores que implementam mecanismos de proteção contra este [13], de forma a proteger o anonimato dos seus utilizadores. Também existe investigação no sentido de desenvolver software que o bloqueia de forma ativa e dinamicamente, isto é, enquanto o utilizador navega a internet e em função dos pedidos que a sua máquina [6].

6 Conclusão

Neste ensaio foi possível explorar alguns exemplos de redes que podem ser consideradas *darknets*, bem como formas de manter o anonimato ao navegar na internet. O foco do trabalho prendeu-se em apresentar vários exemplos e, dado o limite de palavras, não é possível explorar todos os tópicos com muito detalhe.

Resumindo, existem diferentes tipos de *darknets*, com usos distintos, como a rede *Tor* e redes *peer-to-peer*, assim como formas de anonimizar o tráfego na internet, nomeadamente através da utilização de redes privadas virtuais e de mecanismos que dificultem o *fingerprinting* do tráfego de um utilizador da rede.

Com o aumento da tendência de recolher o máximo de informação sobre os utilizadores de um dado website, a utilização destas técnicas para manter o anonimato e privacidade ao navegar em rede tornam-se cada vez mais relevantes.

Referências

[1] Peter Biddle et al. ≪The Darknet and the Future of Content Protection≫. Em: *Digital Rights Management*. Ed. por Joan Feigenbaum. Berlin, Heidelberg: Springer Berlin Heidelberg, 2003, pp. 155–176. ISBN: 978-3-540-44993-5.

[2] ESTEBAN BORGES. Mai. de 2019. URL: `https://securitytrails.com/blog/cybersecurity-fingerprinting`.

[3] S. A. (2015) Chrane C. Kumar. *An examination of tor technology based anonymous internet. Proceedings of Informing Science & IT Education Conference*. [Online; accessed 22-February-2022]. 2015. URL: `http://Proceedings.InformingScience.org/InSITE2015/InSITE15p145-153Chrane1636.pdf`.

[4] *Dark web and its impact on your organization*. Fev. de 2022. URL: `https://sstech.us/blogs/dark-web-impact-on-organization/`.

[5] Pallavi Duttahttps. *Surface web and dark web: Exploring layers of web*. Mar. de 2021. URL: `https://www.kratikal.com/blog/surface-web-and-dark-web-exploring-layers-of-web/`.

[6] Amin FaizKhademi, Mohammad Zulkernine e Komminist Weldemariam. ≪FPGuard: Detection and Prevention of Browser Fingerprinting≫. Em: *Data and Applications Security and Privacy XXIX*. Ed. por Pierangela Samarati. Cham: Springer International Publishing, 2015, pp. 293–308. ISBN: 978-3-319-20810-7.

[7] Syverson P. Goldschlag D. Reed M. ≪Onion Routing for Anonymous and Private Internet Connections≫. Em: *The Onion Router* (1999).

[8] Robert Morris Michael J.Freedman. ≪Tarzan: a peer-to-peer anonymizing network layer≫. Em: *The ACM Digital Library* (2002).

[9] Murat Ozer et al. URL: https://www.researchgate.net/publication/340810728_Plunge_into_the_Underworld_A_Survey_on_Emergence_of_Darknet.

[10] V. Scarlata, B.N. Levine e C. Shields. ≪Responder anonymity and anonymous peer-to-peer file sharing≫. Em: *Proceedings Ninth International Conference on Network Protocols. ICNP 2001.* 2001, pp. 272–280. DOI: 10.1109/ICNP.2001.992907.

[11] *The Tor Project.* http://web.archive.org/web/20080207010024/http://www.808multimedia.com/winnt/kernel.htm. Accessed: 2022-02-19.

[12] *What is a VPN?* https://www.cisco.com/c/dam/en_us/about/ac123/ac147/archived_issues/ipj_1-1/ipj_1-1.pdf. Accessed: 2022-02-22.

[13] *What is fingerprinting and why you should block it.* https://www.mozilla.org/en-US/firefox/features/block-fingerprinting/. Accessed: 2022-02-25.

[14] Wikipedia contributors. *Onion routing — Wikipedia, The Free Encyclopedia.* [Online; accessed 22-February-2022]. 2022. URL: https://en.wikipedia.org/w/index.php?title=Onion_routing&oldid=1073182922.