Darknets e Anonimização

Beatriz Rodrigues[a93230], Francisco Neves[a93202], and Guilherme Fernandes[a93216]

Departamento de Informática
Universidade do Minho, Braga
http://www.di.uminho.pt

Resumo O presente ensaio centra-se em duas *Darknets*, *Tor* e *i2p*, nas suas semelhanças e diferenças, nas suas potencialidades e incovenientes e, por fim, nas ligações existentes entre elas.

Keywords: Darknet · Anonimização · Hidden Services.

1 Introdução

A Internet normalmente conhecida com motores de busca como o *Google* ou o *Bing* representa uma pequena parte da verdadeira Internet, sendo que esta é, geralmente, denominada por *Surface Web*. Além desta, existe ainda a *Deep Web*, caracterizada por não ter os seus conteúdos indexados nos motores de busca tradicionais, embora possam ser visitados através dos seus URLs em *browsers* ditos comuns.

Por fim, dentro da *Deep Web* existe ainda a *Dark Web/Darknet*. Esta caracteriza-se pela necessidade da utilização de *software* específico, tal como o *Tor* (The Onion Router) ou *i2p* (Invisible Internet Project), para aceder ao seu conteúdo.

2 Contextualização

A utilização da *Darknet* ao longo dos tempos tem vindo a apresentar um aumento, isto deve-se, em parte, às suas potencialidades, quer pelo lado positivo, quer pelo lado negativo.

Tendo em conta este software, é dada uma liberdade muito grande ao utilizador, permitindo-o navegar através de domínios obscuros e, até mesmo, de efetuar atividades consideradas criminosas em grande parte dos territórios do nosso globo. Na *Darknet* apenas o utilizador é responsável pelas suas ações, visto que os softwares como o *Tor* ou o *i2p* não lhe bloqueiam atividades que os *browsers* normais bloqueariam.

No entanto, não seria correto efetuar uma breve análise às *Darknets* sem sermos capazes de ver os seus pontos positivos, como a anonimização dos seus clientes e a fuga ao bloqueio de domínios que algum regime opressivo possa considerar prejudiciais ao seu totalitarismo. Como podemos ler em 1984[4] de George Orwell, "Those who control the present, control the past and those who control the past control the future." e, através da desinformação, tornamos possível este cenário algo que, através da utilização das *Darknets* somos capazes de evitar.

3 *Darknets*

Darknet pode referir-se a diversas coisas, sendo que, essencialmente representa o espaço da Internet que se encontra escondido por design através de encriptação ou de diferentes tecnologias sobrepostas de *routing* (encaminhamento).

Esta tecnologia de rede encriptada utiliza a infraestrutura da Internet e os seus conteúdos apenas podem ser acedidos utilizando uma configuração de rede e ferramentas de software especiais, não estando presentes nos motores de busca usuais.

A *Darknet*, sobretudo nos últimos tempos, tem estado ligada a diversas atividades criminosas e ilegais.

3.1 The Onion Router

Tor, "*The Onion Router*", desenvolvido em meados dos anos 90 pelos funcionários do Laboratório de Pesquisa Naval dos Estados Unidos, é um software bastante popular para este fim que já sofreu diversas investigações, possui mais de 2 milhões de utilizadores diários e mais de 6000 *relays*.

Estes últimos são responsáveis por assegurar que a rede funciona mantendo um grande nível de privacidade. Tendo em conta os valores elevados apresentados, pressupõe-se que exista uma comunidade bastante grande e ativa na manutenção e atualização deste *software*.

Nesta ferramenta, é possível criar *Websites* e *Hidden Services* disponíveis apenas aos utilizadores que se conectem através da rede do *Tor*. Inicialmente, era pretendido servir como uma forma de liberdade de expressão, no entanto, acabou por ser, maioritariamente, utilizado para a execução/preparação de atividades criminosas e ilegais.

Onion Routing é a técnica de comunicação anónima *peer-to-peer* adotada pelo *Tor*, esta funciona de forma análoga às camadas de uma cebola.

Numa *onion network* os dados são encapsulados em camadas de encriptação. Estes dados são transmitidos por uma série de *onion routers*, cada um deles remove um nível de encriptação e envia ao próximo. Os dados têm tantos níveis de encriptação quanto o número de *routers* existentes entre o transmissor e o destinatário, logo, quando a última camada de encriptação for removida, a mensagem chega ao seu destino.

Como cada nodo intermediário apenas conhece a localização dos seus nodos anterior e posterior, e as redes *Tor* normalmente contêm centenas de nodos, o transmissor mantém-se anónimo para a maior parte dos atacantes.

Existe, no entanto, uma forma de quebrar este anonimato, conhecida como *timing analysis*. Apesar do *onion routing* esconder o caminho entre uma pessoa e o website que esta está a aceder, os ISPs têm acesso aos registos das conexões, ao tempo em que ocorreram e à quantidade de dados transferidos; assim é possível analisar estes registos do lado do transmissor e do recetor, comparando-os.

3.2 Invisible Internet Project

O *i2p*, "*Invisible Internet Project*", oferece *eepsites*, que são *websites* e serviços apenas disponíveis na sua *Darknet*.

Ao contrário do *Tor*, o *i2p* encripta toda as comunicações *end-to-end*, ou seja, nenhuma informação é enviada sem encriptação, e não é desencriptada no seu caminho; além disso, não depende de uma base de dados centralizada e utiliza *garlic routing*.

Por utilizar um *packet based routing*, o *I2P* evita congestões e interrupções do serviço, tal como o IP routing da Internet. Para além disso, as *routes* da rede são formadas e constantemente atualizadas, visto que os *routers* avaliam-se entre si e atualizam a informação disponível.

Esta *Darknet*, embora menos conhecida, é mantida em constante desenvolvimento, o que indica que existe uma quantidade significativa de utilizadores.

Esta é usada por aplicações que são escritas especificamente para a rede *I2P*. Exemplos podem ser mensagens instantâneas, partilha de ficheiros, *emails* e aplicações distribuídas de armazenamento.

Garlic Routing é a uma variante do *onion routing*, que, encriptando várias mensagens juntas, aumenta a velocidade de transferência e diminui a vulnerabilidade da conexão a *traffic analysis*.

3.3 Interligação entre Darknets

As **LEAs** (*law enforcement agencies*), de forma a tentar impedir atividades ilegais, têm investigado as *Darknets* com a finalidade de poderem relacionar os dados obtidos entre elas.

No artigo "Interconnection Between Darknets"[1] de Cilleruelo, C. et al. foi construído um "mapa" da *Darknet* com os dados obtidos entre o *i2p*, o *Tor* e as ligações presentes entre eles. Através de técnicas de análise de grafos estudaram-se ainda os atores e os serviços mais relevantes de cada rede.

Pôde-se concluir que o Tor não possui qualquer servidor público de DNS, utilizando antes um serviço denominado *Hidden Service DirecTory* (HSDir). Alguns dos seus *relays* são marcados com a *flag* **HSDir**, indicando que estes domínios guardam informação acerca de hidden services.

Os resultados do estudo mostram que a maior parte dos *websites* populares do *Tor* focam-se em indexar domínios (o *Tor* não possui um índice público dos diversos domínios escondidos que possui, então, são várias vezes os próprios sites que mantêm uma lista de domínios possíveis). Por outro lado, quanto ao *i2p*, os domínios mais importantes são sites de *jump* e *proxy* (devido à maneira que o *i2p* funciona estes revelam-se muito importantes, pois, para aceder a qualquer *eepsite* é necessário utilizar um *jump*, visto que este atua de forma análoga a um serviço DNS para os domínios *i2p*).

Além de tudo isto, foi ainda possível denotar que existe uma clara conexão entre o *i2p* e o *Tor* (e provavelmente entre outras *Darknets*). Desta forma, é importante que as *LEAs* possam utilizar isso de forma a tentar captar domínios de atividades ilegais.

No passado, as *LEAs* têm-se focado sobretudo na investigação do *Tor*, o que poderá provocar uma migração dos cibercriminosos para outras *Darknets*.

É ainda importante realçar que os serviços da *Darknet* são altamente voláteis, ou seja, mesmo que um domínio fique *offline* é muito provável que este seja substituído por outro com funcionalidades muito semelhantes. O *i2p* poderá ter uma posição importante em tornar os nodos do *Tor* alcançáveis.

4 Anonimização

Atualmente, softwares como o *Tor*, são utilizados para promover a liberdade de expressão, anonimato e privacidade. Desta forma, é útil para ativismo político e campanhas anti-censura, assim como para comunicação sensível (por exemplo, alguns negócios usam-no para protegerem-se e ganharem uma vantagem competitiva ou os casos de algumas pessoas que se sentem mais seguras para falarem sobre problemas pessoais).

Por outro lado, é ainda utilizado por jornalistas para garantirem comunicação mais segura com os seus informadores.

No entanto, como referido, a anonimização não é perfeita. Existem sempre investigadores e especialistas em segurança a desenvolver novas maneiras de a anular.

5 Utilizações das *Darknets*

As *Darknets* têm vindo a ser utilizadas para atividades ilegais. Exemplos disso são o facto de serem utilizadas para a distribuição de drogas, realização de tráfico sexual, roubo de identidades, venda de armas ou animais exóticos, entre outros. Há ainda uma forte componente relativa a sites de jogos de azar e assassinos a soldo, bem como de pornografia infantil.

No entanto, em algumas ocasiões, a utilização destas surge apenas devido à questão do anonimato que elas fornecem aos utilizadores, podendo assim tornar a navegação na rede privada e permitir buscas que de outra forma seriam bloqueadas ou testemunhos que poderiam não surgir devido a uma possível quebra da confidencialidade, como é o caso do *The New Yorker's Strongbox* que providencia anonimato e segurança à comunicação entre jornalistas e delatores ou dissidentes.

O FBI tem utilizado *malware* na tentativa de identificar utilizadores do *Tor*, nomeadamente cibercriminosos, predadores sexuais, entre outros. Para além disso, têm trabalhado em direção ao desenvolvimento de tecnologias que permitam a investigação de crimes e identificação de vítimas.

Os militares também utilizam a *Darknet*, com a finalidade de estudarem o ambiente em que estão envolvidos e descobrirem riscos para as tropas, como planos de atividades terroristas, uma vez que é um bom local para estes tipo de criminosos disseminarem a sua propaganda e recrutarem e angariarem dinheiro para as suas operações.

6 Pagamentos na *Darknet*

Nas transações na *Darknet*, as criptomoedas são, em geral, a moeda de troca.

Uma dessas moedas, a *Bitcoin*, tem sido utilizada por ser descentralizada e permitir o anonimato através de transações *peer-to-peer*. Quando esta é utilizada, a transação é registada na *Blockchain*. Nestas transações, os endereços dos utilizadores são associados com uma carteira e armazenados também numa carteira que detém uma chave privada, no entanto, estas podem ser *hosted* na *web* sem estarem diretamente associadas ao utilizador em registos, garantido assim a sua privacidade e anonimato.

7 Conclusão e o Futuro das *Darknets*

Tendo tudo isto isto em conta, é esperado que o interesse pelas *Darknets* venha a apresentar um crescimento ainda maior no futuro, ou seja, que estas venham a ser mais utilizadas parte do do utilizador comum, visto que o anonimato que estas lhes conferem traz diversas vantagens. Por outro lado, acreditamos que estas venham também a ser mais utilizadas por parte das forças policiais e por investigadores dos mais diversos campos, visto que estes procuram recolher cada vez mais dados.

Com a evolução das tecnologias, é essencial que as forças de segurança reforcem os seus campos de segurança informática e desencriptação, pois, de forma a conseguir combater os criminosos que beneficiam de melhorias na encriptação da atividade nestes softwares, é necessário que também estes possam evoluir as suas capacidades.

Referências

1. Cilleruelo, C., de-Marcos, L., Junquera-Sánchez, J., Martínez-Herráiz J.: Interconnection Between Darknets. Darknets/Alternative Networks, 61–70 (2021)
2. Adewopo V., Gonen B., Varlioglu S., Ozer M.: Plunge into the Underworld: A Survey on Emergence of Darknet. International Conference on Computational Science and Computational Intelligence, 155–159 (2019)
3. Finkle, K.: Dark Web. Congressional Research Service, 1–16 (2017)
4. Orwell, G.: 1984. Kindle Edition (2013)
5. Tor Project, `https://www.torproject.org`, Acedido pela última vez a 27 Fev 2022
6. I2P Anonymous Network, `https://geti2p.net`, Acedido pela úlima vez a 27 Fev 2022
7. Wikipedia, `https://en.wikipedia.org/wiki/Onion_routing`, Acedido pela última vez a 27 Fev 2022
8. Wikipedia, `https://en.wikipedia.org/wiki/Garlic_routing`, Acedido pela última vez a 27 Fev 2022
9. IVPN, `https://www.ivpn.net/privacy-guides/an-introduction-to-tor-vs-i2p/`, Acedido pela última vez a 27 Fev 2022