DarkNets and Anonymization

Bernardo Saraiva, Gonçalo Santos, and José Gonçalves

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
{a93189, a93279, a93204}@alunos.uminho.pt

Abstract. O presente documento tem como propósito a introdução e apresentação da temática "Darknets and Anonimization", focando no seu funcionamento e contextualização com a atualidade. Atualmente, a presente área poderá sofrer algumas distorções na sua interpretação, nomeadamente a confusão com alguns outros conceitos, o que será esclarecido nas secções seguintes. Apresentar-se-á também alguns projetos e propostas relevantes na área, assim como a explicação do funcionamento deste tipo de redes.

Keywords: Dark Net · Anonimization · Deep Web

1 Introdução e contextualização

Atualmente, a Internet está extremamente evoluída e desempenha um importante papel no quotidiano da grande maioria da população. Existem em todo o mundo cerca de 3,6 bilhões de pessoas que usam a Internet, ou seja 47% da população mundial navega na World Wide Web, utiliza redes sociais, paga as suas contas e até trabalha através da Internet. [1]

A maioria dos utilizadores da Internet conhece e sabe como usar a Internet, mas a utilização de motores de busca como Google, Bing, Yahoo, entre outras, também faz com que as grandes empresas e agências governamentais saibam o que os utilizadores fazem na Internet, assim como as suas informações e pesquisas. Ora, como todos sabemos, por vezes há informações que necessitam de ser mantidas em segredo, e várias plataformas são propositadamente desenvolvidas para se manterem desconhecidas e anónimas, quer seja por o seu conteúdo ser ilegal, obscuro ou secreto.

Para o acesso à DarkNet, fazendo justiça ao seu principio, é essencial que o utilizador se mantenha desconhecido por dois principais motivos: falta de segurança e secretismo da infomação. Deste modo, é geralmente usada a técnica de anonimização conhecida como onion routing, que será descrita nas secções seguintes.

2 Deep Web, DarkNet e Dark Web

Os conceitos de DarkNet, Dark Web e Deep Web têm origem na rede ARPANET, mas têm algumas dessemelhanças. Estes conceitos são frequentemente confundidos ou considerados sinónimos, sendo que geralmente se associa um negativismo

geral a todos eles. Deste modo, passar-se-á a explicar quais as diferenças entre estes três conceitos e quais as suas características e perigos. [2]

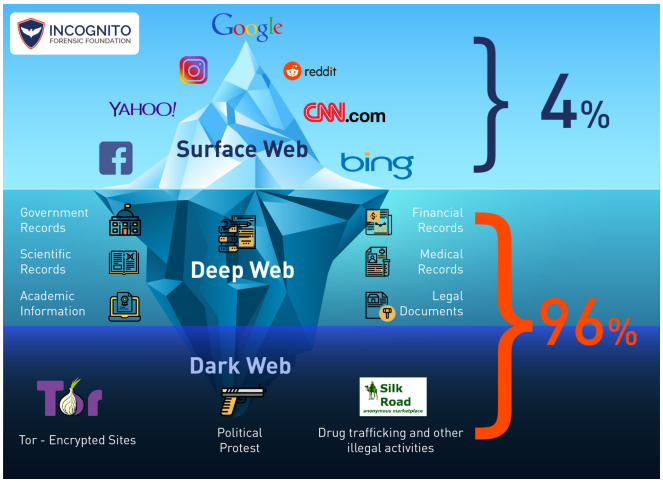

Fig. 1. Imagem exemplificativa da gestão da Web

2.1 Deep Web

A Deep Web é uma parte da World Wide Web que não se encontra indexada por motores de pesquisa convencionais e se encontra imediatamente abaixo da Surface Web. Para aceder a esta zona, no entanto, necessitam de uma autorização especial ou um link direto. É nesta zona da Internet que se encontram os bastidores da Web por conter dados cruciais para a manutenção da rede. Encontram-se nestes parâmetros bancos de dados académicos, registos médicos, informações confidenciais de segurança nacional, registos financeiros, artigos científicos, repositórios de algumas ONGs e etc.

2.2 DarkNet

A DarkNet é uma rede sobreposta *(overlay network)*, construída sobre a Internet regular, ou seja, todos os nodos são conectados entre si por meio de ligações lógicas ou virtuais e cada um deles corresponde a um caminho na rede subjacente (p.e. peer-to-peer e redes cliente-servidor). As DarkNets são apenas acessíveis a um grupo restrito de utilizadores, e por vezes apenas com autorização, software e configurações específicas, e foram desenhadas para garantir a anonimidade.

A DarkNet faz geralmente uso de protocolos de comunicação fora do comum, com vista a ser deliberadamente inacessível pela Internet convencional, pelo que se entrará em detalhe neste ponto nas seguintes secções. [3]

2.3 Dark Web

A Dark Web é um nome para os sites da DarkNet que contêm informação ilegal e bases de dados associadas a atividades criminais. Assim, podemos afirmar que esta parte da DarkNet é conhecida pela ausência de regras, pelo que é possivel encontrar os serviços e fóruns mais obscuros, como por exemplo contratar hackers, organizar crimes, comprar armas, drogas, documentos falsos, etc...

3 TOR - The Onion Router

Apesar da existência de várias ferramentas capazes de aceder à *DarkNet* e estabelecer conexões anónimas com o resto da rede, o *TOR(The Onion Router)* é certamente um dos mais conhecidos, isto devido à sua capacidade de implementar serviços escondidos na sua rede, ocultando assim a sua existência ao utilizador comum.

Esta ferramenta, como qualquer outro *browser*, permite ao utilizador navegar livremente na Internet, sendo que a única diferença imediata que se iria sentir seria a lentidão da ferramenta. Isto deve-se ao uso da rede *TOR*, que é usada neste cenário de forma a proporcionar ao seu utilizador anonimato na rede.[6]

Além desta funcionalidade mais quotidiana do *TOR*, onde esta tecnologia se destaca, poderá ser alcançada a implementação de serviços escondidos na rede, facilmente identificáveis pelo o seu sufixo *.onion*, sendo o seu nome derivado da estratégia usada para a criação de caminhos entre os nodos e garantir o anonimato, que se dá pelo nome de *Onion Routing*. Estes serviços só podem ser acedidos através desta ferramenta, visto que estão incorporados dentro da rede do *TOR*[5]. Os identificadores destes serviços não estão disponíveis ao público, e uma vez que são gerados pelo *TOR*, fazem com que apenas pessoas com conhecimento da sua existência os possam aceder.[4]

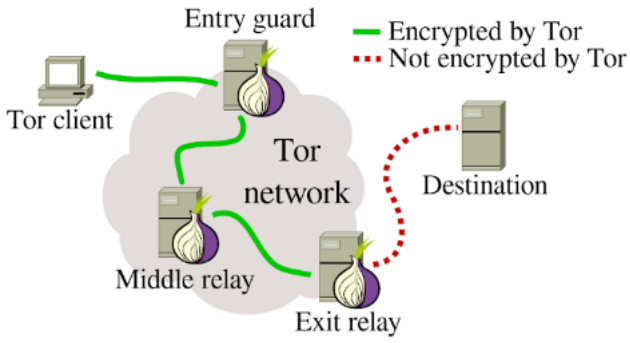

Fig. 2. Funcionamento da rede TOR.

4 Desafios na implementação da Dark Net

Como seria de esperar, um dos principais desafios da *dark net* é manter o anonimato. Neste sentido, as ferramentas para navegar neste ambiente necessitam de possuir algumas características que as diferenciem dos *browsers* comuns.[7]

Quando utilizamos um *browser* convencional para navegar na *web*, o nosso IP é fornecido aos diferentes servidores, aos quais realizamos pedidos. Esta exposição possibilita a deteção de informações acerca do utilizador e a sua localização.

A rede TOR encapsula o IP do utilizador, disponibilizando apenas um IP que pertence à mesma, e não ao utilizador, tornando desta forma os seus utilizadores anónimos. Para tornar isto possível, a rede TOR é formada por várias centenas de nodos de transmissão, sendo que no momento de transmissão das mensagens é gerado um caminho aleatório entre estes servidores, onde cada nodo apenas tem conhecimento do seu sucessor e antecessor no caminho. No entanto, este não é o único mecanismo de segurança suportado pelo TOR. Para processar o envio da mensagem, esta deve ser criptografada tantas vezes quanto o número de nodos existentes no caminho, isto é, este processo começa por encriptar a mensagem de forma a que o último nodo do percurso a consiga desencriptar, e aplica recursivamente este método até a mensagem possuir a encriptação destinada ao primeiro nodo do caminho. Desta forma, cada nodo que recebe a mensagem consegue desencriptar a mesma e reencaminha-la para o próximo servidor do percurso até o destino ser alcançado.

Esta metodologia é conhecida como procedimento "onion", já que, a cada passagem por um servidor TOR, uma camada de encriptação é removida.

Apesar do forte compromisso com encriptação, esta metodologia é passível de falhas, por exemplo, no caso do nodo de saída se encontrar corrompido, é possível aceder aos dados transmitidos que neste ponto se encontram completamente desencriptados, como por exemplo mensagens privadas, dados bancários, e outro tipo de informação pessoal. Dan Egerstad, um pesquisador sueco utilizou este tipo de vulnerabilidade para recolher passwords de mais de 100 contas de email relacionadas com embaixadas estrangeiras.[8]

5 Diferentes usos da Dark Net

Nem tudo na Dark Net é mau. Apesar de todos os seus maus traços associados (pedofilia, tráfico, assassinatos, etc...), pelos quais é predominantemente reconhecida, a Dark Net também tem um lado bom, ambos partilhando um objetivo - manter informação confidencial. [9]

Muitos correspondentes internacionais comunicam com as respectivas redações por meio da Dark Net. Países como o Irão, Coreia do Norte e China costumam controlar a Internet convencional, sobretudo se quem estiver a navegar for um jornalista estrangeiro. Nestes países, as autoridades do governo não só bloqueiam o acesso ao conteúdo dos websites, mas também monitorizam o acesso à internet pelos cidadãos, países estes onde é bastante restrita a liberdade de expressão.

Nesse caso, usar a Dark Net e o seu anonimato associado é uma boa maneira de burlar a censura e fugir da repressão. Para além deste exemplo, vários documentos governamentais e militares confidenciais são mantidos na Dark Net, como por exemplo os apresentados em 2010 pela WikiLeaks relativos à guerra do Afeganistão, espionagem e corrupção política. Outro exemplo relevante é o Secure Drop do Washington Post [1], um jornal Americano que justifica a sua utilização da Dark Net dizendo que *"O SecureDrop do Washington Post é uma maneira discreta e segura para os leitores compartilharem mensagens e materiais com nossos jornalistas. Oferece maior segurança e anonimato do que o e-mail e Internet convencional"*, revelando publicamente o endereço do seu fórum (*https://jcw5q6uyjioupxcc.onion*).

Contudo, com esta vantagem do anonimato surge a pergunta *"Então porque não usamos mais vezes a Dark Net?"*. Tal como tudo, a Dark Net também tem algumas lacunas, pelo que se destaca a falta de segurança existente. Na internet normal temos segurança, mas não temos anonimato. Na Dark Net não temos segurança, mas temos anonimato. É com esta comparação que se reflete no porquê de não se usar a DarkNet mais regularmente. Para além da lacuna referida, a conexão é mais lenta (devido aos vários redirecionamentos), e as extensões como o Java e Flash são bloqueadas como meio de garantir o anonimato, o que torna os layouts bastante mais antiquados e menos apelativos.

No caso da primeira lacuna referida, assumindo que a informação que se pretende comunicar é interna, seria recomendável recorrer a uma rede WAN (Wide Area Network), uma vez que o uso da Dark Net para esse fim se torna bastante lento e com elevada latência, tal como explicado. Assim, a informação estaria efetivamente reservada ao interior desta rede, assegurando que nenhum dos nodos estaria conectado ao exterior.

6 Eventuais projetos atuais relacionados

6.1 Percurso dos pacotes na rede onion

Atualmente, um dos principais objetivos desta área é a possibilidade de conseguir combater a criminalidade presente na DarkNet. Para tal, vários investigadores têm recorrido à inteligência artificial e suas sub-áreas para desenvolver mecanismos de detecção, prevenção e combate ao crime na darkweb.

Um estudo liderado por Seiichi Ozawa tem como mote analisar o tráfego de pacotes, apesar de estes serem fortemente encriptados e redirecionados várias vezes através do Tor. Deste modo, o algoritmo procura fazer uma espécie de *backtracking* a todos os saltos da rede, analisando vários componentes da comunicação, tais como portas de destino, tipos de serviço, tamanhos de janela TCP, pacotes SYN, entre outros.[10]

6.2 Mapeamento de utilizadores

Uma das formas de analisar e interligar informações relativas aos utilizadores da Dark Net é através do recurso à inteligência artificial para encontrar correspondências entre um utilizador, e até mesmo com as suas ligações sociais. Os

utilizadores estão constantemente a criar novos perfis, sendo que nem sempre empregam os mesmos *usernames* para se identificar em cada um dos sites. Mesmo não tendo o mesmo *username* em todos os sites, os vendedores geralmente encaminham os seus clientes para os seus sites, ou sites dos quais colaboram ou possam tirar partido. Estes sinais podem ser utilizados para efetuar um mapeamento entre os vendedores e a sua atividade em fóruns, podendo levar até à sua verdadeira identidade. [12]

Este tipo de tarefa é tipicamente feito manualmente, mas torna-se algo limitado e complexo para o ser humano devido à quantidade de informação que poderá acarretar. Para automatizar o processo, um laboratório com o nome Lincoln Laboratory está a desenvolver um projeto na área de *machine learning* para permitir computar similaridades entre utilizadores de diversos fóruns através de um modelo de autoria, baseando-se em três aspetos chave:

- Como se identificam aos outros utilizadores;
- O que escrevem sobre eles;
- Com quem contactam;

O algoritmo baseia-se em fazer um *authorship model* para cada um dos fóruns analisados e posteriormente comparar as informações, com o objetivo de encontrar evidências e similaridades segundo os aspetos referidos anteriormente. Este projeto tem sido testado não só na Dark Web, mas também no âmbito das redes sociais, tendo sido reportada uma taxa de eficácia de 95%.

7 Conclusão

No presente trabalho, procurou-se descrever sumariamente o conceito DarkNet e distingui-lo de outros conceitos similares, colocando sempre em evidência a dimensão desta camada da Internet em relação à surface web, bem como explicar e avaliar de forma técnica os mecanismos de anonimização desta tecnologia.

Atualmente os problemas que envolvem a privacidade na Internet crescem exponencialmente devido à enorme quantidade de dados sensíveis que são trafegados e detidos por grandes empresas, o que leva ao aumento da preocupação coletiva no que diz respeito à privacidade online.

Desta forma, conclui-se que a Dark Web tem um papel crucial neste contexto e fornece ferramentas capazes de navegar online sem que a privacidade seja comprometida. No entanto, dado que é praticamente impossível controlar toda esta rede, a segurança da mesma pode ser em parte comprometida quando nos focamos principalmente nos sites de conteúdo ilegal.

Em suma, apesar do mau caráter geralmente associado às camadas inferiores da World Wide Web, podemos concluir que este tipo de redes, apesar de todos os perigos associados, também consegue fornecer utilidades exclusivas aos seus utilizadores, e que o recurso à anonimidade se revela de extrema importância quando se navega nesta camada.

References

1. Sérgio. (2019, March 7). Darknet: A rota da seda para as comunicações cifradas - CyberS3c. CyberS3c. https://www.cybers3c.pt/darknet-a-rota-da-seda-para-as-comunicacoes-cifradas/
2. DarkNet / Dark Web vs. Deep Web: What Is the Difference And Is It Illegal to Surf The DarkNet / Dark Web? A Social Links Article. (n.d.). Mtg-Bi.com. https://mtg-bi.com/blog/darkweb-vs-deepweb
3. What is the Darknet? - Definition from Techopedia. (2020). Techopedia.com. https://www.techopedia.com/definition/2395/darknet
4. RFC 7686 - The ".onion" Special-Use Domain Name. (n.d.). Datatracker.ietf.org. Retrieved February 27, 2022, from https://datatracker.ietf.org/doc/html/rfc7686
5. Dingledine, R. (n.d.). Tor: The Second-Generation Onion Router. https://svn-archive.torproject.org/svn/projects/design-paper/tor-design.pdf
6. Tor Project — How do Onion Services work? (n.d.). Community.torproject.org. Retrieved February 27, 2022, from https://community.torproject.org/onion-services/overview/
7. CEOP. (2020). The Dark Web. Thinkuknow.co.uk. https://www.thinkuknow.co.uk/professionals/our-views/the-dark-web/
8. Onion Router - an overview — ScienceDirect Topics. (n.d.). Www.sciencedirect.com. https://www.sciencedirect.com/topics/computer-science/onion-router
9. Mello, J. (n.d.). A Deep Web tem um lado bom. Revista Galileu. https://revistagalileu.globo.com/Tecnologia/Internet/noticia/2015/03/deep-web-tem-um-lado-bom.html
10. Artificial intelligence shines light on the dark web. (n.d.). MIT News — Massachusetts Institute of Technology. Retrieved February 27, 2022, from https://news.mit.edu/2019/lincoln-laboratory-artificial-intelligence-helping-investigators-fight-dark-web-crime-0513
11. Cilleruelo, C., de-Marcos, L., Junquera-Sanchez, J., Martínez-Herraiz, J.-J. (2020). Interconnection Between Darknets [Review of Interconnection Between Darknets]. In 28805 Alcala de Henares (Ed.), FEATURE ARTICLE: DARKNETS/ALTERNATIVE NETWORKS. IEEE Computer Society.
12. Adewopo, V., Gonen, B., Varlioglu, S., Ozer, M. (2019). Plunge into the Underworld: A Survey on Emergence of Darknet (p. 5) [Review of Plunge into the Underworld: A Survey on Emergence of Darknet].
13. Finklea, K. (2017). Dark Web (CRS Report, Ed.) [Review of Dark Web].
14. Sabarinath. (2021, August 22). Darknet vs Dark Web vs Deep Web vs Surface Web — Different Parts Of The World Wide Web [Review of Darknet vs Dark Web vs Deep Web vs Surface Web — Different Parts Of The World Wide Web]. Techlog360. https://techlog360.com/darknet-vs-dark-web-vs-deep-web-vs-surface-web/