# Anonimização e Redes Escuras

Paulo Costa[A87986], Filipe Azevedo[A87969] e Rui Baptista[A87989]

Universidade do Minho, Braga, Portugal

**Abstract.** Nos dias de hoje existe conteúdo na internet que não é acessível através dos motores de busca tradicionais. Nessa zona da internet existe um anonimato bastante superior ao das camadas superiores da mesma, para que seja possível recorrer a meios/ações ilegais, quer sejam eles a liberdade de expressão ou até mesmo a organização de ataques terroristas. Contudo, cabe às forças policiais e militares combater este tipo de ações, impondo assim as leis dos seus respetivos países, transformando as camadas inferiores da internet não só num mundo de informação que não está disponível nas camadas superiores como também num jogo do gato e do rato, entre fugitivos e os seus opressores, ou até mesmo criminosos e a polícia. Para combater a criminalidade, a polícia utiliza metódos de perda de anonimato de forma a tentar encontrar os responsáveis de cada ação, tentando levá-los à justiça. Deste modo, os utilizadores recorrem ao Tor e a outras ferramentas de forma a dificultar ao máximo a sua identificação, que em alguns casos, se esta ocorrer, pode levar à pena de prisão dos mesmos.

**Keywords:** Anonimização, Redes Escuras.

## 1 História

Começou como um projeto militar financiado pela Defesa Agência de Projetos de Pesquisa Avançada (DARPA) nos Laboratórios Naval de Pesquisa dos EUA (NRL) nos anos 90. **[1]**

Foi inicialmente desenvolvido como um método para anonimizar tráfego para que os agentes da lei possam manter a sua identidade em segredo na Internet sem deixar traços do seu IP. **[2]** O Tor permite que os clientes acessem sites regulares impedindo que a análise de utilizadores ocorra, é um software que é instalado no seu navegador e configura as conexões específicas necessárias para acessar sites ocultos.

## 2 Funcionalidades

### 2.1 Conexões

Criticamente, o Tor é uma tecnologia criptografada que ajuda as pessoas a manter o anonimato online. Isso é feito, em parte, roteando conexões através de servidores em

todo o mundo, tornando-os muito mais difíceis de rastrear. O Tor também permite que as pessoas acessem os chamados serviços ocultos - sites subterrâneos nos quais pertencem á Dark Web.

Em vez de ver domínios que terminam em .com ou .org, esses sites ocultos terminam em .onion. Sendo este é um sufixo de domínio de nível superior de uso especial que designa um serviço de host (semelhante ao conceito de .bitnet e .uucp, utilizados em épocas anteriores) utilizado para sites ou serviços que se encaixam na rede The Onion Router, conhecida como Tor. Esses endereços não são DNS reais e o .onion TLD não está no Internet DNS root. Porém, com software de proxy instalado e navegadores de Internet, como browser, é possível aceder a sites .onion através da rede de servidores Tor. **[3]**

### 2.2 Serviços Ocultos

Os serviços ocultos são outro serviço principal do Tor. Estes serviços desejam manter um elemento no anonimato, e por isso só podem ser acessados usando um endereço .onion, que requer o Navegador Tor. Este método, em contrário dos sites convencionais, não revela o endereço IP do host do site.

Portanto, um utilizador pode configurar um servidor, por exemplo, sem se preocupar o rastreamento até ele. Basicamente com o Tor instalado no seu computador, ele oculta a sua identidade na rede e impede que visualizem as tarefas que está a realizar. Isto devido ao mecanismo que utiliza um transmissão de dados que passa por inúmeras máquinas. Por exemplo, se mandarmos uma mensagem a alguém, esta não passará só por um computador mas por vários, até chegar ao destino, isto com o intuito de confundir “terceiros” interessados em invadir a sua privacidade.

## 3 Vulnerabilidades

### 3.1 Ataques Maliciosos

Como em qualquer outro serviço, ataques maliciosos podem ocorrer contra um cliente. Isso pode ser devido ao serviço utilizado, seja um serviço oculto ou um site público, ou através da própria rede Tor. Os serviços ocultos também estão sujeitos aos mesmos tipos de ataques que podem afetar sites regulares. No entanto, no Tor, dado o aspeto de retransmissão das conexões, outros nós também podem ter efeitos maliciosos. Isso geralmente ocorre no nó de saída, pois é o único nó que tem acesso aos dados que entram e saem do serviço. Para além disso, pode incluir a injeção de malware quando o nó de saída os recebe, embora isso só possa ser feito quando o download não é cripto-grafado, por meio de uma conexão HTTP. **[4]**

O Tor possui um sistema para combater esses nós de saída maliciosos. Todos os nós do relé têm bandeiras para indicar o seu estado. Somente alguns nós são configurados para serem nós de saída, o que é indicado por uma bandeira. Se um utilizador do Tor suspeitar que sua conexão foi violada, ele poderá relatar o nó de saída a uma autoridade competente. As autoridades competentes votam no nó e, se houver um consenso que ele é, de facto, malicioso recebe um sinal BadExitNode. Isso garante que o nó não será

mais usado como nó de saída, embora ainda possa ser usado como nó de retransmissão. No entanto, se houver suspeita de uso de um nó numa versão suspeita do Tor ou envolver-se em ataques de correlação de ponta a ponta, a sua bandeira válida pode ser removida, o que significa que não será usado por nenhum utilizador por qualquer motivo. **[5]**

### 3.2 Perda de anonimato

Dado que as pessoas recorrem frequentemente ao Tor como um método de proteger a sua privacidade e se tornarem anónimas, a maioria dos ataques tem o objetivo de cancelar o anonimato de utilizadores e serviços ocultos. Para esclarecer, cancelar o anonimato de um utilizador refere-se à descoberta do endereço IP ou MAC do qual ele se conectou à rede Tor. Os endereços IP e MAC podem ser consultados para recolher a localização geográfica e outros dados. Por vezes, nós próprios podemos destruir o nosso anonimato se o usarmos de maneira errada, visto que, se o Tor nos mantem a identidade anónima, isto não adianta de nada se navergarmos de forma inconsciente, por exemplo ao fazer login no Google, pois este irá conseguir ver as comunicações a ser feitas dentro do sistema. **[6]**

Um membro anónimo foi apanhado porque usava Tor inconscientemente . O rapaz que publicou sobre uma ameaça de bomba falsa em Harvard em 2013, fez login no Tor mas usou o serviço de Internet de Harvard, que é controlado/verificado. Como as autoridades puderam dizer que a mensagem vinha da rede Tor, elas simplesmente analisaram quem estava a utilizar o Tor na Internet de Harvard no momento em que o email foi enviado. Resumidamente, o Tor ajuda em muito a manter o anonimato do utilizador, mas não impede que não sejamos vítimas de explorações existentes na Web comum, pois inclui algumas vulnerabilidades.

### 3.3 Dicas para a utilização da Darkweb

Apenas enviar conteúdo sensível/pessoal através de sites confiáveis, e para além disso encriptar a própria informação. É também importante utilizar redes seguras e desativar programas que possam executar código no computador autonomamente como Java e Flash.

A utilização de VPNs é outro aspeto importante, de forma a dificultar a identificação do utilizador, e a utilização de sites escondidos ao invés de outros na internet superficial é preferível.**[7]**

### 3.4 Comunicação

Quando os utilizadores se conectam à Dark Web, geralmente fazem-no usando um serviço como o Tor, para o seu anonimato. Portanto, sempre que se encontra alguém, nunca se tem ideia de quem sera, nem eles sabem quem somos. Ainda assim, a maior parte do que acontece na Dark Web exige que duas ou mais pessoas possam falar umas com as outras. O que levanta a questão interessante de como isso é feito.

**Tabela 1 [8]**

| | |
|---|---|
| **Email** | Tecnologias como HTTPS e PGP são dois exemplos de como a comunicação de texto pode ser protegida. |
| **Fóruns** | Existem algumas soluções de fórum de código aberto que praticamente qualquer pessoa pode instalar em um servidor Web e começar a oferecer aos utilizadores. |
| **Market Places** | Os mercados agem como um sistema em que vendedores e compradores podem trocar de forma segura e anónima bens e dinheiro. Obviamente, eles precisarão conversar entre si para negociar acordos. É por isso que muitos mercados também fornecem ferramentas de bate-papo e mensagens como parte do serviço total. |

Ao usar o Tor, o conteúdo real da sua comunicação na Dark Web está oculto, mas isso não é suficiente. Apenas o simples facto de estar conectado à rede Tor já pode colocá-lo sob os olhos atentos do governo. A única maneira de manter essas duas entidades afastadas das suas atividades é usar uma VPN. Isso mascara a conexão com o mundo exterior, tornando a escuta praticamente impossível.

# 4 Anonimato na Darkweb

"Concluímos que o anonimato não é completamente verificável na Dark Web, mesmo que o TOR seja dedicado a esse segmento de rede, que se propôs a fornecer atividades anónimas", afirmou um relatório. **[9]**

Por exemplo, o ataque dos Anonymous à Dark Web. Um hacker conseguiu aceder a vários sites dentro da Dark Web e mais de metade destes sites alojados continham pornografia infantil e excediam em muito os espaços disponibilizados para alojamento, o que revelava que a Freedom Hosting II (Um serviço de Host de sites dentro da Dark Web especializado em Tor, agora já extinto) sabia da situação. Para além destes sites, o hacker revelou ainda que estavam alojados muitos outros sites associados a esquemas fraudulentos, criados e mantidos pela Freedom Hosting II, para pagar as suas despesas. **[10]**

## 4.1 A Darkweb é totalmente anónima?

O anonimato garantido não é infalível. Enquanto ferramentas como o Tor visam anonimizar conteúdo e atividade, especialistas em segurança estão constantemente a desenvolver meios pelos quais certos serviços ou indivíduos ocultos podem ser identificados ou "desanonimizados". **[11]**

### 4.2 Porquê ocultar a nossa atividade?

Várias razões foram citadas pelas quais indivíduos podem usar serviços como o Tor para anonimizar a atividade online. Serviços de anonimato têm sido usados para atividades legais e ilegais, que vão desde manter confidenciais as comunicações confidenciais até vender drogas ilegais.

É importante notar que, embora exista uma ampla variedade de usos legítimos do Tor, grande parte da pesquisa e preocupação em torno dos serviços de anonimato envolve o uso para atividades ilegais. Como tal, a maior parte desta secção se concentra nas atividades ilegais.

### 4.3 Privacidade Online

O Tor é usado para proteger a privacidade das atividades e comunicações em vários domínios. Os defensores da privacidade geralmente promovem o uso do Tor e de software similar para manter a liberdade de expressão, privacidade e anonimato. **[12]** Existem vários exemplos de como ele pode ser usado para esses fins:

**Tabela 2**

| | |
|---|---|
| **Anti-censura e ativismo político** | • Permite alcance de destinos ou conteúdos de outra forma bloqueados (vídeos bloqueados na Coreia do Norte).<br>• Anonimização de comunicações e locais, por parte de dissidentes políticos (Ex: movimentos dissidentes no Irão e Egito). **[13]** |
| **Comunicação sensível** | • Porto seguro para discussão de temas particulares ou sociais, como o regime e a religião.<br>• Ocultação da atividade online de crianças, com o intuito de as proteger.<br>• Proteção de ideias e projetos inacabados, por parte de empresas. **[14]** |
| **Informações "libertadas"** | • Permite a divulgação de informações de forma anónima, como o caso de Edward Snowden. **[15]** |

# 5 Atividades ilegais na Darkweb

Assim como atividades ilegais podem ocorrer através do Surface Web, também podem ocorrer no Deep Web e no Dark Web. A web pode servir como um fórum de conversa, coordenação e ação.

Especificamente, podem contar com a Dark Web para ajudar a realizer as suas atividades com risco reduzido de detecção. Embora esta secção se concentre nos criminosos que operam no ciberespaço, as questões levantadas certamente são aplicáveis a outras categorias de utilizadores mal-intencionados.

A Dark Web foi citada como facilitadora de uma ampla variedade de crimes. Bens ilícitos como drogas, armas, animais exóticos, bens e informações roubados são todos vendidos com fins lucrativos. Existem sites de apostas, hackers e assassinos a soldo e bastante pornografia infantil.

Os utilizadores mal-intencionados precisam ou beneficiam da Dark Web para realizar as suas atividades? Pesquisadores apontaram prós e contras de confiar no anonimato da Dark Web. Os criminosos que vendem bens ilícitos podem beneficiar da proteção adicional do anonimato pela Dark Web, ao serem mais capazes de evitar a aplicação da lei. No entanto, eles podem ter mais problemas para conseguir negócios. Por outras palavras, o anonimato pode ser uma barreira online se alguém estiver a tentar vender mercadorias e não tiver sido avaliado de outra forma, ou seja, que não consegue estabelecer uma relação com os clientes, no caso de confiança, pode ser mau para o mercado em que se encontra.

## 5.1 Pagamentos na Darkweb

Bitcoin é a moeda mais utilizada para transações na Darknet. **[16]** É uma moeda digital descentralizada, que usa transações interpessoais anónimas. **[17]** A moeda é normalmente obtida como forma de pagamento, através da compra da mesma ou por mineração. **[18]**

Estas transações são gravadas na blockchain, sendo que as informações guardadas são a ‘morada’ do bitcoin e o recibo. A ‘morada’ serve apenas para identificar particularmente a transação. **[19]** Para manusear a moeda, utilizam-se carteiras virtuais, semelhantes ao paypal mas para cryptomoedas.

# 6 Aplicações militares

Para além dos vários aspetos positivos da Darkweb, esta também tem aspetos negativos. Existem vários lojas online de material e serviços ilícitos como venda de drogas. Assim, as forças policiais vigiam parte da Darkweb e combatem o crime online

A Darkweb é muitas vezes utilizada por agências de inteligência, de forma a obter informações sobre possíveis guerras e ataques terroristas. Devido há existência de vários fóruns extremistas, esta plataforma é excelente para o planeamento de um atentado, coisa que as agências de inteligência e o ramo militar tentam travar a todo o custo.

# 7 Conclusão

A Darkweb tem vindo a despertar cada vez mais o interesse de investigadores, forças policiais e governos de todo o mundo. Contudo, devido ao anonimato, investigar o que quer que seja não é nada fácil. Uma dúvida comum é se realmente TOR é ou não seguro, pode-se responder rapidamente com "depende", pois de facto é competente no que toca a impedir o acesso aos seus dados, escondendo seu IP e a sua localização mas também como é de facto possível este sofrer ataques muitos ficam em dúvida.

Embora o Tor não seja perfeito, continua a ser uma das melhores opções disponíveis, no entanto é necessário manter todos os cuidados para se evitar ser descoberto, e o Tor precisa de continuar a evoluir, para que seja possível vencer a guerra da liberdade de expressão versus a censura.

# 8 Bibliografia

**[1]** DARPA (dark web project): https://www.quora.com/Did-DARPA-create-the-internet-and-the-deep-web

**[2]** DARPA (web search engine): https://www.bbc.com/news/av/technology-31808104/darpa-creates-dark-web-search-engine

**[3]** Torproject, Tor: Onion Service Protocol, every step you need to know. https://2019.www.torproject.org/docs/onion-services.html.en

**[4]** GarethOwen,Tor: Hidden Services and Deanonymisation,2014,https://www.youtube.com/watch?v=-oTEoLB-ses&feature=youtu.be.

**[5]** Project, Tor

**[6]** https://gizmodo.uol.com.br/7-coisas-que-voce-precisa-saber-sobre-o-tor/

**[7]** . "How to safely access the deep and dark webs", by Steve Symanovich, Norton Security https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html

**[8]** How Dark Web Communication Works? Users Communication: https://www.technadu.com/dark-web-communication-works/62189/

**[9]** "Dark Web users are not anonymous anymore, Revealed a new Study" (The privacy and anonymity Dark web): https://www.digitalinformationworld.com/2019/05/dark-web-and-its-impact-in-online-anonymity-and-privacy-a-critical-analysis.html#

**[10]** The Anonymous attack to the dark web: https://pplware.sapo.pt/internet/anonymous-derrubar-20-da-dark-web/

**[11]** Kim Zetter, "New 'Google' for the Dark Web Makes Buying Dope and Guns Easy," Wired.com, April 17, 2014

**[12]** Cooper Quintin, 7 Things You Should Know About Tor, Electronic Frontier Foundation, July 1, 2014

**[13]** Free Software Foundation, "2010 Free Software Awards Announced," press release, March 22, 2011

**[14]** Tor Project, Tor: Overview, https://www.torproject.org/about/overview.html.en

**[15]** Ibid

**[16]** See, for example, Michael Chertoff and Toby Simon, The Impact of the Dark Web on Internet Governance and Cyber Security, Global Commission on Internet Governance, Paper

Series: No. 6, February 2015

"How does bitcoin work?", by bitcoin.com https://bitcoin.org/en/how-it-works

**[17]** Pierluigi Paganini, "What is the Deep Web? A First Trip Into the Abyss," Security Affairs, May 24, 2012. Of note, a number of digital currencies exist, though Bitcoin is the most prominent. These currencies include Ripple and Litecoin, among others. See https://coinmarketcap.com/

**[18]** For more information on Bitcoin, see CRS Report R43339, Bitcoin: Questions, Answers, and Analysis of Legal Issues, by Edward V. Murphy, M. Maureen Murphy, and Michael V. Seitzinger. See also Timothy Lee, "12 Questions About Bitcoin You Were Too Embarrassed To Ask," The Washington Post, November 19, 2013

**[19]** More information is available at https://bitcoin.org/en/faq#how-does-one-acquire-bitcoins.

"P2P Transactions", by Plutus https://medium.com/plutus-it/what-are-peer-to-peer-transactions-596d6fc0bdda