Anonimização e "Dark Web"

André Gonçalves, Diogo Gonçalves, and Maria Pires

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a80368,a81860,a86268}@alunos.uminho.pt

Abstract. A *dark web* é uma pequena parte pertencente à *deep web*, no entanto algumas vezes estas duas designações são erradamente confundidas.
deep web é a parte da internet que não se encontra registada, logo não é possível acedê-la pelas ferramentas de busca tradicionais ou ao escrever o endereço de IP em browsers normais. Trata-se de um conjunto de redes encriptadas (conhecidas como *darknets*) que estão intencionalmente escondidas da Internet dita visível através de sistemas de encriptação.
A *dark web* contém conteúdo que foi intencionalmente ocultado porque apesar de poder ser utilizado para fins legítimos,esta está associada à ocorrência de crimes e compartilhamento de situações e informações ilícitas, entre as quais: compra de drogas, documentos ilegais, serviços de assassinato, pornografia infantil, etc.
A maioria dos sites da *dark web* não fazem o menor sentido, os seus URL estão cheios de letras e números aleatórios seguidos do domínio ".onion". Para aceder a estes sites, é necessário instalar software especial que permite salvaguardar o anonimato do utilizador, sendo o mais conhecido o Tor: *The Onion Router*.
Por um lado, a *deep web* permite visualizar diferentes conteúdos como artigos científicos e participar em fóruns de discussões específicas assegurando a privacidade dos utilizadores. Por outro lado, o anonimato leva também à propensão da prática de ilegalidades.

1 Introdução

A *deep web* é uma qualquer página que exige métodos bastante específicos para ser acedida. Esta rede é desconhecida por grande parte das pessoas e é muito maior do que aquilo que imaginamos, ao ponto de não conseguirmos medir a sua dimensão. Os especialistas estimam que é 500 vezes maior que a *surface web* e que o seu crescimento é exponencial. A *surface web* diz respeito ao sites que estão registados e é a parte da web a que estamos habituados a usar no nosso dia-a-dia, enquanto que dentro da *deep web* existe uma pequena porção de sites não registados e que só podem ser acedidos através do uso de uma *darknet*, constituindo assim a *dark web*.

Este relatório visa abordar a anonimização e *dark web* e mais concretamente o que levou à criação desta rede, quais as ferramentas necessárias para a sua utilização e o que esta permite ou não fazer. São objetivos deste trabalho apresentar uma visão geral de o que é a *dark web* e o porquê da sua crescente popularidade.

A metodologia utilizada foi a pesquisa na internet, enriquecida com alguns *papers* relacionados com o tema.

2 História

O desenvolvimento do *The Onion Routing* para realizar pesquisas e analisar sistemas de comunicação anónimos foi elaborado por três cientistas: Mike Reed, Paul Syversin e David Goldshlag. Um facto surpreendente é que foi criado e implementado pelo *United States Defense Advance Research Projects Agency* sendo depois o seu crescimento financiado por várias entidades tais como : *State Department, Electronic Frontier Foundation, National Science Foundation, e USA Naval Research Lab* sendo o contributo deste último o mais reconhecido.

O objetivo deste conceito era proteger as comunicações militares, fazendo com que as mensagens chegassem ao seu destino de forma aleatória, confundindo o inimigo. No entanto, existia um pequeno problema: se este software só fosse utilizado pelos militares era fácil de identificar e o seu uso seria absurdo. Portanto tinham que expandir o software para ser utilizado por mais pessoas. Assim, através da cooperação de Roger Dingledine e Nick Mathewson em 2002 Tor tornou-se *free and open source project for anyone*.

3 Onion Routing

The Onion Routing é uma técnica para estabelecer comunicação anónima numa rede de computadores. Neste tipo de redes todas as mensagens são encapsuladas em camadas encriptadas, surgindo assim a analogia a uma cebola. A ideia desta técnica é redirecionar o tráfego de internet através de uma rede encriptada de servidores voluntários. Neste capítulo será explicado como é feita toda a ligação entre servidores e utilizadores.

3.1 Tor

O Tor roteia cada pedido de um utilizador por múltiplos nodos de retransmissão(*relay node*) encriptados, de modo a que seja impossível seguir a mensagem. Desta forma qualquer pedido passa por vários endereços IP e o destino não consegue descobrir quem enviou o pacote. A parte complicada do Tor é que nenhum dos nodos pode saber de onde originou a informação ou qual será o seu destino porque assim estaria a criar vulnerabilidades na rede que estaria sujeita a ataques. A solução encontrada para resolver este problema é utilizar uma chave de encriptação publica e publicar a lista de todos os *relay node*.

O processo inicializa-se no cliente, este contacta um servidor de administração Tor para obter uma lista atualizada de todos os *relay node*. Ele utiliza esta lista para criar um caminho de nodos onde se liga ao nodo de entrada (*guard node*) e o nodo de saída (*exit node*) que conecta ao servidor. Depois de estabelecido o caminho, o cliente encripta a mensagem com a chave publica do *exit node*, de seguida pega na mensagem encriptada e envia para todos os nodos intermédios para fazerem o mesmo até chegar ao *guard node*. Depois da mensagem estar encriptada pelos múltiplos nodos o cliente envia a mensagem para o *guard node*. Esta mensagem depois de desencriptada contém o endereço do nodo seguinte para lhe enviar a mensagem, isto é feito até chegar ao *exit node* onde este enviará a mensagem final ao servidor dando a ideia que é o *exit node* que está a mandar a mensagem.

O tamanho normal de um circuito Tor são 3 nodos. As mensagens são transmitidas usando uma *stream cipher*, onde os bits são transmitidos um de cada vez utilizando a encriptação *128-bit Advanced Encryption Standard (AES)*. Cada nodo tem uma chave de autenticação obtido através da encriptação *public-key 1024-bit RSA* que nunca deve ser alterado e é usado apenas para identificação do mesmo.

3.2 Hidden services

Outro serviço disponibilizado pelo Tor são os *hidden services*, isto permite que não só os usuários se mantenham anónimos mas também os servidores, estes só poderam ser acedidos se o seu endereço acabar em .onion. Este método não revela o IP do *host*, logo um utilizador poderá configurar um servidor sem a preocupação do conteúdo do mesmo.

Para garantir este anonimato o *hidden service* comunica com os outros nodos utilizando um circuito Tor. O *hidden service* seleciona uns nodos introdutórios e configura circuitos Tor neles, isto permite com que possam ser transmitidas mensagens para o *hidden service* sem que a sua localização seja conhecida. Depois o *hidden service* deve configurar um descritor que contem a chave publica do *hidden service* e referencias para os nodos introdutórios, apos isto ser feito é realizado o *upload* para a database hash table que contem todos os nodos.

Um cliente pode encontrar o *hidden service* através do seu endereço .onion e ira obter o descritor que contem os nodos introdutórios para a hash table. O cliente cria um circuito Tor para um nodo aleatório que atua como ponto de encontro, o cliente manda uma mensagem para um dos nodos introdutórios do *hidden service* que contém o nodo de encontro e uma password. Esta password é utilizada como autenticação entre o servidor e o utilizador. Após o *hidden service* receber a mensagem este cria um circuito Tor com o nodo de encontro e envia-lhe a password. De seguida o nodo de encontro envia a password para o cliente a informar que a conceção com o hidden service foi estabelecida e autenticada, a partir desse ponto esta criada uma ligação entre os dois agentes através dum nodo de encontro. Outro serviço disponibilizado pelo Tor são os *hidden services*, isto permite que não só os usuários se mantenham anónimos mas também os serviços, para isso os serviços só podem ser acedidos se o seu endereço acabar em .onion. Este método não revela o IP do host, logo um utilizador pode configurar um servidor sem se preocupar que o seu conteúdo seja associado a ele.

4 Vantagens e desvantagens

4.1 Desvantagens

Sendo que o Tor proporciona um acesso completamente anónimo à *dark web* não deixando qualquer traço da atividade ou da entidade dos seus utilizadores,tornando-se assim um local propício a atividades criminais, tais como o tráfico humano, de drogas, armas, órgãos, assassinatos, terrorismo, pedofilia, entre muitos outros. Um estudo feito pela universidade de Portsmouth em 2014 concluiu que o conteúdo mais procurado através do Tor era pornografia infantil, seguido pelo mercado negro de drogas e armas.

O site *Silk Road*, fundado em 2011, cujo foco das vendas recaía sobre as drogas ilícitas, efetuava todas as suas transações em *bitcoin* e em apenas um ano as vendas anuais atingiram os 22 milhões de dólares. O site foi fechado pelo FBI em 2013. Embora bens ou serviços destinados a fraudes ou ameaças à integridade física das pessoas, tais como números de cartões de crédito roubados, moedas falsas, informações pessoais, assassinatos, e materiais utilizados para construir armas fossem proibidos neste site,o mercado da *dark web* abrange todo esse tipo de bens ilícitos.

As autoridades por todo o mundo têm prestado cada vez mais atenção a este modo de interação encriptada o que levou a que as suas capacidades de deteção e encerramento de sites operados na *dark web* tenha vindo a aumentar. Contudo estes mercados são excecionalmente adaptáveis e há constantemente formas mais seguras e descentralizadas a nascer que são mais difíceis de combater, por exemplo o sistema de pagamentos online, os cartões de créditos seriam demasiado fáceis de rastrear, pelo que o método preferido é o uso da criptomodea, bitcoin*bitcoin*, recorrendo também a um processo chamado *multi-sig escrow* que reforça a segurança do pagamento, sendo este concluído com a autorização de 2 das 3 pessoas obrigatórias na transação e, adicionalmente, existem processos de *micro-laundering*, todos com a finalidade de esconder a identidade do comprador.

Ao nível das comunicações, o Tor possui serviços de email e chat tais como a *Torbox*. O onion routing permite a encriptação das mensagens que são enviadas através de diversos nós da rede tornando impossível que estes nós intermédios conheçam o destino, origem e conteúdo das mensagens. Este tipo de comunicação é muito popular entre os jihadistas, a *dark web* tornou-se a plataforma de recrutamento principal da ISIS, dado que através de fóruns e chats encriptados, a sua identidade e localização permanece oculta podendo assim informar militantes e simpatizantes sem medo de serem detetados pelas autoridades. Para além de um meio seguro para comunicar fornece também a estes grupos terroristas financiamento através de transferências ilícitas de *bitcoins*, a criptomoeda é enviada direta e anonimamente para as contas pretendidas através de apps como a *Dark wallet*, havendo um aumento de grupos terroristas a solicitar financiamento através de doações de *bitcoin*. [5]

4.2 Vantagens

Apesar deste lado grotesco, existem bastantes benefícios no uso da anonimização pois tal como esta pode ser usada para fins criminosos, bem aplicada, permite que as autoridades vigiem e controlem operações seguramente e que os civis informem a policia de forma anonima, não correndo riscos. De modo a conseguir rastrear criminosos o FBI desenvolveu o *CIPAV*, *computer and internet protocol address verifier* de modo a identificar suspeitos que estejam a esconder a sua localização com servidores proxy ou serviços de anonimização como o Tor [1]. O *CIPAV* é uma ferramenta de recolha de dados que opera no computador do alvo como qualquer outro *spyware* ilegal, monitorizando e reportando todas as suas atividades, permitindo assim a localização de hackers, predadores sexuais, extorsionistas entre outros.

Tendo as comunicações militares sido a base do desenvolvimento do *onion routing* esta continua a ser uma das áreas que mais ganha com a anonimização, sendo usada para proteger a identidade dos comandos militares e prevenir a penetração por parte dos atacantes. A *dark web* pode ser usada para estudar o ambiente em que opera e descobrir atividades que possam comprometer as tropas operacionais. Os militares podem também intercetar ou impedir as comunicações dos inimigos.

Existem sites específicos para jornalistas, tais como a *securedrop* do *The New Yorker*, que permitem a partilha de ficheiros e artigos, receber denuncias de qualquer pessoa anonimamente sem correr o risco de expor a identidade dos seus informantes.

A anonimização facilita a liberdade de expressão, embora os países ocidentais a tomem por garantida, possibilita a manifestação de qualquer opinião e tópico a cidadãos de países com regimes autoritários, superando a censura. A informação é uma arma poderosa em governos opressivos e o uso da internet é severamente monitorizado de modo a evitar ideias revolucionárias [6]. Neste contexto o Tor é uma solução que permite a comunicação segura não só a nível nacional como internacional de modo a denunciar certas situações.

Embora a anonimização alimente o crescimento de organizações criminosas e grupos terroristas esta também deu origem ao nascimento do grupo de *hacktivistas anonymous*, um grupo que, como indica o nome, é anónimo e descentralizado, focado no ativismo politico, entre as suas atividades levou a cabo ataques contra o estado islâmico, revelando as identidades dos participantes em atentados e alguns membros desta organização terrorista, ataques conta sites de pornografia infantil, entre outros ciberataques de modo a chamar a atenção das autoridades para as atividades ilegais online de certos grupos.

5 Conclusão

A *deep web* tem como propósito oferecer uma maior segurança e privacidade aos seus utilizadores. Apesar de o seu uso ser muito vantajoso é preciso ter algum conhecimento de todos os perigos que o uso desta parte da internet representa.O uso de certas ferramentas como por exemplo o Tor permite que o acesso a esta rede seja facilitado e que o propósito da anonimização na internet seja atingido.

"The dark net is a world of power and freedom: of expression, of creativity, of information, of ideas. Power and freedom endow our creative and our destructive faculties. The dark net magnifies both, making it easier to explore every desire, to act on every dark impulse, to indulge every neurosis." [12]

References

1. Flinkia, Kristin: "Dark Web" (2017)
2. Hale, Jennifer: "HIDDEN WEB What is the dark web? From drugs and guns to the Chloe Ayling kidnapping, a look inside the encrypted network" (2018)
3. Chertoff, Michael: "A public policy perspective of the Dark Web" (2016)

4. Bartlett, Jamie: "Dark Net Markets: The eBay of Drug Dealing" (2014)
5. Bertrand, Natasha: “ISIS is taking full advantage of the darkest corners of the internet” (2015)
6. https://www.linkedin.com/pulse/pros-cons-deep-web-ernest-nwankwo-ceh/
7. Jacoby, Corianna: “The Onion Router and the Darkweb” (2016)
8. "https://www.youtube.com/watch?v=QRYzre4bf7I"
9. "https://www.youtube.com/watch?v=lVcbq_a5N9I"
10. "https://torstatus.blutmagie.de/"
11. "https://run.unl.pt/bitstream/10362/18052/1/WPSeries$_0$1$_2$016$DDuarteTMealha.pdf$"
12. https://www.goodreads.com/author/quotes/7489747.Jamie$_Bartlett$