Anonimização e Redes Escuras

Diogo Braga, João Silva, and Ricardo Caçador

University of Minho, Department of Informatics, 4710-057 Braga, Portugal
e-mail: {a82547,a82005,a81064}@alunos.uminho.pt
PL4, Grupo 7

Abstract. No âmbito da unidade curricular de Redes de Computadores, abordamos o tema "Anonimização e Redes Escuras". Incidimos maioritariamente sobre a anonimização e as razões que levam ao seu uso, tanto em redes escuras como na Internet.

1 Introdução

A internet é, basicamente, uma rede aberta baseada na confiança. Quando alguém se liga a um servidor web através da internet, o seu tráfego passa por muitos routers diferentes, pertencentes a uma grande variedade de instituições, corporações e indivíduos. A princípio, cada um destes routers tem a capacidade de expor totalmente os seus dados, os endereços de destino e envio de mensagens e, com frequência, também o conteúdo dos dados transferidos. Mesmo que os seus dados estejam criptografados, com o uso de um protocolo seguro, é possível ao seu ISP monitorizar a quantidade de dados transferidos, assim como a origem e o destino destes dados. Isto é o bastante para reunir um perfil completo de actividades online. [1]

Surge assim um problema, como nos podemos tornar anónimos nas nossas pesquisas? Poderá existir alguma forma de o tráfego não ser rastreado por outras entidades?

As camadas da Internet vão muito além do conteúdo superficial que muitas pessoas acedem geralmente nas suas pesquisas diárias. O outro conteúdo é o da Deep Web, conteúdo que não é indexado por motores de busca tradicionais como o Google. A informação mais profunda da Deep Web, conhecida como Dark Web, contêm conteúdo que foi intencionalmente escondido. A Dark Web pode ser usada para fins legítimos tais como contornar a censura, aceder a conteúdo bloqueado ou manter a privacidade de comunicações confidenciais, assim como atividades criminosas ou maliciosas que geralmente incluem contrabando de drogas ilícitas, armas, dinheiro falso, tráfego de orgãos e pornografia infantil.

Assim como os criminosos podem confiar na anonimização da Dark Web, as comunidades policiais, militares e de inteligência também podem fazê-lo. Eles podem, por exemplo, usá-lo para realizar operações de vigilância on-line. A anonimização na Dark Web pode ser usada para proteger funcionários de identificação e invasão por parte de adversários. Também pode ser usada para conduzir uma operação de rede de computadores clandestina ou secreta, como derrubar um site ou um ataque de negação de serviço, ou para interceptar comunicações. Segundo relatos, as autoridades estão continuamente a trabalhar na expansão de técnicas para tornar não anónima a atividade na Dark Web e identificar agentes maliciosos online. [2]

2 O Porquê da Anonimização

Os utilizadores do presente estão muito acostumados à Internet. Estão constantemente a partilhar informação sobre as suas vidas pessoais. Devido a isso, se alguém tentar espiar um utilizador conseguirá ter acesso à sua verdadeira identidade, localização, sistema operativo, histórico, browser usado, e muita outra informação sobre a vítima que esta não quererá certamente que seja partilhada com estranhos, que podem depois utilizar facilmente esses dados para expor a vítima.

Os Dark Web Providers protegem os dados dos utilizadores da vigilância de certas empresas e governos. Por exemplo: Se o utilizador viver num país em que o acesso à internet é restrito; Se o utilizador não quiser que certas empresas tirem vantagem do uso da sua informação pessoal, como o Facebook ou o Google.

Estes serviços fazem com que os utilizadores pareçam todos a mesma pessoa, o que confunde o observador e faz com que o utilizador fique anónimo. Deste modo, quantas mais pessoas usarem estes serviços mais fácil se torna estar anónimo pois é o mesmo do que se esconder numa multidão toda igual.

Usando estes serviços, os sites visitados por um utilizador não têm maneira de saber quem ele é, a não ser que o utilizador faça login e lhes diga. Consegue-se assim proteger a anonimidade de pessoas como ativitistas, jornalistas, bloggers e mesmo aqueles que são mal intencionados (ilegalidades). [3]

3 Internet

Se toda a atividade de um utilizador da internet pode ser observada por outros utilizadores, que tipo de mecanismos cada pessoa pode usar para se defender deste tipo de ataques estando a usar a internet? De seguida encontram-se 3 possíveis formas de anonimização na internet.

3.1 Private Browsing

A navegação privada de um browser (neste caso usando o exemplo da Google) apenas faz com que os outros utilizadores do dispositivo não vejam a atividade. O histórico e a informação colocada não é guardada e os cookies são apagados ao fechar o modo navegação privada.

Toda a atividade feita em modo privado continua a poder ser vísivel para os sites frequentados, o empregador/universidade que possui a rede a qual se está ligado e para quem providencia o serviço de internet. [4]

3.2 VPN

É basicamente um túnel seguro entre 2 ou mais dispostivos, possibiliando assim uma solução para envio de dados sensíveis através de redes inseguras. Apenas esconde os dados, ou seja, é mais usado como ferramenta para proteção de espionagem. [5] Os VPN's não tem a função de ocultar o endereço de IP, como tal são normalmente utilizados com outras técnicas. [6]

Num dos lados da ligação está um cliente de VPN e no outro está um dispositivo chamado "VPN Concentrator". O cliente utiliza uma app para entar no "VPN Concentrator" e estabelece uma ligação. Quando a ligação é feita, os dados passam a ser transferidos não pela interface normal, mas sim pelo túnel encriptado da VPN. [7]

3.3 Proxy

Os servidores de proxy aumentam a segurança e a performance no tráfego de dados entre utilizador e o servidor. Um servidor proxy coloca-se entre a conexão utilizador/servidor. Ou seja sempre que o utilizador quiser aceder ou receber algo do servidor, a informação passará pelo proxy. [8]

No servidor proxy a informação poderá ser filtrada para evitar ataques ou conteúdo não desejável ou para fornecer uma maior segurança aos equipamentos envolvidos. [7]

3.4 Traffic Analysis

Apesar dos Dark Web providers conseguirem evitar a maioria destes ataques, pois todos os utilizadores parecem iguais perante o observador, os utilizadores da internet são quem mais sofre com este tipo de ataques, mesmo estando devidamente protegidos.

O Traffic Analysis retira a informação dos PDUs.

Os PDUs da Internet têm duas partes: a carga útil de dados e o cabeçalho usado para o roteamento. A carga de dados é o que quer que seja, seja uma mensagem de email, uma página da Web ou um arquivo de áudio. Mesmo se a carga de dados for criptografada, a Traffic Analysis ainda revela muito sobre o que se está a fazer e possivelmente o que está dizer. Isso porque se concentra no cabeçalho, que divulga a origem, destino, tamanho, tempo... [9]

A Traffic Anlysis pode ser usada para inferir quem está a falar e com quem através de uma rede pública. Conhecer a origem e o destino do tráfego da Internet permite que outras pessoas acompanhem o seu comportamento e os seus interesses.

Os sites seguros usam o TLS (Transport Layer Security) para criptografar os dados, mas o cabeçalho não é criptografado para que o Internet provider (ISP) possa descobrir para onde enviar a solicitação e a resposta. [10]

4 DarkWeb Providers

Como opção mais viável à anonimização surgem os DarkWeb providers que permitem o acesso a camadas mais profundas de web, e oferecem anonimização doutras formas que não as usuais como já visto na internet. De seguida encontram-se 3 DarkWeb providers que funcionam de formas distintas.

4.1 Tor

As pessoas podem aceder à Dark Web usando um software especial, como o Tor .

O Tor possui uma rede de computadores voluntários para rotear o tráfego da web dos utilizadores por meio de uma série de computadores de outros utilizadores, de modo que o tráfego não possa ser rastreado até o usuário original. No mínimo o tráfico passa por 3 servidores Tor distribuídos algures no planeta e providencia 3 níveis de encriptação.

O Tor funciona apenas para fluxos TCP e pode ser usado por qualquer aplicativo com suporte a SOCKS(protocolo). [9]

Aquando do seu uso os endereços de IP permanecem escondidos.

Devido à sua implementação o Tor minimiza em muito as possibilidades de Traffic Analysis, pois distribui a informação através de vários servidores onde nenhum sabe sobre o destino dessa mesma informação.

Contudo, se alguém puder controlar todos os nós usados no circuito de um cliente, claramente podem-se conectar o usuário ao serviço que eles estão a aceder. No entanto, isso é difícil em prática, dado o alto número de nós Tor e o facto de que os circuitos expiram ao fim de um certo tempo. Isso significa que, mesmo que alguém fosse capaz de fazer isso, provavelmente seria apenas capaz de aceder a dados durante a janela de tempo em que o circuito foi usado. [10]

4.2 I2P

I2P é outro Dark Web provider. Como o Tor, este fornece serviços de Dark Web e acesso à Internet.

A rede em si é estritamente baseada em mensagens (IP), mas há uma biblioteca disponível para permitir uma comunicação de streaming confiável sobre ela (TCP).

Para anonimizar as mensagens enviadas, cada cliente tem seu "router" I2P para construir alguns "túneis" de entrada e saída - uma sequência de peer's que passam mensagens

numa direção (de e para o cliente, respectivamente). Cada router da rede escolhe o tamanho desses túneis e, ao fazê-lo, faz uma troca entre anonimização, latência e rendimento de acordo com suas próprias necessidades. [13]

Uma grande diferença é que o I2P é totalmente distribuído, ou seja, todos os dados são armazenados nos computadores dos utilizadores e encontrados através da rede enquanto Tor usa diretorias. Este sistema permite que o I2P forneça uma funcionalidade peer-to-peer, onde um utilizador pode simplesmente interagir com outros utilizadores confiáveis e com os seus peer's confiáveis.

I2P usa criptografia (AES - Advanced Encryption Standard) que é considerada mais segura do que a do Tor (4 camadas criptográficas). [10]

4.3 Freenet

As comunicações pelos nós da Freenet são criptografadas e são roteadas por outros nós para tornar extremamente difícil de determinar quem está a solicitar as informações e qual é seu conteúdo.

A Freenet esconde os IP dos utilizadores sendo assim impossível saber a localização de cada um. [15]

Acredita-se que o aspecto peer-to-peer da Freenet geralmente forneça mais segurança, já que o utilizador interage apenas diretamente com outros utilizadores confiáveis e os pedidos são quase-aleatoriamente passados para outros nós, usando algumas regras direcionais que garantem que não demore demais para encontrar uma solicitação, mas também garantir que uma solicitação seja difícil de ser seguida.

Os utilizadores contribuem para a rede fornecendo largura de banda e uma parte do seu disco rígido (chamado de "data store") para guardar arquivos.

Os ficheiros são criptografados, então geralmente o utilizador não pode descobrir facilmente o que está no seu "data store", e espera-se que não possa ser responsabilizado por isso. Fóruns de chat, sites e browsers de pesquisa são todos construídos tendo por base esse repositório de dados distribuídos. [14]

5 RGPD

O Regulamento Geral sobre a Proteção de Dados (RGPD) é um regulamento do direito europeu sobre privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia. O RGPD tem como objetivo dar aos cidadãos e residentes formas de controlar os seus dados pessoais.

O regulamento revoga a Diretiva de Proteção de Dados Pessoais de 1995, que dizia que o tratamento de dados pessoais se devia processar de forma transparente e no estrito respeito pela reserva da vida privada, bem como pelos direitos, liberdades e garantias fundamentais. [11]

O novo regulamento contém agora cláusulas e exigências relativas à forma como são tratadas informações pessoais na União Europeia e é aplicável a todas as empresas que operem no Espaço Económico Europeu. Os processos empresariais que tratem dados pessoais são obrigados a ser desenhados de raiz e por padrão com medidas que respeitem os princípios da proteção de dados por defeito e desde a sua conceção, o que significa que os dados devem ser guardados usando anonimização completa e as mais elevadas configurações de privacidade por padrão, de modo a que os dados não possam ser disponibilizados sem consentimento explícito, e não possam ser usados para identificar alguém sem informação adicional armazenada em separado.

O regulamento não permite o tratamento de quaisquer dados fora do contexto legal especificado no regulamento, exceto no caso em que quem controla os dados tenha recebido consentimento explícito e opt-in do proprietário dos dados. O proprietário tem ainda o direito de revogar esta permissão em qualquer momento. [12]

6 Conclusão

A anonimização total é impossível de garantir. Embora ferramentas como os falados Dark-Web providers visem anonimizar o conteúdo e a atividade, os investigadores e especialistas em segurança estão constantemente a desenvolver meios para que certos serviços ou indivíduos ocultos possam ser identificados ou "deanonimizados". [2]

Para esclarecer, deanonimizar um utilizador refere-se a descobrir o endereço IP ou MAC com o quais se conectaram à rede Tor. Os endereços IP e MAC abrem mais informações do que simplesmente um único identificador, eles também podem ser consultados para aceder à geolocalização e outros dados. E se um utilizador se conectar ao Tor usando uma VPN ou proxy, ainda haverá passos para descobrir o proprietário da máquina. No entanto, agências de aplicação da lei frequentemente podem solicitar essas informações dos providers e, em seguida, serem capazes de ligar um IP a seu pedido através de VPN ou proxy. [10]

Concluindo, constata-se que obter anonimização total não é uma tarefa simples, talvez até seja impossível mesmo com todos os cuidados e proteções. Apesar disto, os DarkWeb providers descritos continuam a ser das melhores opções para cada utilizador se manter minimamente anónimo no mundo da Web.

References

1. Tor e anonimizadores: https://wirelesspt.net/wiki/Tor_e_anonimizadores
2. Kristin Finklea: Dark Web (March 10, 2017)
3. How Tor Browser Protects Your Privacy and Identity Online: https://www.youtube.com/watch?v=JWII85UlzKw&list=PLwyU2dZ3LJErtu3GGElIa7VyORE2B6H1H&index=2&t=0s
4. How private browsing works: https://support.google.com/chrome/answer/7440301.
5. O que é VPN?: https://www.expressvpn.com/pt/whatisvpn.
6. Edelberto Franco Silva: Anonimização e a Anti-anonimização: http://www2.ic.uff.br/ es-ilva/2012.1/seguranca/arquivos/monografia/apresentacao.pdf .
7. Diogo Mendes: Técnicas de Hacking para Anonimização na Internet (Abril de 2014).
8. Proxies, o que são?: https://pplware.sapo.pt/informacao/proxies-o-que-sao/.
9. Tor project: https://www.torproject.org/about/overview.html.en.
10. Corianna Jacoby: The Onion Router and the Darkweb (December 15, 2016).
11. Comissão Nacional de Proteção de Dados: https://www.cnpd.pt/bin/legis/nacional/lei_6798.htm.
12. Wikipédia: https://pt.wikipedia.org/wiki/Regulamento_Geral_sobre_a_Prote%C3%A7%C3%A3o_de_Dados.
13. I2P: https://geti2p.net/en/about/intro.
14. FREENET: https://freenetproject.org/pages/about.html.
15. Stefanie Roosy, Benjamin Schillerz, Stefan Hackerz, Thorsten Strufey: Measuring Freenet in the Wild: Censorship-resilience under Observation (2014).