DEEPWEB: ANONIMATO?

Cap Luiz Paulo Lopes dos Santos
Pós-graduado em Guerra Cibernética

RESUMO. O uso da Internet possibilitou o surgimento de "seções" que não são acessados por sites de busca como o Google e Bing, hospedando assim sites de forma anônima, sem registro algum, dando origem a *Deep* Web. Motores de busca como o Google contam com programas chamados de rastreadores que reúnem informações seguindo trilhas de hiperlinks que ligam tudo que está na internet, isso é chamado de indexação. Essa abordagem funciona adequadamente às páginas que compõem a Surface Web, que seria composta por todo conteúdo visivel da internet (sites e conteúdo em geral), que pode ser visitado e indexado por rastreadores nos mecanismos de busca; porém esses programas têm dificuldades em penetrar bancos de dados que não são configurados para responder a consultas digitadas pelos usuários que realizam esta busca. A *Deep* Web (também chamada de *Deepnet*, Web Invisível, *Undernet* ou Web oculta) é composta por todo conteúdo que não está na *Surface* Web, ou seja, é tudo que não está indexado por ferramentas de busca padrão, trazendo um novo modo de utilizarmos a rede.

Palavras-Chave: Segurança cibernética. Comportamento humano. Engenharia social.

INTRODUÇÃO

Segundo Paganini(2012), o Deep Dark WEB é um lugar misterioso, onde se faz o anonimato, chamado pelo autor de hacker's Paradise, sendo a porção do ciberespaço inacessível por muitos aspectos.

As regras e os procedimentos válidos para a Surface Web, que corresponde a parte da internet que é indexada, ou seja, todos os sites e bancos de dados que são reconhecidos por sites de busca como o Google, o Yahoo, Bing, são muitas das vezes alterados, e onde os mecanismos de busca através de seus rastreadores não conseguem identificar o que é site e o que não é na Deep Web.

Para um melhor entendimento, pode-se fazer analogia a um Iceberg, figura 1, como é mostrado pelo site Brandpowder, onde os buscadores são navios sob a superfície do mar com todo o conhecimento indexado à sua disposição, e a *Deep* Web é a zona profunda do mar, pela qual navegam os hackers anonimamente.

Como fala Bergma, (2001), CEO da Structured Dynamics LLC, um dos fundadores, diretor de tecnologia e presidente da Corporação Bright Planet, os mecanismos de busca utilizam numa página na internet uma espécie de scanner, varrendo todo o site com seus computadores até achar outros sites no qual o primeiro site faz referência, ou possui links relacionados.

FIGURA 1 - CONCEITO DA DEEP WEB

Fonte: www.brandpowder.com

Novamente, é feito outro vasculhamento que parte destes novos sites encontrados, analisando as páginas da Web e seguindo os links contidos nelas, como um usuário faz ao navegar na Internet. Eles avançam de link em link e transmitem, aos servidores do Google, os dados destas páginas da Web, relacionando todos os sites que são encontrados e registrados.

Esses sites são registrados nos buscadores a fim de tornar visível o site aos mecanismos de busca. Outra forma dos motores de busca obterem estes sites, ocorre quando o autor do site apresenta as suas próprias páginas da Web para serem listadas diretamente por um motor de busca.

Na *Deep* Web, os sites não seguem obrigatoriamente a mesma métrica de registro. Sites simplesmente são criados e ativados sem nenhuma espécie de registro. Sem informações, os buscadores não tem como saber de onde são os sites, muito menos como achá-los a fim de indexá-los e torná-los visíveis.

Páginas que não possuem referências ou links que as identifiquem, e apresentam conteúdo textual codificado em arquivos multimídia (imagem ou vídeo) ou formatos de arquivo específicos, acabam atuando como verdadeiros mecanismos de bloqueio de acesso ao seu conteúdo. Estas páginas tornam-se invisíveis aos scanners de rede, chamados de web crawlers, e não são manipulados pelos motores de busca.

Os motores de busca não conseguem encontrar ou recuperar o conteúdo da *Deep* Web porque muitas das fontes da *Deep* Web necessitam de consulta direta aos seus bancos de dados, e esses motores não são construídos para fazer isso.

1 UTILIZAÇÃO DA DEEP WEB

Segundo os criadores da tecnologia, pessoas usam o Tor (um navegador da internet de software livre e de código aberto que proporciona o anonimato pessoal ao navegar na Internet e em atividades online) para acessar a Deep Web, a fim de impedir que sites rastreiem seus familiares, evitar a identificação ao se conectar a sites de notícias, serviços de mensagens instantâneas ou similares, quando se encontram bloqueados pelos seus provedores de Internet. Jornalistas usam o Tor para se comunicarem de forma mais segura com contatos, como afirmado por Quintin (2014).

As organizações não-governamentais (ONGs) usam o Tor para que os seus trabalhadores possam se conectar ao seu site, enquanto estão em um país estrangeiro, sem notificarem que estão trabalhando com essa organização.

Serviços ocultos do Tor permitem aos usuários publicar web sites e outros serviços sem a necessidade de revelar a localização do site. Um ramo da marinha americana usa Tor para recolher informação de fonte aberta, e uma de suas unidades usou Tor enquanto operava no Oriente Médio recentemente como afirma Levine (2014).

Parte da população, usa o anonimato para quebrar a censura, e usufruir do livre acesso à internet e a privacidade de conversa, usufluindo do meio sem quebrar conceitos legais e/ou morais.

No entanto, existe também o uso que é ilegal, conforme apresentado no começo do trabalho. O usuário que navega na Deep WEB está mais propenso, mesmo que acidentalmente, a ser direcionado a sites de conteúdo ilegal ou impróprio. Na Deep WEB todo cuidado é pouco.

O uso ilegal da Deep Web é o que causa preocupação aos governos e o cidadão comum. Mesmo quem a conhece evita usá-la, com vistas a evitar a vinculação de seus nomes as atividades ilegais associadas a este meio, como mosta a Figura 2.

Figura 2 Site de contratação de assassinatos na Deep Web

Na Deep Web, como os sites podem

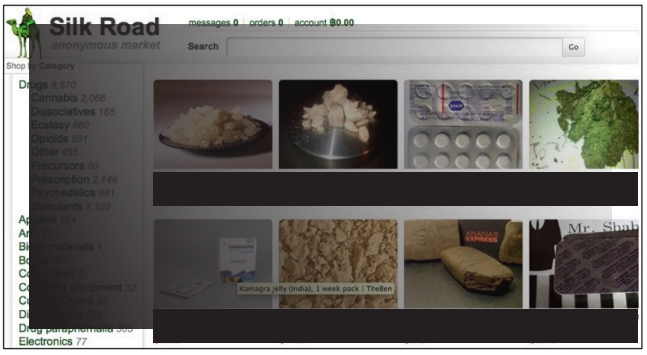
ser criados dentro de total anonimato, sem saber onde está o servidor ou quem é o dono, muitas pessoas usam essa oportunidade para realizarem atividades ilícitas, como afirma Gomes (2017), que vão desde a venda de drogas até contratação de assassinatos.

Em 2 de outubro de 2013, o FBI (Federal Bureau of Investigation) fechou um famoso site de venda de drogas da Deep Web chamado Silk Road o qual teria vendido drogas, movimentando mais de 1,2 bilhões de dólares. A existência do site foi revelada em 2011 e não podia ser acessado sem a intervenção do navegador Tor como disse Greenberg (2013).

Segundo Altieres Rohr (2013), quando um serviço na rede Tor é criado, ele é cadastrado na rede e o site não registra o endereço real de seus visitantes. A Bitcoin (moeda virtual anônima irrastreável), fazendo uso desse anonimato, tornou o site Silk Road popular, como afirma o site "buybitcoinworldwide".

Se o anonimato era tão importante para um dos sites mais famosos de venda de drogas da Deep Web, como o FBI chegou ao dono do site? Simples, por intermédio da engenharia social! Dois clientes do site ameaçaram divulgar informações sobre seus usuários. Aliás, um deles era ex-funcionário do Silk Road.

Figura 3 Site Silk Road de venda de drogas na Deep Web



O dono do site, Ross William Ulbricht, teria contratado um assassino de aluguel, serviço que também pode ser achado na Deep Web, para matá-los e acabar com as ameaças. Porém, o assassino de aluguel era na verdade um agente secreto do FBI, que falsificou a realização do homicídio, e chegou até o local onde o ex-funcionário do site estaria.

Outros erros foram cometidos por Ulbricht, tal como participar de fóruns on-line não anônimos, publicando endereços com o nome de seu site Silk Road, usando inclusive seu e-mail pessoal para que interessados entrassem em contato para colaborar com seu "projeto".

Ulbricht usou seu e-mail pessoal no fórum, também se cadastrou em sites para programadores e pediu ajuda para criar códigos relacionados ao uso de serviços ocultos na rede Tor. Em redes sociais divulgou por conta própria o Silk Road, o que facilitou ainda mais sua identificação pelas autoridades.

O relato exposto caracteriza bem o maléfico uso da deep web e, como o site DailyMail (2011) apresentou, não se trata de mau uso isolado do ambiente anônimo. Em dada ocasião, o grupo de hackers Anonymous publicou 190 IPs de usuários acusados de prática de atividades ligadas à pedofilia, exemplos que reforçam o mau uso da Deep Web.

Verificou-se, que, embora tenha havido esforços de autoridades americanas em prender o dono e fechar o site Silk Road na Deep Web em 2011, o site voltou à ativa, verificado no mês de setembro de 2014, com o nome de Silk Road 2.0, e que mantém todas as atividades normalmente, incluindo também a venda de materiais eletrônicos, livros, quadros, álcool, jóias, entre outros. Consegue-se achar diferentes tipos de sites na Deep Web, pode-se até encontrar uma réplica do site Facebook, que na Deep Web se chama "Torbook", e até mesmo uma réplica do Twitter, "Twitter Clone".

2 ANONIMATO SEGURO?

Percebe-se que, quer sejam agentes governamentais ligados à atividade de inteligência ou agentes macomunados em práticas ilegais, o anonimato é um fator extremamente relevante na deep web, mas é apenas uma das preocupações de seus usuários.

Segundo Mitnik (2018), a eficiência

de qualquer sistema de segurança está diretamente relacionada aos usuários do sistema. O fator humano sempre será o elo fraco na cadeia e, portanto, o mais explorado. Segundo essa lógica, e conforme comprovações supracitadas, mesmo o ambiente hermeticamente criado para produzir anônimato é incapaz de fazê-lo, porquanto seus usuários sempre deixam rastros que os identificam.

Por exemplo, não adianta se preocupar com o anonimato da rede se forem cometidos erros de se expor na Surface Web, como utilizar e-mails particulares em blogs na Deep Web, utilizar nomes verdadeiros, divulgando assim a sua identidade dentro de uma rede criptografada.

A criptografia da rede Tor só funciona dentro da rede junto com os nós de entrada ou os nós intermediários. O grande problema da criptografia da rede Tor são os nós de saída. Esses nós de saída decriptografam o conteúdo para fazer a integração com o site no qual se faz a comunicação.

Ou seja, um provável usuário que esteja tentando ver o conteúdo que está trafegado na rede, tem apenas que ficar no nó de saída do Tor, cuja lista está disponível publicamente, e ver o conteúdo dos dados que está trafegando com um analisador de tráfego.

Para corrigir isso, é necessário usar uma criptografia fim a fim, como o SSL. Como no próprio site do ToR-Project fala, o navegador Tor é uma solução parcial à anonimidade.

Acredita-se que grande parte desses nós de saída são vigiados por governos para saber o que está tramitando na rede, a fim de verificar o conteúdo do tráfego, como cita Altieres Rohr (2014), editor do site de segurança Linha Defensiva, quando fala que a internet inteira nasceu de um projeto das forças armadas norte-americanas e que a intenção não é "colocar uma pedra no próprio sapato".

Rohr ainda fala que a NSA (National Security Agency) tem uma missão conflitante, pois precisa possuir a capacidade de espionar as comunicações, e caso a tenha em larga escala, provavelmente agentes adversários também a terão, o que colocará a segurança nacional dos Estados Unidos em risco.

Em prol disso, Altieres Rohr afirma que os chamados "nós de saída" são controlados pela NSA e outras agências de espionagem. Tais agências têm acesso a todo o conteúdo que sai e entra na rede, funcionando para ocultar a origem das comunicações, mas não protege conteúdo algum.

Em seu artigo para a Wired Magazine, Zetter (2007) expõe que um consultor de segurança de computadores sueco Dan Segerstad revelou nomes de usuário e senhas de mais de 100 contas de e-mails usados por vítimas, através da informação do acolhimento de cinco nós Tor de saída colocados em locais diferentes na internet.

Segundo Zefter (2007) Dan Segerstad, disse em entrevista que:

> É aprovado pelo EFF (Electronic Frontier Foundation), organização sem fins lucrativos sediada em San Francisco, Califórnia, cujo objetivo declarado é proteger os direitos de liberdade de expressão, e outros grupos de defesa das liberdades civis como método de denunciantes e os trabalhadores de direitos humanos para se comunicar com os jornalistas, entre outros usos.

Porém, como já foi dito aqui, o Tor somente promove a anonimidade não sabendo de onde vem a informação, mas para o seu conteúdo também ser anônimo, precisa da criptografia SSL.

No dia 30 de Julho de 2014, a rede Tor sofreu um ataque que tentou expor seus usuários. No post de seu blog oficial em 2014, a equipe do ToR-Project afirma ter identificado alguns computadores, que voluntariamente aderiram ao sistema (os chamados "relays"), tentando identificar seus usuários.

Segundo TOR *Security Advisory* (2014):

> Parece que eles estão mirando em

> pessoas que operam ou acessam os serviços anônimos do Tor. O ataque envolveu em modificações em protocolos, exigindo 'ataques de confirmação de tráfego'.

Esse ataque foi uma tentativa de localizar a origem do tráfego através dos nós que compõem a rede, a equipe do ToR-Project descobriu que os "relays" entraram na rede em 30 de janeiro de 2014 e foram removidos no dia 4 de julho de 2014. O post no blog oficial diz:

> como não sabemos quando começou o ataque, os usuários que usaram serviços anônimos nesse período devem presumir que foram afetados.

Como resposta, ToR-Project avisa que removeu os "relays" dos quais tomou conhecimento, atualizou o software de seu navegador (e aconselha seus usuários a realizarem o mesmo procedimento).

CONCLUSÃO

Para navegar na rede oculta de computadores, concluiu-se que o mais importante é incorporar procedimentos de salvaguarda e segurança, tais como:

- não instalar addons, (recursos adicionais que complementam um programa), pois podem ter falhas ou vulnerabilidades;
- acessar somente sites que tenham criptografia HTTPS (protocolo HTTP com Security) o qual fornece criptografia dos dados tramitados entre a máquina e o site no qual está se fazendo o acesso; e
- não abrir documentos através do navegador, prática comum em alguns e-mails, como, por exemplo, o Gmail e o Hotmail, que o usuário pode visualizar e editar arquivos no próprio Browser, sem fazer o download para a máquina.

Acessar a Deep Web, é utilizar um SO chamado Tails, que foi desenvolvido para que seus usuários acessem a rede Tor, e se mantenham anônimos na internet, com algumas características que favorecem esse anonimato.

Caso a navegação seja realizada sem seguir esses cuidados, pode ocorrer a quebra do anonimato ou causar contaminação na máquina, fortalecendo o acúmulo de rastros da navegação.

Também pode haver a danificação da máquina por algum malware que tenha se obtido durante a navegação da Deep Web, caso isso ocorra, é recomendado a formatação.

A Deep Web ainda é um território digital pouco estudado e por demais mistificado. O advento da guerra cibernética e a crescente preocupação dos governos com a segurança virtual de suas infraestruturas críticas, certamente, promoverão, maiores e diversificados estudos, a respeito desse espaço, ainda, pouco explorado.

DEEP WEB: ANONYMITY?

ABSTRACT. The use of the Internet allowed the appearance of "places" that are not accessed by search engines such as Google and Bing, thus hosting anonymous sites without any registration giving rise to Deep Web. Search engines like Google rely on programs called crawlers that gather information by following trails of hyperlinks that link everything that is on the internet, it's called indexing. This approach works properly to the pages that make up the Surface Web, which is formed by all the content of the Internet, sites, content in general, that can be visited and indexed by crawlers in the search engines; But these programs have difficulties in penetrating databases that are configured to respond to queries typed by users who perform this search. The Deep Web (also called Deepnet, Invisible Web, Undernet or Web Hiding), is composed of all content that is not on the Web surface, that is, it is anything that is not indexed by standard search tools, bringing a new How to use the network.

Keywords: Cyber security. Human behavior. Social Engineering.

REFERÊNCIAS

GOMES, HELTON. **Da Dark Web a pen-drives engolidos:**

como a PF investiga pornografia infantil na internet, 07 agosto 2017. Disponivel em: <https://g1.globo.com/tecnologia/noticia/da-dark-web-a-pen-drives-engolidos-como-a-pf-investiga-pornografia-infantil-na-internet.ghtml>. Acesso em: 21 Fevereiro 2018.

GREENBERG, ANDY. **End Of The Silk Road:** FBI Says It's Busted The Web's Biggest Anonymous Drug Black Market, 02 outubro 2013. Disponivel em: < https://www.forbes.com/sites/andygreenberg/2013/10/02/end-of-the-silk-road-fbi-busts-the-webs-biggest-anonymous-drug-black-market/#12ce49325b4f>. Acesso em: 21 Fevereiro 2018.

_____. **Bitcoin Anonymity** - Is Bitcoin Anonymous?. Disponivel em: <https://www.buybitcoinworldwide.com/anonymity/>. Acesso em: 21 fevereiro 2018.

BBC. G1. Internet oculta: os segredos de um universo paralelo, 19 Julho 2014. Disponivel em: <http://g1.globo.com/tecnologia/noticia/2014/07/internet-oculta-os-segredos-de-um-universo-paralelo.html>. Acesso em: 19 Julho 2017.

BECKETT, A. **The Guardian.** The dark side of the internet, 26 Novembro 2009. Disponivel em: <http://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet>. Acesso em: 26 Agosto 2017.

BERGMA, M. K. **White Paper: The Deep Web**: Surfacing Hidden Value, Agosto 2001. Disponivel em: <http://quod.lib.umich.edu/cgi/t/text/text-idx?c=jep;view=text;rgn=main;idno=3336451.0007.104>. Acesso em: 28 Setembro 2017.

BREWSTER, T. F. Forbes. **Can You Completely Trust Tor To Protect Your Privacy?**, 10 Julho 2014. Disponivel em: <http://www.forbes.com/sites/thomasbrewster/2014/07/30/can-you-completely-trust-tor-to-protect-your-privacy-fresh-attacks-would-suggest-not>. Acesso em: 06 Agosto 2017.

BRIGHT PLANET, D. W. I. **DEEP WEB:** A PRIMER, 2014. Disponivel em: <http://www.brightplanet.com/deep-web-university-2/deep-web-a-primer/>. Acesso em: 28 Julho 2017.

CARDOSO, C. **Putin oferece US$ 111 mil pra quem quebrar o Tor**, 26 julho 2014. Disponivel em: <http://meiobit.com/293647/russia-kgb-oferecera-111-mil-dolares-para-quem-quebrar-o-tor/>. Acesso em: 26 Julho 2017.

DIGITAL, R. O. V**eja 4 cuidados na hora de usar o Tor**, navegador da Deep Web, 21 Agosto 2014. Disponivel em: <http://m.olhardigital.uol.com.br/noticia/veja-4-cuidados-na-hora-de-usar-o-tor-navegador-da-deep-web/43682>. Acesso em: 28 Agosto 2017.

DREDGE, S. The Guardian. **What is Tor?** A beginner's guide to the privacy tool, 05 Novembro 2013. Disponivel em: <http://www.theguardian.com/technology/2013/nov/05/tor-beginners-guide-nsa-browser>. Acesso em: 09 Setembro 2017.

ESTES, A. C. Gizmodo. **Rússia abre concurso caça-níquel para quem quiser tentar quebrar o Tor**, 28 Julho 2014. Disponivel em: <http://gizmodo.uol.com.br/russia-concurso-tor/>. Acesso em: 30 Julho 2017.

GLENNY, M. The New York Times. **Cyber Subterfuge,** 27 Novembro 2013. Disponivel em: <http://www.nytimes.com/2013/11/28/opinion/cyber-subterfuge.html?pagewanted=all&module=Search&mabReward=relbias%3As%2C%7B%222%22%3A%22RI%3A18%22%7D>. Acesso em: 21 Agosto 2017.

GUERNESY, L. The New York Times. **Mining the 'Deep Web' With Sharper Shovels**, 25 Janeiro 2001. Disponivel em: <http://www.nytimes.com/2001/01/25/technology/mining-the-deep-web-with-sharper-shovels.html?module=Search&mabReward=relbias%3As%2C%7B%222%22%3A%22RI%3A18%22%7D>. Acesso em: 21 Agosto 2017.

HERN, A. The Guardian. **US government increases funding for Tor**, giving $1.8m in 2013, 29 Julho 2014. Disponivel em: <http://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router>. Acesso em: 26 Agosto 2017.

KAUFMAN, L. Media Decoder. Book by 2 From Google Takes a Deep Look at the Web, 2 Dezembro 2012. Disponível em: <http://mediadecoder.blogs.nytimes.com/2012/12/02/a-book-by-two-from-google-takes-a-deep-look-at-the-web/?_r=0>. Acesso em: 21 Agosto 2017.

KISS, J. The Guardian. **Tor 'deep web' servers go offline as Irish man held over child abuse images**, 06 Agosto 2013. Disponível em: <http://www.theguardian.com/technology/2013/aug/05/tor-deep-web-servers-offline-freedom-hosting>. Acesso em: 06 Agosto 2017.

MACDIARMID, P. Exame. Computadores do governo alteraram Wikipedia, 28 Agosto 2014. Disponível em: <http://exame.abril.com.br/tecnologia/noticias/computadores-do-governo-alteraram-wikipedia-diz-folha>. Acesso em: 30 Agosto 2017.

PAGANINI, P. **The Deep Dark Web**. 212 Providence St: Paganini-Amores, 2012.

QUINTIN, C. **7 coisas que você precisa saber sobre o Tor**, 04 Julho 2014. Disponível em: <http://gizmodo.uol.com.br/7-coisas-que-voce-precisa-saber-sobre-o-tor/>. Acesso em: 07 Julho 2017.

ROHR, A. G1. **Conheça a Deep Web e a 'internet invisível', 06 janeiro 2012**. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/conheca-a-deep-web-e-a-internet-invisivel.html>. Acesso em: 26 agosto 2017.

_____. **É possível combater a censura sem ajudar o crime na internet?**, 29 Outubro 2013. Disponivel em:

<http://g1.globo.com/tecnologia/blog/seguranca-digital/post/e--possivel-combater-a-censura-sem-ajudar-o-crime-na-internet.html>. Acesso em: 01 Agosto 2017.

_____. **Se a rede Tor foi desenvolvida pelos EUA, ela é confiável?**, 13 fevereiro 2014. Disponivel em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/pacotao--se-rede-tor-foi-desenvolvida-pelos-eua-ela-e-confiavel.html>. Acesso em: 26 Agosto 2017.

STATCOUNTER. Stat Counter Global Stats. [S.l.]: [s.n.]. Disponivel em: <http://gs.statcounter.com/#desktop+console-os-ww--monthly-201406-201408>. Acesso em: 26 Setembro 2017.

TOR security advisory. “relay early” traffic confirmation attack, 30 Julho 2014. Disponivel em: <https://blog.torproject.org/blog/tor-security-advisory-relay-early-traffic-confirmation-attack>. Acesso em: 05 setembro 2017.

WILLIAMS, A. C. **Russia Declares War On Bloggers With Sweeping New Censorship Law**, 07 Maio 2014. Disponivel em: <http://thinkprogress.org/world/2014/05/07/3435292/what-its-like-to-use-the-internet-in-russia/>. Acesso em: 28 Julho 2017.

WRIGHT, A. **Exploring a ‘Deep Web’ That Google Can’t Grasp**, 22 Fevereiro 2009. Disponivel em: <http://www.nytimes.com/2009/02/23/technology/internet/23search.html?pagewanted=1&_r=0&th&emc=th>. Acesso em: 21 Agosto 2017.

ZETTER, K. **Rogue Nodes Turn Tor Anonymizer Into Eavesdropper’s Paradise**, 09 outubro 2007. Disponivel em: <http://archive.wired.com/politics/security/news/2007/09/embassy_hacks>. Acesso em: 01 Setembro 2017.

LEVINE, YASHA. **Almost everyone involved in developing tor was (or is) funded by the us government**, 14 julho 2014. Disponivel em: < https://www.infowars.com/almost-everyone--involved-in-developing-tor-was-or-is-funded-by-the-us-government/>. Acesso em: 21 Fevereiro 2018.

O autor é graduado em Ciências Militares pela Academia Militar das Agulhas Negras (2011). Tem experiência na área de Defesa, com ênfase em Defesa Cibernética. Carreira desenvolvida nas áreas de TI, Redes, Infraestrutura e Segurança da Informação e Telecomunicações. Dentro da área de segurança da informação, possui possui expertise em Forense computacional, Tratamento de incidentes de segurança da informação, Políticas de segurança da informação, Auditoria, Hardening Linux, Segurança física e Firewall. Possui proficiência em Inglês nível intermediário e pode ser contactado pelo email luizpaulo.santos@eb.mil.br.