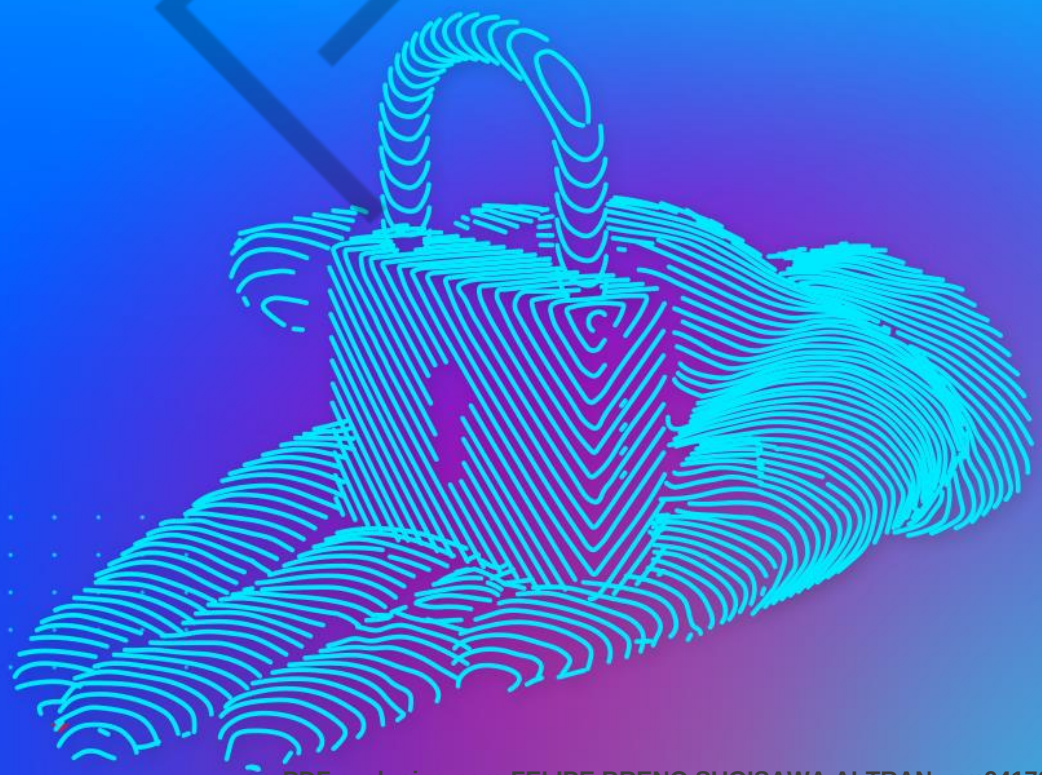
FIAP ON

BIOHACKING, DEEP WEB E CRIPTOGRAFIA

DEEP WEB – DEFINIÇÃO E CARACTERIZAÇÃO

OSMANY D.R DE ARRUDA



3

LISTA DE FIGURAS

SUMÁRIO

3 DEEP WEB – DEFINIÇÃO E CARACTERIZAÇÃO

De acordo com Forouzan (2008), as redes podem ser entendidas como um conjunto de dispositivos de comunicação, como computadores, entre outros, conectados entre si; sendo internet (reparar no “i” minúsculo) o termo empregado para definir redes que podem se comunicar entre si. Ainda segundo o referido autor, a Internet (reparar no “i” maiúsculo), surgida em 1969, é a mais notável entre as internets, representando o resultado da colaboração entre milhares e milhares de redes interconectadas, atingindo, assim, abrangência mundial.

Com base em pesquisa realizada pelo Pew Research Center, intitulada *The Web at 25 in the U.S.* (2014), Büchi, Just e Latzer (2016) afirmam que, no futuro, somente os mais afortunados saberão como proteger sua privacidade, enquanto, para muitos, os ganhos imediatos obtidos pela divulgação indiscriminada de suas informações superarão as preocupações. Ou seja, em função disso, a privacidade e o controle sobre informações pessoais poderão se tornar, essencialmente, “artigos de luxo”.

Hoffman, Novak e Venkatesh (2004) alertam ainda para três relevantes questões que, certamente, continuarão a ganhar importância nas próximas décadas: a privacidade, a proteção e a segurança dos dados. Para eles, a onipresença da Internet tem um lado obscuro, na medida em que relatos sobre “roubos” de identidade continuam aumentando, mensagens ofensivas persistem e, ainda, a sociedade fica angustiada diante das potenciais consequências advindas do acesso – por crianças – de informações e conteúdos inadequados.

Embora os termos “Internet” e “World Wide Web” sejam por vezes empregados indiscriminadamente por alguns como sinônimos, é importante que seja estabelecida a diferença entre eles. Tendo-se a definição de Internet já anteriormente exposta, pode-se simplificadamente entender a World Wide Web (ou simplesmente, www) como um sistema de documentos em hipermídia, interligados e executados na Internet.

De acordo com Pompéo e Seefeldt (2013), a busca por conteúdo na Internet pode ser executada com duas abordagens diferentes: (a) a primeira delas na Internet já “conhecida e tradicional”, denominada s*urface web*. A segunda, na

chamada (b) *deep web*. Enquanto a *surface web* se refere às páginas facilmente encontradas por mecanismos de busca, a *deep web* tem como foco páginas que, pelos mais diferentes motivos, ficam alheias aos provedores de conteúdo tradicionais, dada a forma diferenciada como são indexadas, não aparecendo em buscas tradicionais.

Em outras palavras: "[...] cada página da rede possui padrões que as registram em servidores, como 'Google' e 'Yahoo!'. Caso não sigam os padrões definidos, elas ficam à margem da listagem de seus resultados de pesquisa, mesmo que contenham o conteúdo pesquisado pelo usuário" (POMPÉO E SEEFELDT, 2013). A Figura "As camadas da Internet" ilustra a ideia geral das camadas da Internet.

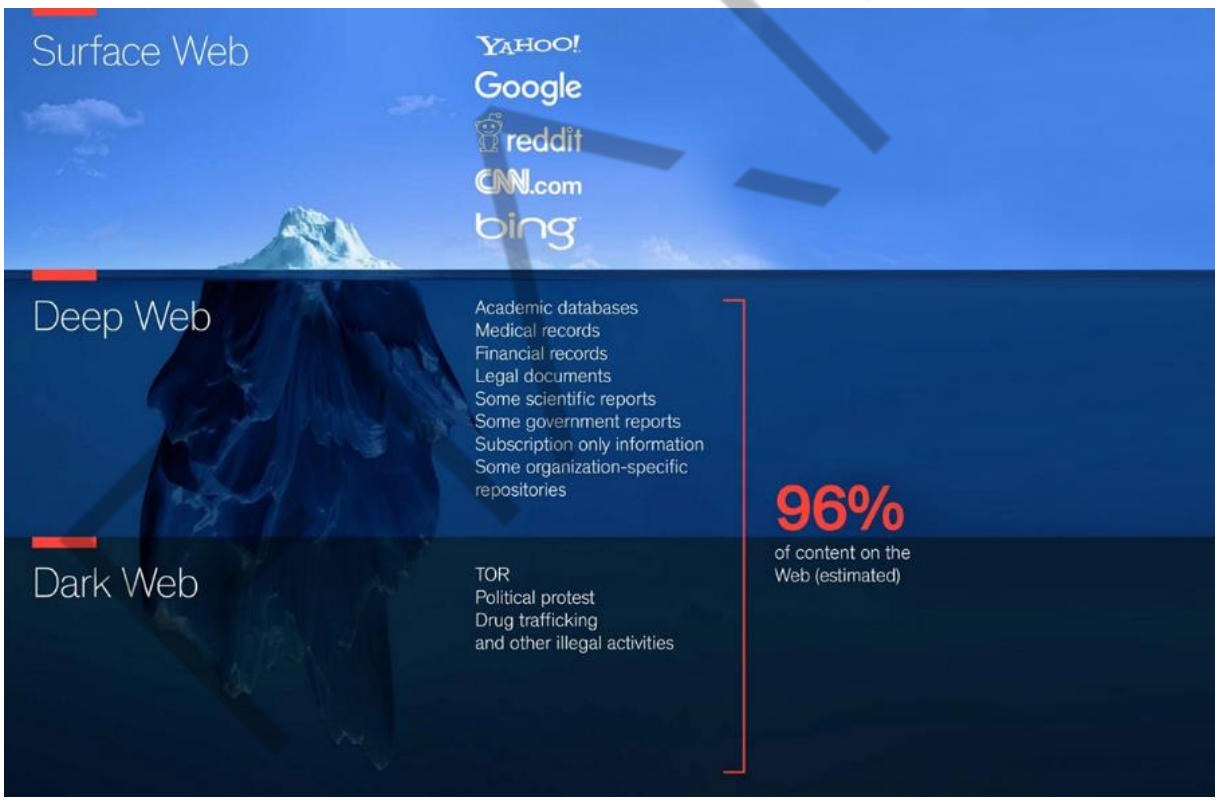


Figura 3.1 – As camadas da Internet
Fonte: https://medium.com/@smartrac/ (2020)

O site MEDIUM.COM ilustra as diferentes camadas da Internet com base em uma analogia com um *iceberg*, em que na parte superior, conhecida como s*urface web*, têm-se os provedores de conteúdo e mecanismos de busca tradicionais, a exemplo do Google, Yahoo e Bing, entre outros.

Imediatamente abaixo da *surface web* vem a *deep web*, em que, ainda segundo o referido site, encontra-se conteúdo específico, não indexado pela *surface*

web (e, portanto, inacessível a partir dela), como, por exemplo, registros médicos e financeiros, ou, ainda, alguns relatórios científicos e governamentais, entre outros tipos de informação. A *deep web* inclui um subconjunto de conteúdo referido como *dark web*, residente em *darknets*. A utilização de *darknets* inclui (mas não se limita) atividades ilegais, a exemplo de redes terroristas, pedófilos e traficantes de drogas.

3.1 As profundezas da grande rede

O termo *deep web* foi cunhado por Michael K. Bergman, fundador da *Bright Planet* (<https://brightplanet.com/>), empresa especializada em coletar, classificar e procurar conteúdo na *deep web* para uso corporativo. De acordo com Bergman (2001), a importância da coleta de informações na web e o papel inquestionável dos mecanismos de busca – mais a frustração expressada por usuários em relação à eficiência desses mecanismos – fazem deles o foco óbvio de investigação.

A fim de melhor expressar a importância da coleta de informações da *deep web*, Bergman (2001) acrescenta ainda que: “Até Van Leeuwenhoek haver observado pela primeira vez uma gota d’água sob o microscópio no final dos anos 1600, a pessoas não tinham ideia que havia um mundo inteiro de ‘animáculos’ além de sua visão”. Ainda de acordo com esse autor, os mecanismos de busca obtêm suas listagens (indexam o conteúdo) de duas maneiras diferentes: (a) os autores cadastram suas *web pages* diretamente nesses mecanismos ou, (b) elas são rastreadas seguindo-se seus *hyperlinks*. Esta última é a forma que retorna o maior volume de informações.

Em seu trabalho, Pompéo e Seefeldt (2013) afirmam que a *deep web* é constituída por sites dispersos por toda a Internet, os quais, entretanto, são propositalmente programados para não serem encontrados, mantendo, dessa forma, a *deep web* oculta do grande público, nas “profundezas” da rede. A Figura “A *surface web*” representa as limitações dos mecanismos de busca típicos, nos quais o conteúdo identificado limita-se ao encontrado na superfície, sendo a coleta bastante indiscriminada.

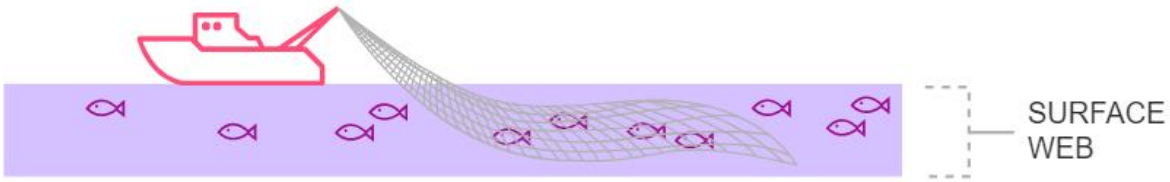


Figura 3.2 – A *surface web*
Fonte: https://quod.lib.umich.edu (2020)

Um enorme valor reside abaixo desse conteúdo superficial, a informação está lá, mas escondida sob a superfície da web (BERGMAN, 2001). Em 1994, o Dr. Jill Ellsworth empregou pela primeira vez o termo "*invisible web*" (web invisível) ao fazer referência ao conteúdo (informação) "invisível" aos mecanismos de busca convencionais. Em seu trabalho, entretanto, Bergman (2001) evita o emprego do termo "web invisível" por considerá-lo impreciso, uma vez que, sob sua perspectiva, "A única coisa 'invisível' sobre bancos de dados pesquisáveis é que eles não são indexáveis nem podem ser consultados por mecanismos de busca convencionais".

3.2 Os perigos da "invisibilidade" e o Tor

Em seu trabalho, Pompéo e Seefeldt (2013) afirmam que a restrição do conteúdo a membros de grupos específicos, bem como o compartilhamento de dados por governos estatais representam dois, dentre vários outros, motivos que poderiam justificar a não indexação de páginas da *deep web*, por mecanismos tradicionais de buscas. "Seria ingênuo demais, é claro, pensar que, em meio à imensidão da *deep web,* não existam ações que controvertam as normas legais vigentes" (POMPÉO & SEEFELDT, 2013).

Para melhor abordagem do tema, faz-se conveniente, ainda, introduzir o conceito de *dark web*. Pederson (2013) refere-se a esta última como qualquer página web que tenha sido ocultada ou que resida em uma camada separada, mas pública, da Internet-padrão. Conforme anteriormente discutido, a Internet é construída sobre páginas que fazem referência umas às outras. Se uma página de destino não tiver *links* de entrada que a referenciem, ela permanecerá oculta dos mecanismos de busca tradicionais e dos usuários até que sua URL exata se torne conhecida.

Pederson (2013) acrescenta que as VPNs (*Virtual Private Networks*) são um dos aspectos da *dark web* encontrados na Internet pública, tendo no Tor (*The Onion*

Router) um dos exemplos mais conhecidos. A Tor *network* é uma rede aberta, oculta dentro da Internet pública, cujo conteúdo diferenciado pode ser acessado, exclusivamente, por meio de seu próprio *web browser*, um software livre também chamado Tor.

Neste sentido, Pederson (2013) destaca que enquanto a liberdade pessoal e a privacidade são objetivos louváveis, o anonimato oferecido pela rede Tor para navegação na Internet tem proporcionado uma plataforma sólida para práticas consideradas ilegais em diferentes países incluindo, dentre outras:

- Comércio de substâncias controladas.
- Vendas de diferentes tipos de armas.
- Pornografia infantil.
- Vazamento de informações sensíveis.
- Lavagem de dinheiro.
- Violação de direitos autorais.
- “Roubo” de identidade e fraudes com cartões de crédito.

De acordo com o site vpnoverview.com, o Tor é útil, porém, tem suas imperfeições, não garantindo navegação tão anônima quanto apregoado por eles, pois já teve sua proteção quebrada no passado. Quando isso aconteceu, o projeto Tor afirmou não haver sido sua rede, propriamente dita, quebrada; mas, sim, navegadores individuais. Com o auxílio de provedores de acesso à Internet, autoridades podem vir a expor a identidade de usuários do Tor.

Embora isso ocorra apenas pontualmente, de forma especial, mediante suspeitas fundamentadas de práticas delituosas, evidencia também, em última análise, que o anonimato promovido pelo Tor realmente não é total. Em 2015, o site extremetech.com publicou artigo descrevendo, em linhas gerais, como pesquisadores do MIT (Massachusetts Institute of Technology) quebraram o anonimato do Tor sem, entretanto, quebrar a criptografia utilizada por ele. O processo tinha início no nó de entrada da rede (algumas vezes, referenciado como *guard node*), único conhecedor do endereço IP real do usuário que envia a solicitação.

O próximo nó da sequência só conhece o IP do nó de entrada, o seguinte conhece apenas o endereço IP do nó anterior e assim sucessivamente até chegar ao destino. Dessa forma, pretende-se evitar que outras pessoas venham a identificar quem está acessando qual site via Tor, especialmente, se esse site estiver oculto (*hidden service*) dentro da própria rede deste, a exemplo do extinto *Silk Road* e similares. Ou seja, além da navegação anônima na Internet, o Tor oferece ainda *hidden services*, serviços que protegem o anonimato também do site de destino. Segundo o extremetech.com, a quebra da criptografia para revelar os usuários do Tor é um processo complicado e não poderia ser feito de forma confiável na ocasião (2015).

Leia mais em: <https://www.extremetech.com/extreme/168277-silk-road-how-to-be-a-deep-web-criminal-and-get-away-with-it>

Isso posto, ao invés de tentar quebrar a criptografia, o MIT optou por realizar um *fingerprint* inteligente do tráfego. O ataque tem como alvo o nó de entrada da rede (Figura “Representação simplificada da rede Tor”), basicamente, o atacante configura um computador na rede Tor como um nó de entrada e espera pelas solicitações enviadas por usuários através desse nó. Quando uma conexão for estabelecida pelo Tor, dados são trocados entre nós à frente e atrás.

Os pesquisadores do MIT usaram algoritmos de aprendizado de máquina para monitorar esses dados e contar os pacotes. Com base unicamente nessa métrica, o sistema pode determinar com 99% de precisão que tipo de recurso o usuário acessava (por exemplo, a web aberta ou um serviço oculto, entre outras possibilidades).

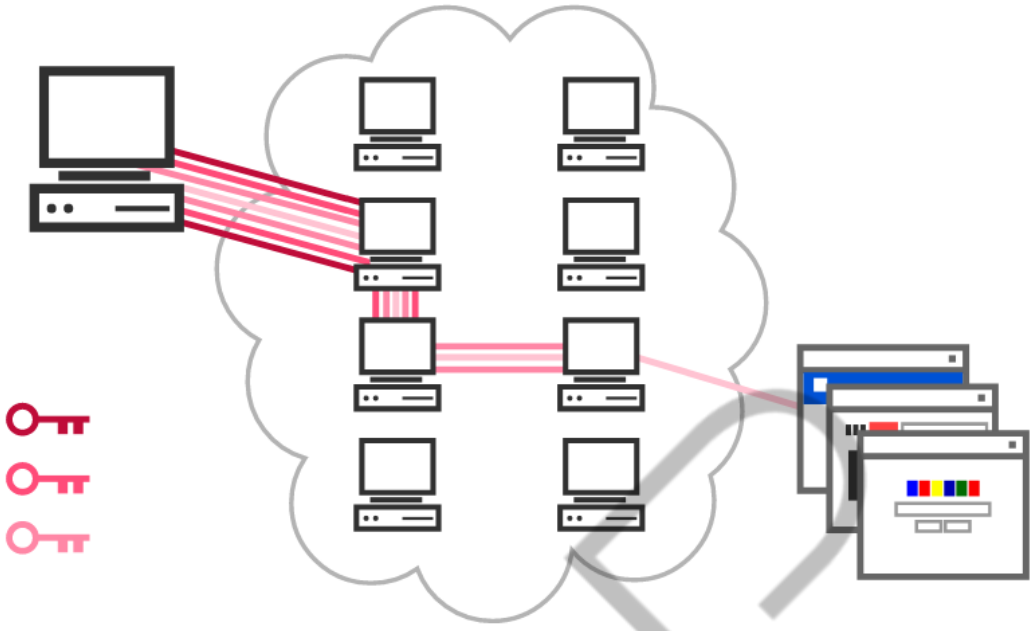


Figura 3.3 – Representação simplificada da rede Tor
Fonte: https://www.extremetech.com (2020)

Com base no *fingerprint* do tráfego, mais especificamente no padrão de pacotes enviados, os pesquisadores do MIT afirmaram ser possível identificar com 88% de precisão os *hidden services* (rebatizados pelo Tor de *onion services*) acessados pelo usuário. Isso é possível em razão de ser o computador de um atacante o nó de entrada utilizado pela vítima para acesso à rede (*guard node*). Entretanto, há que se observar que o nó de entrada é escolhido aleatoriamente a cada sessão, o que significa que um atacante terá de rodar vários *guard nodes* para identificar uma quantidade significativa de conexões e seria muito difícil direcionar-se a um usuário específico.

De acordo com o trabalho dos pesquisadores do MIT, a correção para esse ataque é simples. A rede Tor precisa começar a enviar pacotes fictícios que façam todas as solicitações parecerem iguais. Se não houver um padrão discernível para os dados, o destino não poderá ser determinado. Os desenvolvedores do Tor reconheceram o problema e, à época (2015), já consideravam as possíveis formas para implementação de uma correção.

3.3 As ameaças surgidas da *dark web* e redes para anonimato

Chertoff e Simon (2015) definem a *dark web* como a porção da *deep web* que foi intencionalmente ocultada e tornada inacessível aos *web browsers* comuns.

Ainda segundo os referidos autores, os sites da *dark web* servem como plataforma para aqueles em que o anonimato é essencial, uma vez que, além de protegerem contra usuários não autorizados, geralmente utilizam criptografia para evitar monitoramento.

Além da já bem conhecida rede Tor, outras redes, como a I2P, oferecem muitos dos recursos ofertados pela primeira. Entretanto, a I2P (https://geti2p.net/pt/about/intro) foi projetada para ser uma rede dentro da Internet, mantendo seu tráfego confinado a seus limites. De acordo com o site do projeto I2P, esta é uma rede anônima, que expõe uma camada simples que os aplicativos podem usar para trocar mensagens de forma anônima e segura entre si. Toda a comunicação utiliza criptografia fim a fim (quatro camadas, no caso do envio de mensagens). Embora seja uma rede estritamente baseada em mensagens, há uma biblioteca disponível que permite a transmissão confiável de *streaming*.

Outra rede que merece destaque é a *Freenet* (https://freenetproject.org/). Esta é uma rede de publicação anônima, ponto a ponto, totalmente distribuída, que oferece maneiras seguras para armazenar dados e algumas abordagens que tentam endereçar a carga de *flash floods*. Enquanto a *Freenet* é projetada como um repositório de dados distribuídos, as pessoas criaram aplicativos sobre ela para fazer uma comunicação anônima mais genérica, como sites estáticos e *message boards*.

De acordo com o site da I2P, a *Freenet* oferece substanciais benefícios em relação à sua rede, uma vez que, sendo um repositório de dados distribuído, diferentemente da I2P, permite às pessoas buscarem conteúdo publicado por terceiros, mesmo quando eles não estiverem mais on-line. Paganini (2012) afirma que o anonimato na Internet é alcançado quando endereços IP não podem ser rastreados, e as informações do usuário são ocultadas, evitando, assim, quaisquer atividades de monitoramento. Entretanto, isso torna a *dark web* muito apropriada para cibercriminosos, os quais estão constantemente tentando esconder seus rastros.

Chertoff e Simon (2015) apontam ainda que a *dark web* é também o canal preferido para os governos trocarem documentos secretamente, para jornalistas burlarem a censura do Estado e, ainda, para dissidentes evitarem o controle de regimes autoritários. No início do século XXI, Grabosky (2001) afirmou que o crime

virtual não é diferente do crime (no mundo) real – é simplesmente executado de uma nova forma.

Reforçando, e complementando, o anteriormente exposto, Chertoff e Simon (2015) afirmam que a *dark web* e o terrorismo parecem se completar, no sentido de que o último precisa de uma rede prontamente disponível, entretanto, geralmente inacessível. Seria difícil para os terroristas manterem-se na *surface web*, dada a facilidade com a qual seus sites poderiam ser tirados do ar e, ainda pior, a facilidade com a qual seus autores poderiam ser rastreados. Outras ameaças características da *dark web*, apontadas por Chertoff e Simon (2015), recaem sobre o hacktivismo – o qual tem no grupo Anonymous um de seus representantes mais notórios, e os e*xploits markets*.

Estes últimos podem ser definidos como plataformas para comercialização de *zero-day exploits*, ou seja, *exploits* que exploram vulnerabilidades ainda desconhecidas por determinado fornecedor ou outros com interesse em mitigá-las.

Em matéria publicada em 2018, a *Computerworld* afirmou que:

> Ao encontrar o tipo certo de falha Zero Day de um iPhone, um usuário pode vendê-lo para a Zerodium e ganhar até US$ 1,5 milhão, de acordo com a empresa. Corretores como eles vendem somente para o complexo de espionagem militar, mas a polícia secreta de regimes controladores em todo o mundo também pode comprar essas falhas para hackear jornalistas ou perseguir pessoas.

Ainda de acordo com os referidos autores, sites como o do Banker & Co. e InstaCard viabilizam transações financeiras não rastreáveis, valendo-se de diversos meios. Por exemplo, a lavagem de bitcoins – disfarçando dessa maneira a verdadeira origem das transações, ou fornecendo a seus usuários cartões de débito anônimos, emitidos por um banco. Usuários também podem receber cartões de crédito virtuais emitidos por operadores confiáveis na *dark web*.

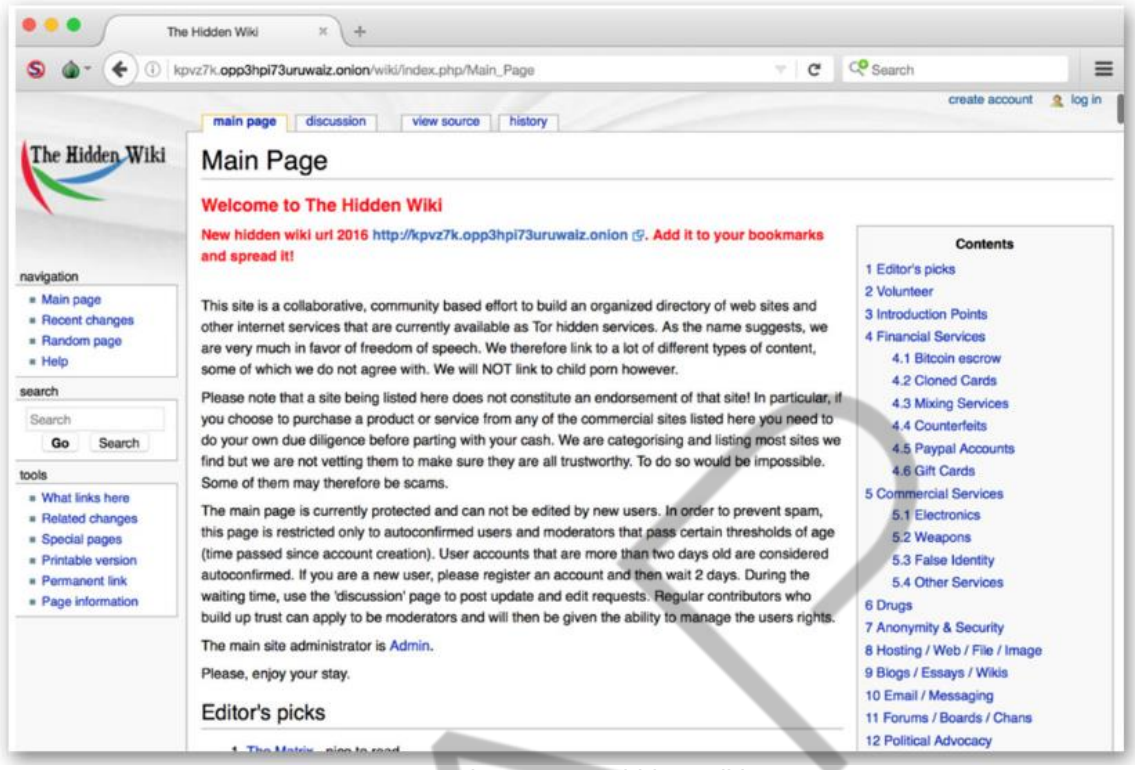


Figura 3.4 – Hidden Wiki
Fonte: https://www.darkowl.com/blog/2017/3/9/a-hidden-story-behind-the-hidden-wiki (2020)

Williams (2011) se refere à Hidden Wiki (Figura “Hidden Wiki”) como o principal diretório da *dark web*, no qual também são promovidas atividades ilegais, como lavagem de dinheiro, assassinatos por encomenda, ataques cibernéticos e acesso a produtos químicos restritos – além de instruções a respeito da fabricação de explosivos, acrescentando ainda que, a exemplo de outros sites da *dark web*, os links para esses sites frequentemente mudam a fim de evitar que sejam descobertos. De acordo com Falconer (2012), ao se navegar por fóruns mais profundos, referências à experimentação humana também passarão a ser encontradas com frequência.

Segundo esse autor, muitos dos sites referenciados nesses tópicos já não existem mais, não havendo razões concretas para se acreditar que tais sites realmente existam. Ele complementa, ainda, afirmando que, mesmo que esses sites folclóricos fossem reais, seria difícil para seus donos prová-los. O Human Experiment afirma ter quatro armazéns operacionais, cada um com capacidade para até 20 objetos de teste. A primeira página do referido site afirma que tais experimentos incluem fome e restrição de fluidos, vivissecção, doenças infecciosas, testes de drogas, esterilização e tolerâncias neonatais e infantis a várias coisas, estando, entretanto, inativo desde 2011 (FALCONER, 2012).

Chertoff e Simon (2015) afirmam ainda ser possível encontrar na *dark web* páginas voltadas a “roubos sob encomenda”, hospedadas por pessoas que se julgam hábeis na prática desse tipo de conduta e que se dispõem a roubar qualquer coisa pela qual o interessado não possa, ou não esteja disposto, a pagar. Eles fazem referência ainda ao Euroarms, um site que vende todo tipo de arma que possa ser entregue à porta do cliente, em qualquer lugar da Europa.

Muitos sites populares de apostas em bitcoin bloqueiam endereços IP dos EUA, pois temem processos judiciais dos Estados Unidos. Com a ajuda da *dark web*, os usuários desses sites podem continuar seus jogos de azar disfarçando seu endereço IP dos EUA (O’NEILL, 2013). Ainda de acordo com este último, “*To gamble with bitcoins is to double down: It’s a wager on top of a risk*” (algo como: jogar com bitcoins é dobrar: é uma aposta em cima de um risco), afinal, a aquisição de criptomoedas é, em si, uma aposta no futuro de uma nova ideia que ainda precisa enfrentar uma ampla gama de testes legais, regulatórios e especulatórios em todo o mundo.

Chertoff e Simon (2015) afirmam, ainda, ser a pedofilia – ou pornografia infantil – muito acessível na *dark web*. Embora seja relativamente comum observar-se o emprego desses termos como sinônimos, vale salientar que não são. De acordo com o site safenet.org, a pedofilia consta na Classificação Internacional de Doenças e Problemas Relacionados à Saúde (CID) e diz respeito aos transtornos de personalidade causados pela preferência sexual por crianças e adolescentes.

O pedófilo não necessariamente pratica o ato de abusar sexualmente de meninos ou meninas. Já a pornografia infantil é descrita pela Interpol como a consequência da exploração ou abuso sexual perpetrado contra uma criança. Pode ser definida como qualquer meio de representar ou promover o abuso sexual contra uma criança, incluindo impressão e/ou áudio, centrado em atos sexuais ou nos órgãos genitais de crianças. O Código Penal (brasileiro) e o Estatuto da Criança e do Adolescente (ECA) não preveem redução de pena ou da gravidade do delito, se for comprovado que o abusador é pedófilo.

3.4 Um pouco sobre monitoramento da *dark web*

A *dark web,* de maneira geral, e especialmente a rede Tor, oferece uma plataforma segura para prática das mais diversificadas atividades delituosas – de mercados anônimos a meios seguros de comunicação que proporcionem uma infraestrutura não rastreável e difícil de combater para a implementação de *malwares* e *botnets* (CHERTOFF & SIMON, 2015).

Assim sendo, o monitoramento e o rastreamento das atividades da *dark web* vêm se tornando cada vez mais relevantes para as agências de segurança, com especial atenção à rede Tor, possivelmente se estendendo também a outras tecnologias emergentes – I2P, por exemplo. Entretanto, dado seu intrincado projeto e encadeamento, grandes desafios emergem, sendo os esforços para endereçá-los especialmente concentrados em (CIANCAGLINI, BALDUZZI & GONCHAROV, 2013):

- **Mapeamento de serviços de diretório ocultos:** tanto o Tor quanto o I2P usam um *domain database* construído sobre um sistema distribuído conhecido como *Distributed Hash Table* (DHT). Um DHT funciona tendo nós no sistema colaborativamente responsáveis pelo armazenamento e manutenção de um subconjunto do banco de dados, na forma de *key-value store*. Graças a essa natureza distribuída de resolução de domínio de serviços ocultos, é possível implantar nós no DHT para monitorar solicitações provenientes de um determinado domínio (https://donncha.is/2013/05/trawling-tor-hidden-services/#comments). Ao fazer isso, é possível ter uma visão parcial do banco de dados de domínios e inspecionar solicitações em andamento. Mesmo que isso não permita rastrear quem está tentando acessar um determinado serviço, ele oferece uma boa estimativa estatística dos novos domínios que estão ganhando popularidade. Além disso, a execução de mais desses nós fornecerá uma visão estatística melhor das solicitações gerais na rede.
- **Monitoramento dos dados dos clientes:** agências de segurança podem se beneficiar da análise dos dados de navegação web do cliente em busca de conexões com domínios não padrão. Dependendo do nível de uso da web no lado do cliente, isso pode não ajudar no rastreamento

de links para a *dark web*, mas ainda pode fornecer *insights* sobre atividades hospedadas em domínios maliciosos de alto nível, sem invadir a privacidade do usuário, uma vez que somente os destinos das requisições precisam ser monitorados e não quem está se conectando a eles.

- **Monitoramento de site social:** sites como o Pastebin são frequentemente usados para a troca de informações e de endereços referentes a novos serviços ocultos (*hidden services*) e, assim, devem ser mantidos sob ostensiva vigilância.
- **Monitoramento de serviços ocultos:** serviços ocultos tendem a ser muito voláteis, desaparecendo e, posteriormente, reaparecendo, com novo nome de domínio. Dessa forma, é essencial tirar-se *snapshots* de cada novo site assim que ele venha a ser detectado, seja para posterior análise ou para monitoramento de suas atividades on-line. Embora o rastreamento na *surface web* seja uma prática, geralmente, envolvendo a recuperação de recursos relacionados a um site, isso não é recomendado na *dark web*, pois, por exemplo, há possibilidade de baixar automaticamente conteúdos como pornografia infantil, cuja simples posse é considerada ilegal na maioria dos países.
- **Análise semântica:** depois que os dados de um serviço oculto (qualquer site da *dark web*) forem recuperados, a construção de um banco de dados semântico que contenha informações relevantes sobre esse site pode ajudar a rastrear futuras atividades ilegais nele e associá-las a agentes maliciosos.
- ***Marketplace profiling*:** finamente, seria útil concentrar-se na construção dos perfis das transações efetuadas nos *marketplaces* (simplificadamente, pontos de comércio) na *dark web*, a fim de coletar informações a respeito dos vendedores, usuários e tipos de mercadorias trocados. Perfis individuais podem ser construídos ao longo do tempo.

Enfim, a *deep web*, mas especificamente as redes na *dark web* – a exemplo da Tor –, pode acabar se tornando uma forma viável, também, para que agentes maliciosos venham a praticar condutas delituosas de forma anônima.

REFERÊNCIAS

BERGMAN, M. K. White Paper: The Deep Web: surfacing hidden value. **The Journal of Electronic Publishing**. 2001. Disponível em: <http://dx.doi.org/10.3998/3336451.0007.104>. Acesso em: 14 jun. 2020.

BÜCHI, M.; JUST, N.: LATZER, M. Caring is not enough: the importance of Internet skills for online privacy protection. **Information, Communication & Society.** Advance online publication. 2016. Disponível em: <http://dx.doi.org/10.1080/1369118X.2016.1229001>. Acesso em: 14 jun. 2020.

CHERTOFF, M.; SIMON, T. **The impact of the dark web on Internet Governance and Cyber Security.** Global Comission on Internet Governance. 2015. Disponível em: < https://www.cigionline.org/sites/default/files/gcig_paper_no6.pdf>. Acesso em: 14 jun. 2020.

CIANCAGLINI, V.; BALDUZZI, M.; GONCHAROV, M. **Deepweb and cybercrime**: it's not all about Tor. Trend Micro Research Paper. 2013. Disponível em: <https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-deepweb-and-cybercrime.pdf>. Acesso em: 14 jun. 2020.

FALCONER, J. **A Journey into the Dark Corners of the Deep Web.** The Next Web. 2012. Disponível em: <https://thenextweb.com/insider/2012/10/08/mail-order-drugs-hitmen-child-porn-a-journey-into-the-dark-corners-of-the-deep-web/>. Acesso em: 14 jun. 2020.

FOROUZAN, B. A. **Comunicação de dados e redes de computadores.** 4ª ed. São Paulo: McGraw-Hill, 2008.

FREE NET PROJECT. **About**. Disponível em: <https://freenetproject.org/>. Acesso em: 14 jun. 2020.

GRABOSKY, P. Virtual criminality: old wine in new bottles? **Social & Legal Studies**, v. 10, n. 2, p. 243-49, 2001. Disponível em: <http://sls.sagepub.com/content/10/2/243.full.pdf>. Acesso em: 14 jun. 2020.

HARDESTY, L. Shoring up Tor. **MIT News,** 28 jul. 2015. Disponível em: <http://news.mit.edu/2015/tor-vulnerability-0729>. Acesso em: 14 jun. 2020.

HARGITTAI, E. The digital reproduction of inequality. In: GRUDSKY, D. (ed.). **Social Stratification.** Boulder: Westview Press, 2008. p. 936-944.

HOFFMAN, D. L.; NOVAK, T. P.; VENKATESH, A. Has the Internet become indispensable? **Communications of the ACM**, v. 47, n. 7, p. 37-43, 2004. Disponível em: <https://www.researchgate.net/publication/200111136_Has_the_Internet_Become_Indispensable>. Acesso em: 14 jun. 2020.

I2P. **O projeto da Internet invisível.** Disponível em: <https://geti2p.net/pt/>. Acesso em: 14 jun. 2020.

O'NEILL, P. H. Inside the Bustling, Dicey World of Bitcoin Gambling. **The Daily Dot,** 17 dec. 2013. Disponível em: <https://www.dailydot.com/business/bitcoin-gambling-just-dice-video-casino/>. Acesso em: 14 jun. 2020.

PAGANINI, P. The good and the bad of the Deep Web. **The Harcker New Magazine,** 17 set. 2012. Disponível em: <https://securityaffairs.co/wordpress/8719/deep-web/the-good-and-the-bad-of-the-deep-web.html>. Acesso em: 14 jun. 2020.

PEDERSON, S. **Understanding the Deep Web in 10 minutes.** 2013. Disponível em: <https://bigdata.brightplanet.com/hs-fs/hub/179268/file-22990148pdf/docs/deep_web_whitepaper_v3_for_approval.pdf>. Acesso em: 14 jun. 2020.

PEW RESEARCH CENTER. **Digital Life in 2015**. 2014. Disponível em: <http://www.pewinternet.org/2014/02/25/the-web-at-25-in-the-u-s>. Acesso em: 14 jun. 2020.

POMPÉO, W. A. H.; SEEFELDT, J. P. Nem tudo está no Google: Deep Web e o perigo da invisibilidade. 2º CONGRESSO INTERNACIONAL DE DIREITO E CONTEMPORANEIDADE. Universidade Federal de Santa Maria, 2013.

PORTAL EDUCAÇÃO. **World Wide Web – WWW**: O que é?. Disponível em: <https://www.portaleducacao.com.br/conteudo/artigos/direito/world-wide-web-www-o-que-e/37918>. Acesso em: 14 jun. 2020.

PORUP, J. M. Zero Day: tudo o que você precisa saber sobre este tipo de falha. **Computerworld,** 27 jun. 2018. Disponível em: <https://computerworld.com.br/2018/06/27/zero-day-tudo-o-que-voce-precisa-saber-sobre-esse-tipo-de-falha/>. Acesso em: 14 jun. 2020.

SMART COSMOS. The deep web, the dark web and simple things. **Medium,** 1º ago. 2017. Disponível em: <https://medium.com/@smartrac/the-deep-web-the-dark-web-and-simple-things-2e601ec980ac>. Acesso em: 14 jun. 2020.

TEMPLETON, Graham. Silk Road: how to be a Deep Web criminal and get away with it. **ExtremeTech,** 9 oct. 2013. Disponível em: <https://www.extremetech.com/extreme/168277-silk-road-how-to-be-a-deep-web-criminal-and-get-away-with-it>. Acesso em: 21 set. 2018.TOR PROJECT. **Onion Services**. Disponível em: <https://www.torproject.org/docs/onion-services.html.en>. Acesso em: 14 jun. 2020.

VIGNOLI, R. G.; MONTEIRO, S. D. **A topologia da dark web e seus não lugares.** In: XIV Encontro Nacional de Pesquisa em Ciência da Informação, 2013. Disponível em: <http://enancib.sites.ufsc.br/index.php/enancib2013/XIVenancib/paper/viewFile/204/312>. Acesso em: 14 jun. 2020.

VPNOVERVIEW. **The Tor browser – What is it and why would you use it?** Disponível em: <https://vpnoverview.com/privacy/anonymous-browsing/tor/>. Acesso em: 14 jun. 2020.

WHITWAM, R. MIT researchers figure out how to break Tor anonymity without cracking encryption. **ExtremeTech,** 29 jul. 2015. Disponível em: <https://www.extremetech.com/extreme/211169-mit-researchers-figure-out-how-to-break-tor-anonymity-without-cracking-encryption>. Acesso em: 14 jun. 2020.

WILLIAMS, C. The Hidden Wiki: An Internet Underworld of Child Abuse. **The Daily Telegraph**, 2011.

GLOSSÁRIO

Animáculos	Animal muito pequeno, visível somente ao microscópio.
Domain database	Em gerenciamento de dados e análise de bases de dados, um *data domain* se refere a todos os valores que um elemento de dados pode conter. A determinação do limite de um domínio pode ser tão simples quanto um tipo de dados com uma lista enumerada de valores.
Fingerprint	Técnica de levantamento de informações, geralmente, para identificação do sistema operacional da máquina-alvo.
Hipermídia	Sistema de registro e exibição de informações informatizadas por meio de computador, que permite acesso a determinados documentos (com textos, imagens estáticas ou em movimento, sons, softwares etc.) a partir de *links* que acionam outros documentos e assim sucessivamente.
Hyperlink	Referência dentro de um documento em hipertexto a outras partes desse documento ou a outro documento.
Key-value store	É um paradigma de armazenamento de dados projetado para armazenar, recuperar e gerenciar matrizes associativas.
Message board	Uma área de discussão on-line na qual usuários com interesses similares discutem tópicos. Essas conversas ou discussões são disponibilizadas na forma de postagens.
Virtual Private Network (VPN)	VPNs estendem as redes privadas através de uma rede pública, permitindo que usuários enviem e recebam dados por meio de redes públicas ou compartilhadas, como se seus dispositivos de computação estivessem diretamente conectados à rede privada.
Web crawlers	Também conhecidos como rastreadores, robôs ou spiders, são programas ou scripts automatizados que navegam a www de forma metódica e automatizada, sendo utilizados, principalmente, para criar cópias de todas as páginas visitadas para posterior processamento por mecanismos de busca, os quais indexarão essas páginas a fim de agilizar as buscas.