MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO TRIÂNGULO MINEIRO – CÂMPUS PARACATU

O universo da Deep Web

Professor: **Roitier Campos Gonçalves.**

Aluno: **Abner Matheus Gomes Silva.**

Paracatu - MG
2016

1. INTRODUÇÃO

A Deep Web que também conhecida por Deepnet, Web Invisível, Undernet ou Web oculta, são conteúdos da web que não são encontrados por mecanismos de busca padrão como os navegadores convencionais ou sites de pesquisa como Google , Bing e Yahoo, ou seja, são sites e conteúdos que não fazem parte da Surface Web(web convencional na qual acessamos todos os dias ex: Facebook ,Twitter ,YouTube).

Em um estudo realizado por alunos da Universidade da Califórnia em 2001 , foi especulado que a deep web possuía mais de 7500 terabytes de informação. Estimativas feitas por He et al. em 2004, detectaram cerca de 300.000 sites da deep web e, de acordo com Shestakov, cerca de 14.000 destes eram da parte russa da Web em 2006. Em 2008, a web chamada "Deep Web", não referenciada pelos motores de busca representa 70 a 75% do total, ou seja, cerca de um trilhão de páginas não indexadas. Os endereços são muitas vezes códigos alfanuméricos com sufixo .onion em vez de .com. Em algumas redes, como a I2P, é necessário fazer configurações de rede e proxy para que se tenha acesso a determinados sites da rede. A Deep Web não é organizada através de camadas, e sim, através de redes de computadores totalmente independentes entre si. São elas: Onion (TOR), I2P, Freenet, Loky, Clos, Osiris e muitas outras.

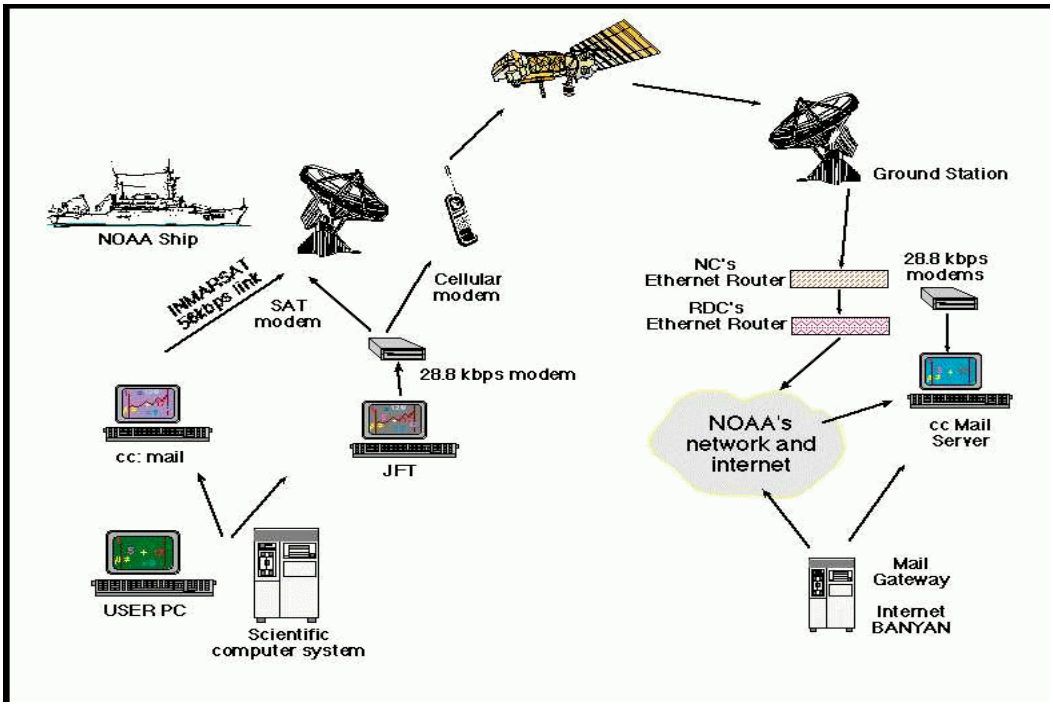
Acessar a deep web nunca foi uma tarefa difícil, porem muitas pessoas tem medo, pois os rumores que se espalham na internet, deixam a impressão de que a deep web é um local ruim, principalmente para sites da rede TOR. Algumas redes exigem grande conhecimento em criptografia e redes ou simplesmente um usuário e senha. Não existem leis que proíbam as pessoas de navegarem na Deep Web, principalmente na constituição brasileira. O que é contra a lei são as ações tomadas, e as atitudes que os usuários cometem dentro da rede, com o conteúdo que está disponível e, obviamente, qualquer negociação no mercado negro, como por exemplo, acessar sites de pedofilia, contrabando, pirataria, trafico de órgãos e pessoas, entre outros. Em agosto de 2013, o FBI derrubou um dos maiores servidores da rede Tor da Deep Web, o famoso Freedom Hosting. Milhares de usuários foram expostos às autoridades e o cerco para os criminosos que mantinham negócios ilegais começou a fechar. Com essa queda o maior site de mercado negro da Deep Web também caiu, o Silkroad. Em março de 2015, foi a vez do Evolution, também mercado negro, que foi devastado pelo FBI. Em total desespero, seus administradores desligaram os servidores e sumiram do mapa, junto com uma quantia de aproximadamente 12 milhões de dólares em Bitcoins. A melhor parte da Deep Web são os fóruns e bibliotecas. Existem inúmeros meios de obter conhecimento sobre qualquer assunto e em qualquer idioma - desde anatomia humana e animal até estudos sobre ufologia, de como fazer uma bomba a invadir um computador. Tem de tudo. Quando se navega em algum site da Deep Web, é possível que ele tenha vários links que redirecionem para outros sites, porém sempre com o mesmo assunto. Ao navegar em um fórum de tecnologia, clicando nos links disponíveis neste site, dificilmente você será redirecionado para um site de mercado negro, pedofilia ou fóruns de canibalismo. Resumidamente o que você procurar, vai achar nada aparece na sua tela por acaso, mesmo sendo nesse submundo.

O maior perigo de navegar na Deep Web são os vírus de computador e a quebra do anonimato, pois, uma vez que descobrem quem você é, em uma terra sem lei, você vira um alvo fácil para crackers e pessoas má intencionadas que podem desde invadir sua máquina até extorquir você de alguma forma, como já aconteceu com inúmeras pessoas desavisadas. Recomendamos que você não faça downloads em sites que não são confiáveis , não entrar na rede em computadores desprotegidos , sem um bom antivírus e um firewall potente ,

também e recomendando que use uma maquina com o sistema operacional Linux , pois é um sistema que geralmente os crackers não tem muito foco , pois é pouco usando.

2. O que é a deep web?

No ano de 1991, Tim Berners-Lee criou a web (World Wide Web) que é um meio de comunicação global no qual usuários podem ler e escrever através de computadores conectados à Internet. Sendo um projeto desenvolvido dentro do CERN (European Organization for Nuclear Research), com objetivo de ser uma ferramenta de compartilhamento de dados, de modo que todos os pesquisadores e cientistas pudessem compartilhar resultados e pesquisas com os demais para agilizar o processo científico. Por ser uma ferramenta fácil de ser ulitizada e não precisar de conhecimento técnico para ser usada, a web se popularizou rapidamente e atingiu, no ano de 2014, a marca de 968.882.453 websites abertos.

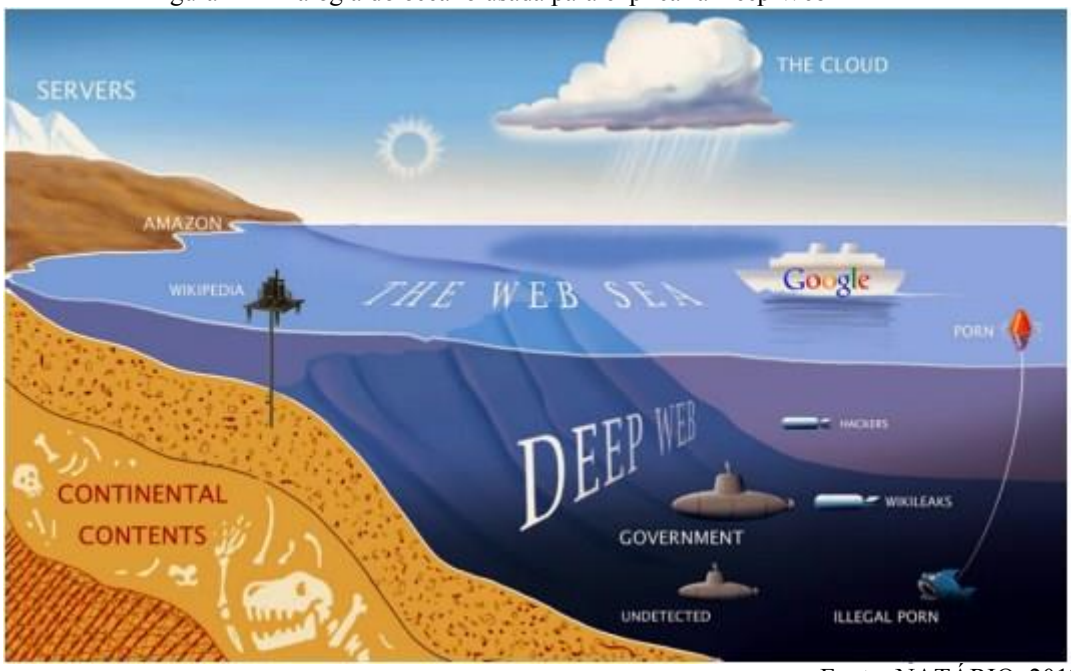


Fonte:https://pt.wikipedia.org/wiki/Hist%C3%B3ria_da_World_Wide_Web

Com este volume gigantesco de paginas web, destacam-se as redes sociais como facebook , twitter , youtube, sites pessoais ou blogs, portais de conteúdo,os wikis, as ferramentas de busca, os chats e os sites de compartilhamento de mídia. A popularização da internet impulsionou a criação de varias ferramentas de pesquisa, como os buscadores. Todavia, ser visível nem sempre é uma alternativa válida para todas as pessoas. Varias pessoas preferem o anonimato. Em 1994, poucos anos depois da criação da web, o termo "web invisível" foi criado pelo Dr. Jill Ellsworth (BERGMAN, 2001), quando se referia a conteúdos presentes na web daquela época e que eram invisíveis aos mecanismos de busca existentes. Nascendo assim o conceito de Deep Web. Porem observe que, naquela época, os buscadores da web existentes eram baseados em serviços de diretório e para que o site pudesse aparecer nos resultados de busca, era necessário que o dono ou mantenedor da página executasse um cadastro, fornecendo dados como título do site, endereço, categoria da página e palavras-chave relacionadas. Por isso, não podemos afirmar sites que não apareciam nos buscadores queriam fazer parte da Deep Web. Poder ser que eles entrassem nela sem querer.

O interesse de navegar de forma anonima fez com que essa a deep web crescesse muito. Em julho de 2000, a Deep Web já possuía um volume de dados 500 vezes maior que a web convencional (HE et al., 2007). Para melhor explicar a Deep Web, alguns autores fazem a seguinte analogia: se a web fosse um grande oceano de informações, a Deep Web seria a parte mais profunda, onde as ferramentas de busca não conseguiriam lançar suas redes.

Figura 1 – Analogia do oceano usada para explicar a Deep Web



Fonte: NATÁRIO, 2012

É necessário separar duas etapas na Deep Web: o processo de criar sites invisíveis e o processo de navegação invisível. Para fazer com que um site dique invisível, 7 cuidados devem ser tomados. O primeiro é o não uso de servidores DNS na pagina. Servidor DNS é o responsável por traduzir nomes de domínio em endereços IP. Ou seja, é ele que nos ajuda a recordar que para que possamos acessar, por exemplo, o site do Facebook tem que digitar no navegador www.facebook.com, não sendo necessário sempre saber de cabeça o endereço IP do servidor do facebook, que no caso do facebook é 31.13.80.36. Sem o uso de um servidor de DNS, o site torna-se acessível somente para o usuário que sabe do endereço do IP do site e, consequentemente, inacessível para quem não o possui. Da mesma maneira, os buscadores como Google, Bing e Yahoo, são baseados em programas chamados crawlers, que não conseguem, de maneira tão simples, localizar a página. A segunda medida usada para que o site permaneça invisível é que o mesmo seja dinâmico. Isto é, ele somente apresentará o conteúdo da página ao usuário caso este efetue uma busca que contenha palavras-chave específicas. Como os buscadores tradicionais varrem a página (sem entrarem com nenhum tipo de informação na mesma), os sites da Deep Web, na visão dos motores de busca, são páginas em branco e, portanto, não são indexadas. O terceiro fator que impede a indexação das páginas desta rede anônima pelos buscadores é a pequena quantidade ou total ausência dos hyperlinks entre as páginas, o que impede os crawlers de indexá-los. Por fim, o quarto fator aplicado aos sites da Deep Web é o uso de sistemas de login, exigindo do usuário um cadastro prévio, que costuma passar por um processo de seleção e aprovação. Esse processo de login também acaba por bloquear os buscadores de executarem o processo de indexação das páginas, tornando os sites da Deep Web ocultos na web convencional.

É importante ressaltar que a Deep Web e a “web convencional” operam ambas dentro do mesmo contexto da internet. Portanto, são essas quatro técnicas apresentadas que garantem a separação de ambas.

3. ANONIMATO

Privacidade é com certeza uma das maiores preocupações quando se navega da internet. A noticia de que o governo dos Estados Unidos está espionando o planeta inteiro de forma indiscriminada, dá ainda mais força para essa afirmação. Edward Snowden é vitima de perseguições por denunciar e mostrar abertamente fatos que comprovam essa ilegalidade, porem, se observarmos com cautela , apenas essa denuncia está sendo apurada, como não ligamos para todas as denuncias que já foram feiras , inclusive de outros países, podemos chegar a conclusão de que não estamos seguros na internet. Saber que o governo chinês espiona o Skype, e a Microsoft não fazem nada a respeito, ou de que pessoas como Edward Snowden e Julian Assange são perseguidos e tratados como terroristas por denunciarem.

A internet foi incorporada na vida de quase todas as pessoas do planeta, com isso varias vantagens, benefícios e facilidades foram adquiridos pela população, como a facilidade de comunicação com pessoas e empresas que estão longe , acesso e compartilhamento de informações , musicas , vídeos , imagens etc. Mas se não tomarmos muitos cuidados , todas essas facilidades podem ser usadas para fazer o mal , causar danos e causar riscos a segurança de quem navega na rede. Nos dias atuais, as pessoas cada vez mais trocam dados por meio eletrônico, principalmente através de redes sociais. Essas tecnologias causam vários tipos de tragédias que podem gerar danos exponenciais. Estamos momento de evolução, onde as relações humanas se tornam cada vez menos interativas através dos celulares , com isso também estamos nos tornando vulneráveis aos ataques a nossa esfera de privacidade. Se analisarmos bem essa evolução , perceberemos que uma das grandes dificuldades é preservar a reputação e a privacidade diante de um ambiente de conexão causado pela evolução tecnológica que faz uma esfera publica nova atacando a credibilidade por pessoas físicas e jurídicas nesta nova era social. A reputação pessoal e das empresas é algo inestimável que com toda certeza deve ser encarado como uma poupança, onde se procura acumular valores diante da percepção do público que ora está sendo potencializada através da internet.

As pessoas na maioria do tempo não se comportam se forma segura na internet, pois o brasileiro de forma geral adora tecnologia, e ama se exibir na rede, o que é prejudicial, pois, o seu pouco conhecimento sobre a vulnerabilidade do excesso de exposição da sua privacidade pelo meio eletrônico, como locais que freqüenta, fotos intimas, fotos de família etc. A falsa sensação de estar seguro propiciada pela tecnologia, e o desconhecimento das leis, atraem os infratores para a prática de ilícitos que vem sendo cada vez mais desvendados e punidos pela Justiça Brasileira.

As pessoas precisam se conscientizar que, a medida que a tecnologia avança , a privacidade esta sendo afetada. Tudo isso e provocado pela tecnologia não deve ser encarada como desprotegida pelo direito , já criaram leis suficientes sobre o tema para coibir os abusos praticados contra as pessoas no meio tecnológico. E muito importante criar o hábito de monitorar a divulgação de textos, imagens, vídeos para que seja possível identificar rapidamente o conteúdo ilícito visando retirá-lo imediatamente de circulação como forma de minimizar o dano. Todos sabemos que estamos passando por uma necessidade de aprendermos uma nova etiqueta de comportamento social através do mundo eletrônico, demandando um aprendizado para que estejamos preparados para críticas e

execrações digitais que nem sempre poderão ser controladas pela vítima, mas que serão punidas pela Justiça.

3.1 A rede tor

A rede tor é um grupo de servidores mantidos por um grupo de usuários operando ao redor do mundo, com o intuito de melhorar a segurança e a privacidade na internet. Os usuários são conectados na rede tor através de uma serie de túneis virtuais, ao invés de fazer uma conexão direta, permitindo assim que ambas as organizações e indivíduos, possam compartilhar informações através de uma rede publica sem comprometer a privacidade. Na mesma linha, Tor é uma ferramenta eficaz contra censura evasão, permitindo que seus usuários possam chegar a sites , vídeos , musicas e qualquer tipo de arquivos de forma diferente ou desbloquear conteúdos bloqueados. O Tor também pode ser usado como um bloco de construção para desenvolvedores de software para criar novas ferramentas de comunicação com built-in e funcionalidades de privacidade.

Tudo que você faz na internet, desde ver um vídeo a ler um livro , tudo isso pode ser utilizado para rastrear seu endereço IP. A função do tor é exatamente ocultar essa informação. Antes que os dados sejam enviados para a rede, o tor cria diversas conexões aleatórias com algumas máquinas, logo se algum vírus ou hacker tentar rastrear o seu endereço de IP, ficará perdido em meio a tantos redirecionamentos.

Os servidores que são responsáveis por redirecionar o trafego são conhecidos como Tor Relays, sendo eles: os *middle relays*, os *end relays* e *bridges*. Os *end relays* são os últimos da cadeia de conexões, enquanto os *middle relays* cuidam do tráfego no caminho. Qualquer computador na rede pode ser um roteador intermediário sem temer problemas com atividades ilícitas que passem por essas conexões. Já os que servem como finais precisam ser cuidadosos já que são eles os alvos da polícia e dos detentores de direitos autorais caso alguma crime seja detectado. *Bridges*(pontes), são relays que não são listados publicamente, provavelmente para proteção contra bloqueadores de IP. Você não precisa rodar um relay para usar o Tor, mas é legal que você rode.

Pessoas que utilizam o Tor estão quase sempre seguras. O software é usado por jornalistas, políticos, órgãos governamentais , universidades e mais para garantir a privacidade e segurança. É realmente difícil rastrear alguém usando o Tor. Ele é usado até por uma área da Marinha dos EUA para operações de segurança (na verdade, ele foi criado como parte de um projeto da Marinha dos EUA cujo propósito era criar formas de proteger as comunicações do governo dos EUA). Até onde sabemos, a NSA presta atenção no Tor. Mas se ele é bom o suficiente para uso militar, então é bom também para você.

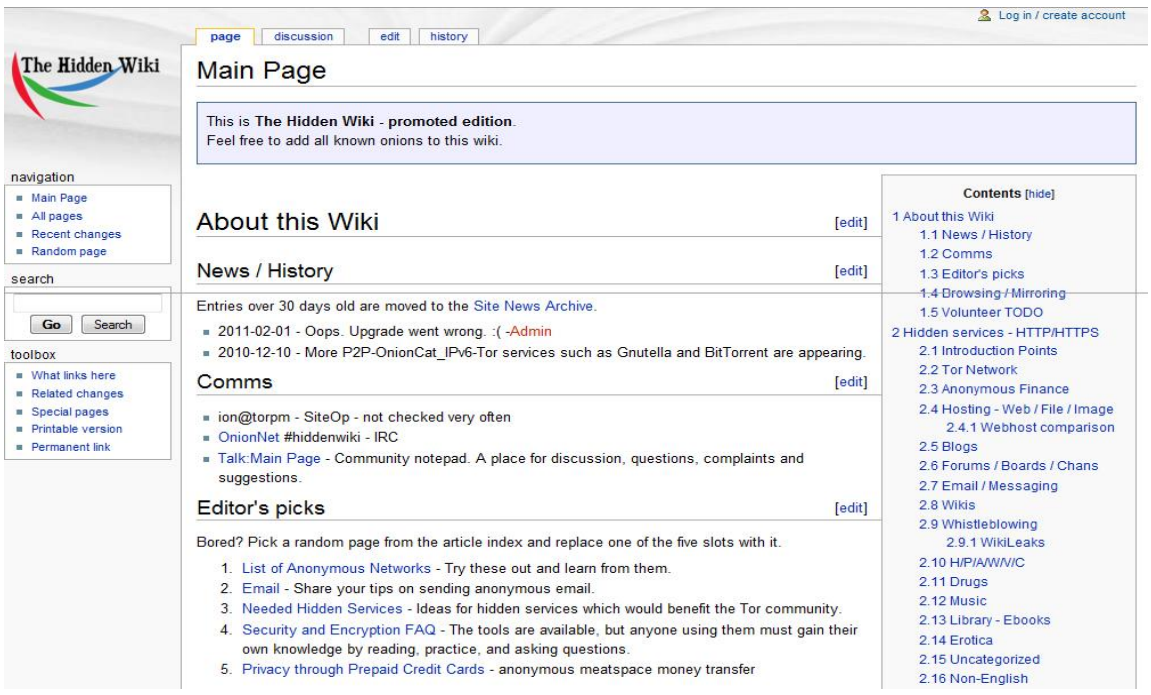
Uma das desvantagens de usar o Tor está na velocidade de navegação. Pois o tráfego da internet está sendo roteado por ao menos três camadas, ele acaba se perdendo no caminho deixando a navegação lenta; Isso é especialmente perceptível em elementos mais

pesados como áudio e vídeo, e dependendo da quantidade de usuários agindo como relays, pode piorar com mais pessoas na rede.

O Tor oferece também a criptografia dos dados trocados entre o seu dispositivo e a internet. Com isso, mesmo que alguém consiga interceptar os pacotes, não conseguirá decifrá-los.

3.2 sites da rede tor

O layout de paginas que estão na Deep Web quase nunca são bem feitos e bonitos na verdade são bastante feios pois pessoas interessadas em navegar por lá não estão preocupadas com o layout mais sim com o conteúdo das paginas. É importante destacar que é preciso conhecer o inglês pois na DeepWeb a grande maioria dos sites e links estão com conteúdos em inglês, sendo assim se a pessoa não tiver um bom conhecimento da lingua vai ter muita dificuldade para navegar e achar o que procura [PEREIRA 2012]. Um fato importante a se falar são as URLs dos sites na Deep Web, diferente das URL dos sites normais que são padronizadas como "www.facebook.com.br", por exemplo, e com demais extensões como .net, .gov e demais, na DeepWweb a URL contém um código criptografado sendo que as de alguns sites mudam constantemente para não serem encontrados e finalizam com .onion por causa que estão na rede TOR como mostra a URL para acessar um site de pesqusas na DeepWeb chamado TORCH xmh57jrzrnw6insl.onion igual ao buscador google o mais famoso e conhecido . Outro exemplo disso é o site Hidden Wiki uma das principais páginas da DeepWeb com a aparência semelhante do site conhecido Wikipédia a enciclopédia livre. Assim como o Wikipédia o Hidden Wikki tem um menu inicial que é o ponto de partida para aqueles que iniciam a navegar na Deep Web. A imagem a seguir mostra a página inicial do Hidden Wiki e os tópicos disponíveis para iniciar a navegação na Deep Web. É possível observar a URL da página cheia de códigos e números kpvz7ki2v5agwt35.onion/wiki/index.php/Main_Page. Também é possível observar o layout do site de uma biblioteca de livros contendo 55Gb de livros disponíveis divididos por categorias acessado na DeepWeb através do próprio Hidden Wiki.



Fonte: Google imagens.

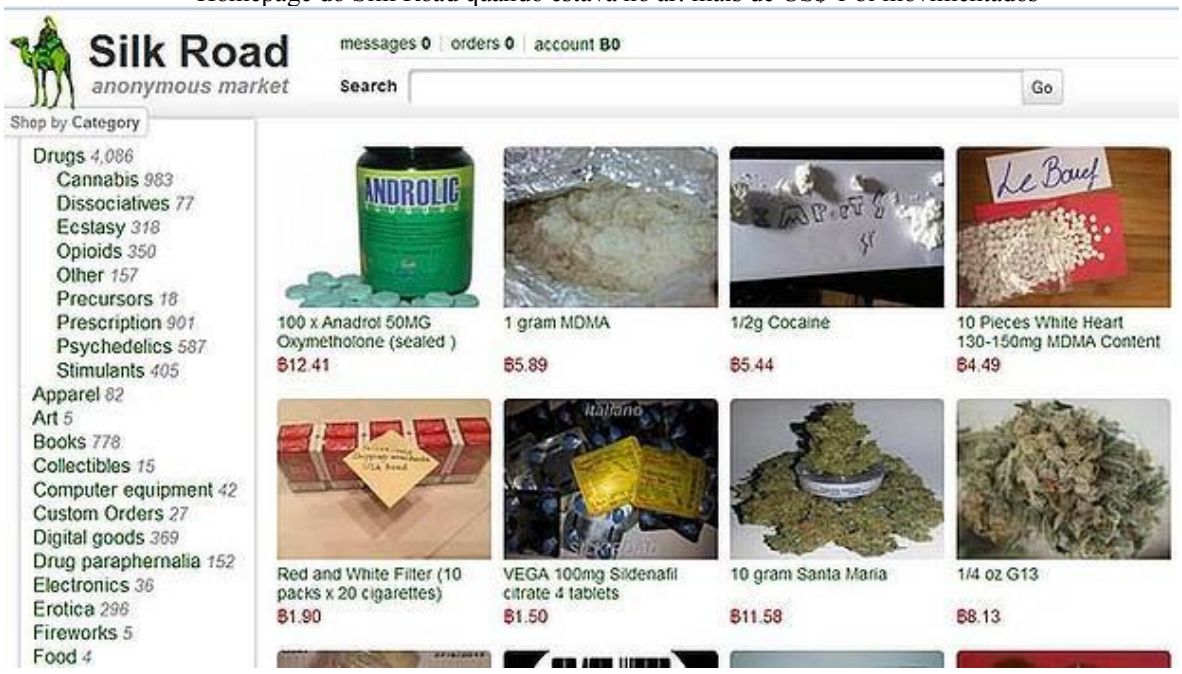
3.3 O lado Obscuro da rede tor

Os primeiros sites da DeepWeb Surgiram nos EUA , é hoje é o lugar perfeito para atividades ilegais , crimes e pirataria como pornografia e venda de drogas. Geralmente, transações "obscuras" tendem a acontecer nessa rede, envolvendo venda online de drogas, pornografia infantil, informações sobre cartões de crédito e armas, por exemplo. Originalmente desenvolvida pelo governo dos EUA, a darknet também serve hoje de plataforma para lavagem de dinheiro e compra e venda de outros bens e atividades ilegais com relativa impunidade.Órgãos do FBI e da CIA tentam invadir e descobrir quem está por trás do misterioso mercado negro online.

Um caso que marcou a deep web foi um grupo de hackers chamados de "Impact Team", eles publicaram dados de 37 milhoes de integrandes dos sites de enconstros Ashley Madison e Established Men.

Em novembro de 2014 o FBI, o Departamento de Segurança Interna dos Estados Unidos e a Europol conduziram a operação Onymous, foram retirados do ar 27 sites ocultos da Deep Web, um deles era o Silk Road 2.0, que teve o seu operador foi preso.

Homepage do Silk Road quando estava no ar: mais de US$ 1 bi movimentados



Fonte:Google imagens

A maneira que está investigação foi conduzida, é desconhecida. Em entrevista da revista Wired, o chefe da Europol, Troels Oerting, disse que os agentes preferiam manter a metodologia em segredo. "Não podemos compartilhar com todo mundo a forma como fizemos isso, porque queremos fazê-lo de novo, de novo e de novo."

Desde então, a deep web tem estado relativamente tranquila, mas não foi desativada. Não é aconselhável visitar sites da deep web, pois, além da ilegalidade de muitos produtos oferecidos, não é possível verificar que informações do usuário serão recolhidas ou roubadas durante a visita.

3.4 O lado bom da rede tor

Existe, entretanto, o lado bom da deep web: a liberdade de expressão. Como a rede é oculta e permite que os usuários que navegam se comuniquem de forma anônima, exigindo que os governos tenham que adotar esforços extremos para tentar localizá-los e identificá-los.

Para usuários que vivem em regimes ditatoriais, que monitoram ativamente, bloqueiam conteúdo na internet ou adotam ações punitivas contra dissidentes, a deep web oferece maneiras alternativas de se expressar livremente.

Vale o mesmo para whistleblowers. A darknet é um lugar seguro para publicar informações de crucial importância para a opinião pública, mas que pode colocar a pessoa responsável pelo seu vazamento em perigo.

A darknet tem, portanto, seu lado mau e, ocasionalmente, um lado bom. Se ao invés de publicarem nomes de usuários, os hackers do caso Ashley Madison tivessem feito vazamentos de emails provando corrupção em governos, a opinião do público sobre os sites anônimos poderia ser agora bem diferente.

4. CONCLUSÃO

Embora a Deep Web seja uma parte temida da rede mundial de computadores a internet, toda a sua criação se deu devido ao desejo de manter o anonimato. Criminosos se aproveitam desse benefício para praticar seus crimes com mais frequência no lado oculto da internet, mas isso não quer dizer que crimes não sejam praticados na Web convencional, só que com menos agressividade, pois na Deep Web você pode encontrar todos os tipos de coisas desumanas e inimagináveis, mais para quem usa a Deep Web para o bem é aproveitada de forma muito benéfica. Na Deep Web quem escolhe o que buscar depende de cada um, se a pessoa buscar conteúdo criminoso ela vai encontrar, se buscar um livro um cd ou até mesmo filmes, jogos e demais também vai encontrar, por isso é importante focar bem o que se busca por lá, pois um link errado que se acesse pode te levar para um caminho totalmente diferente do que se busca. O desenvolveu esse lado da internet com o intuito de beneficiar o anonimato e a quem necessita desse benefício como militares, jornalistas, policias entre outros, mas a criminalidade existe de todo lado inclusive na web, por isso é importante não falar com ninguém e ter certo conhecimento para navegar nesse mundo oculto e perigoso.

5. Referências

Tor Project: Anonymity Online. Disponível em: <http://www. https://www.torproject.org/ >. Acesso em 9 de novembro de 2016.

Deep Web Brasil. Disponível em: <http://www.deepwebbrasil.com/ >. Acesso em 9 de novembro de 2016.

Fatos Desconhecidos. Disponível em: <http://www.fatosdesconhecidos.com.br/como-entrar-na-deep-web-e-o-que-vou-encontrar-la/ >. Acesso em 9 de novembro de 2016.

Wilkipedia – Deep Web. Disponível em: <https://pt.wikipedia.org/wiki/Deep_web >. Acesso em 9 de novembro de 2016.

Deep web: saiba o que acontece na parte obscura da internet. Disponível em: < http://olhardigital.uol.com.br/fique_seguro/noticia/deep-web-saiba-o-que-acontece-na-parte-obscura-da-internet/31120 >. Acesso em 9 de novembro de 2016.

Tecnoblog **-** Como entrar na deep web utilizando o Tor**.**
Disponível em: < https://tecnoblog.net/189897/como-acessar-deep-web-links/ >. Acesso em 9 de novembro de 2016.

Wikipedia - Tor (rede de anonimato). Disponível em: <https://pt.wikipedia.org/wiki/Tor_(rede_de_anonimato) >. Acesso em 9 de novembro de 2016.

Canaltech - Como usar o Tor Project e se manter anônimo na web? Disponível em: < https://canaltech.com.br/dica/seguranca/como-usar-o-tor-project-e-se-manter-anonimo-na-web/ >. Acesso em 9 de novembro de 2016.