Deep Web a web oculta de olhos inexperientes

Salve jovem padawan, o tiozão hoje inspirado vem apresentar um tema, que mexe com a imaginação e atualmente rendeu muito bla bla bla, uns contra outros a favor e a poleminca não para.

Em algum momento deve ter ouvido sobre privacidade, navegação oculta e o sub-mundo da internet, terra sem lei onde podemos encontrar de tudo mais um pouco, muito utilizados para negócios escusos e venda de dados sigilosos.

Mas afinal o que é a Deep Web

A internet profunda, de uma maneira bem simplista podemos dizer que é o quartinho de bagunça da internet, local não indexado pelos motores de busca, sem endereçamento fixo, dinâmica, que aparece e desaparece deixando o mínimo de rastros.

Os motores de busca pensados na performance, confiabilidade e coerência dos dados, deixa de indexar servidores não confiáveis, muitos administradores de servidores para evitar olhares de xeretas não convidados criam mecanismos que bloqueiam o acesso dos spider dos indexadores.

Com isso, milhões de web-pages, diretórios de arquivos e dados não existem nos motores de busca, dificultando a consulta e em casos extremos os endereços IPs são restritos a poucos grupos e com isso a informação é quase invisível.

A ideia surgiu na época da guerra fria.

Onde ambos os lados desejavam manter algumas informações ocultas, nos primórdios da internet, o temor de serem espionados e dados sensíveis passarem para o outro lado, evoluindo na década de 90, quando a internet se popularizou e quase todos queriam ter sua web-page.

Infelizmente alguns grupos começaram a espionar através de sniffers e tentar ganhar alguma vantagem com isso, durante duas décadas a venda de dados foi um negócio amplamente lucrativo, usando canais do MIRC e outros fóruns obscuros.

Nessa época os motores de busca exibiam esses dados abertamente a depender da consulta especifica, porem os governos e suas policias começaram a espionar e prender cidadãos através de dados capturados nestas comunidades.

Foi uma época sem lei, onde tudo podia e muitas barbaridades aconteceram, inclusive com alguns governos censurando alguns servidores e mesmo derrubando sites de opositores, uma loucura que gerou reações em todos os países.

O Echelon foi um deles, um projeto de espionagem mundial, que ficava lendo pacotes de dados que trafegavam na internet e acabavam enfileirados em servidores de ligação, os famosos backbones.

O que é Echelon?

Popularmente conhecido como os Cincos Olhos é o maior sistema de espionagem mundial, um software, que le e analisa dados que trafegam na WEB, mantido por um consorcio de 5 países ( EUA, UK, Canada, Austrália e Nova Zelandia), entrou em operação no século passado e após o desastre do 11 de setembro, tem sido atualizado e expandido , sempre vigilante e atento ao que as pessoas conversam no mundo virtual.

O que é um Softwares farejador?

Sniffer ou softwares farejadores são aplicativos que monitoram segmentos de rede, monitorando o trafego de redes, usado tantos por órgãos de segurança estatais como por cyber-criminosos em busca de dados sensíveis e possíveis ganhos ilícitos por furto ou chantagem.

A Deep Web como grande repositório

Uma terra sem lei, onde pode-se encontrar desde softwares a dados pessoais indexáveis, porem um lugar de liberdade para cyber-ativista e anarquistas digitais fugindo de estado opressores e censura.

Com isso surgiu a necessidade de um navegador WEB, que pudesse escapar as barreiras da WEB comum, preparado para navegar na Deep Web, mantendo o anonimato e a segurança do usuário.

Navegador TOR : The Onion Router

Um navegador web que protege a identidade do usuário, funcionando como uma cebola, com inúmeras camadas de acesso, saltando de máquina em máquina, tornando a navegação irrastreavel, codificado em C e com a primeira versão lançada em 2002.

Ocultando o seu IP, não permitindo gravação de cookies e bloqueando o acesso a dados sensível, que possam de alguma maneira identificar sua máquina ou localização geográfica.

O perigo dos cookies

Notou que muitas vezes recebe propagandas em suas redes sociais relativas a pesquisas feitas no navegador? Infelizmente nossa privacidade é ameaçada com gravações de áudio de maneira oculta, acesso a dados do navegador tais como histórico de navegação, texto digitados e comportamento em redes sociais.

Infelizmente grupos econômicos usando métodos ilícitos, manipulam as massas através destes dados inocentemente gravados em cookies. Olhos maliciosos acompanham nossos passos e geram receitas fabulosas em publicidade e envio de conteúdo.

Conversas nem sempre inocentes

Muitas vezes softwares de IA interagem conosco em Redes Sociais, aproveitando da nossa inocência para instalar trojans em nossos equipamentos e com isso manipular nosso perfil e acessar a dados de nossos amigos em Redes Sociais.

Cuidado e atenção com aquilo que publica nas redes sociais, nunca se sabe onde essa informação será usada, nos últimos anos vimos diversos exemplos do mau uso das redes, vejam o Brexit, a eleição do Trump, Bolsonaro e Fake News.

Senhas fortes e antivírus

Infelizmente devemos ter uma atitude mais ofensiva, criando senhas mais fortes, tendo cuidados nas redes onde nos conectamos, mantendo os softwares atualizados, proteger nosso computador com firewalls e antivírus.

Evite navegar em sites suspeitos, não divulgue informação sensível na redes sociais e cuidados com a segurança de sua família. Apesar de existir a LGPD, muitos hackers agem de outros países e estão longe da lei brasileira.

Pode parecer papo de tiozão, mas como desenvolvedores devemos pensar nos usuários, temos conhecimentos técnicos superiores a maioria e com isso temos a responsabilidade de proteger nossos clientes.

Criando códigos que respeitem os dados sensíveis das pessoas, codificando com ética e responsabilidade nos testes para evitar bugs e backdoors, que permitam acesso indesejável e oportunistas de cyber-criminosos.

Conclusão,

Veja jovem padawan, que loucura é a deep-web, um submundo cheio de armadilhas para os incautos e perigosamente tentadora para os aspirantes a hackers, mas um local onde tudo pode acontecer e com muito ouro de tolos. Fique atento e seja ético.

Procure proteger-se usando senhas fortes, possuindo antivírus atualizado e firewall, quando codificar fique atento as boas práticas e ferramentas seguras, pois a LGPD em vigor possui sanções altíssimas a empresas com softwares inseguros na manipulação de dados pessoais.

Com isso terminamos nossos primeiros passos na Deep Web e o navegador TOR..