Segredos da DARK WEB para Padawans

Navegando pelo Porto Royale da Internet

Salve jovem padawan, finzinho de domingo e vamos nos iniciarmos mais uma semana, dura e ao mesmo tempo animada, vésperas de Carnaval, pena que a Pandemia do Corona vírus nos prende e amedronta, dificultando a saída segura.

Resolvi conversar sobre Porto Royale inspirado na Aceleração Global Dev #21 GFT, onde num momento muito descontraído foi comentado por segurança nos projetos, a problemática dos ataques hackers e o uso de ransomware, a computação em nuvem e toda a problemática da cyber segurança.

Hoje 20 de Fevereiro está sendo comemorado o dia do Teste de Software e nos desenvolvedores temos o compromisso moral de proteger nossos usuários e os demais stakeholders. Por isso necessitamos produzir material de qualidade, instruir o usuário e proteger o Sistema, por isso conhecimento é poder, como isso desembarcamos em Porto Royale, uma parte integrante da DEEP WEB, mais conhecida como DARK WEB.

O que é Dark Web?

Como foi explicado no artigo sobre a Deep Web, estamos num território sem lei, livre de controle de órgãos governamentais, onde policiais e criminosos, ativistas e curiosos, espiões, hackers, crackers e lammers convivem harmoniosamente.

Mas não pense que é um lugar idílico, kumbaya e cheio de paz e amor, nada disso, aqui é um lugar de gente grande, um posto avançado onde esconde-se aqueles que não querem ser encontrado.

Existe uma grande probabilidade de ser apunhalado e jogado aos tubarões, neste território, seu IP será capturado, o risco de um malware invadir seu equipamento é enorme e provavelmente alguma agencia governamental irá capturar seus dados.

Após alguns parágrafos alarmistas, informe que tecnicamente, são uma rede dentro da rede, com IP aleatórios, mascarado e roteado centenas de vezes, para nunca sabermos onde o computador servidor está hospedado, firewall poderosos, VPN altamente sofistica garantem o anonimato.

Quando foi criada Dark Web?

Eu acredito que a Dark Web surgiu antes da Arpanet, provavelmente a ARPANET foi criada através de um no da Dark Web, que cresceu e emergiu para o publico final, pense caro padawan, após a queda do Fascismo e o surgimento do Mundo Livre separado pela cortina de ferro, Ocidente Versus Oriente, Azuis Versus Vermelhos, Capitalistas Versus Comunistas, o mundo vivia uma paranoia da Guerra Nuclear e informação virou poder.

As redes telegráficas e redes radiofônicas eram facilmente grampeáveis e os dados eram fáceis de serem roubados, por isso agencias de segurança usavam suas redes TOP Secrets, então é difícil precisar a data, mas com toda certeza foi anterior a 1969.

Primeiramente usada por agências de espionagem no melhor estilo James Bond, com poucos nos e poucos usuários, mas mesmo assim ligando continentes e coma ARPANET, estudantes e cientistas começaram a explora-la.

Imagine que sempre terá pornografia, drogas e segredos escondidos no fundo dos diretórios de computadores e acessados por meios obscuros. Protegido dos olhares curiosos e indiscretos, vamos avançar um pouco mais.

O surgimento da Clear Web

Com a Arpanet funcionando e interligando o mundo, foi dado o passo seguinte, a internet torna-se universal e democraticamente acessível, para quem tivesse capital suficiente para comprar um microcomputador e ter acesso há uma linha telefônica e um provedor de acesso via Modem.

A década de 80 foi a década das redes internas e fechadas interligadas por cabo coaxial e os anos 90 foram a democratização total, porem os Governos com a experiência dos anos anteriores continuavam com sua missão de Vigiar e Punir, um grupo de cyberativistas que lutavam pela liberdade e queriam maior liberdade de falar sem censura, desenvolveram tecnologias de ofuscamento e redes privadas, com alto grau de virtualização, mas mesmo assim não conseguiam escapar da vigilância, principalmente com o Echelon funcionando em suas versões Alfa.

Neste ponto a necessidade fez a ocasião, a contra inteligência estrangeira estava capturando muitos espiões e operacionais norte-americanos, devido a vigilância da rede e a captura de pacotes navegando na rede.

A necessidade de segurança e proteção a essas pessoas, fez oficiais da inteligência da Marinha desenvolvessem um projeto, o TOR – The Onion Router, o roteador cebola ou em camadas, fez tanto sucesso, porem era caro e necessitava de uma equipe dedicada e cara, qual a solução? Tornou-se um projeto open source.

O que é TOR?

Resumidamente é um navegador WEB, ao melhor estilo IExplore, Firefox, Opera ou Chrome, porem com uma camada de ofuscação e invisibilidade que garante o anonimato e proteção do usuário, mas atenção na internet nada é 100% seguro.

Como funciona a DARK WEB

São website anônimos sem registros em servidores DNS e praticamente intermitentes, as vezes existem outras não, com endereços dinâmicos, muitas vezes funcionam em pontos peer-to-peer, em que os visitantes recebem as urls e acessam, porem expirando após algum tempo.

Para que serve a DARK WEB

Além de playground para crackers é um bar aberto semelhante a Porto Royale, uma terra sem dono e que tudo podem, venda de segredos, armas, drogas, pornografia e coisas proibidas. Uma grande dor de cabeça para as autoridades, pois os grupos utilizam-se da burocracia estatal e pouco poder da policia local, com equipes multinacionais e altamentes treinadas.

Onde fica a DARK WEB?

Normalmente existem servidores em países com legislação fraca e altamente corruptos, ou seja 10 a 15 países do mundo, porem com o alto grau de ofuscamento em alguns países ricos pequenos servidores e repetidores são instalados nos lugares mais incríveis possíveis.

Mercados Proibidos SILK ROAD

Foi um dos mais mediáticos mercados proibidos da DEEP WEB, situado nas profundezas da DARK WEB, onde as transações eram pagas em BITCOINS e outras criptomoedas, transações anônimos e secretos.

Deu muito trabalho para o FBI até que em 2013 foi fechado e seu administrador preso e condenado a Prisão Perpetua, mas como uma hidra de lerna, suas ramificações ganharam vida própria e a polícia fecha um, abrem três ou quatro outros.

Os antigos sites de Torrent segue o mesmo princípio, neste jogo de gato e rato interminável, duro e louco.

Posso visitar a DARK WEB

Sim, mas lembre-se que somos DEVs e temos um código de ética e regras de conduta, que proíbem nossa participação em associações criminosas, ninguém quer ter o nome fichado pela polícia e ter um araponga investigando nossos equipamentos.

Existe risco em visitar?

Sim, risco alto devido aos inúmeros malwares, a melhor alusão é andar num campo minado, vai por conta e risco próprio.

Antivírus me protegera?

Infelizmente não, lembre-se os antivírus são reativos, apenas protegem contra ameaças conhecidas, as novidades testadas nos LABs da Dark Web possuem tecnologia anti-antivirus, usar o TOR protege, mas não eficientemente, os protótipos do mal estão a solta.

O sistema operacional ideal: LINUX

Para os curiosos de plantão, o ideal para iniciar os estudos é dominar o LINUX, por ser um sistema operacional com muitas ferramentas e ser mais seguro para navegar pelas profundezas da WEB, saber usar via linha de comandos é uma arte.

Explore as redes E-Mule e Bit-Torrent

São antigos softwares peer-to-peer evoluindo através da comunidade do software livre, onde o open-source permitiu a comunidade incluir novas funcionalidades, testa-las e libera-las mais rapidamente.

Conclusão

PAdawan espero ter sido claro e explicado bem o conceito da DARK WEB, o lugar mais escuro e profundo da DARK WEB, não é um lugar para visitar e bobear, se for por curiosidade acadêmica, saiba que ira dar-se mal.

Muitos trolls habitam esses lugares em busca de diversão, prontos a fazerem maldades e judiar de novatos, este texto será evoluindo ao longo do tempo, por isso volte mais vezes, afinal é um trabalho em curso delongo prazo.