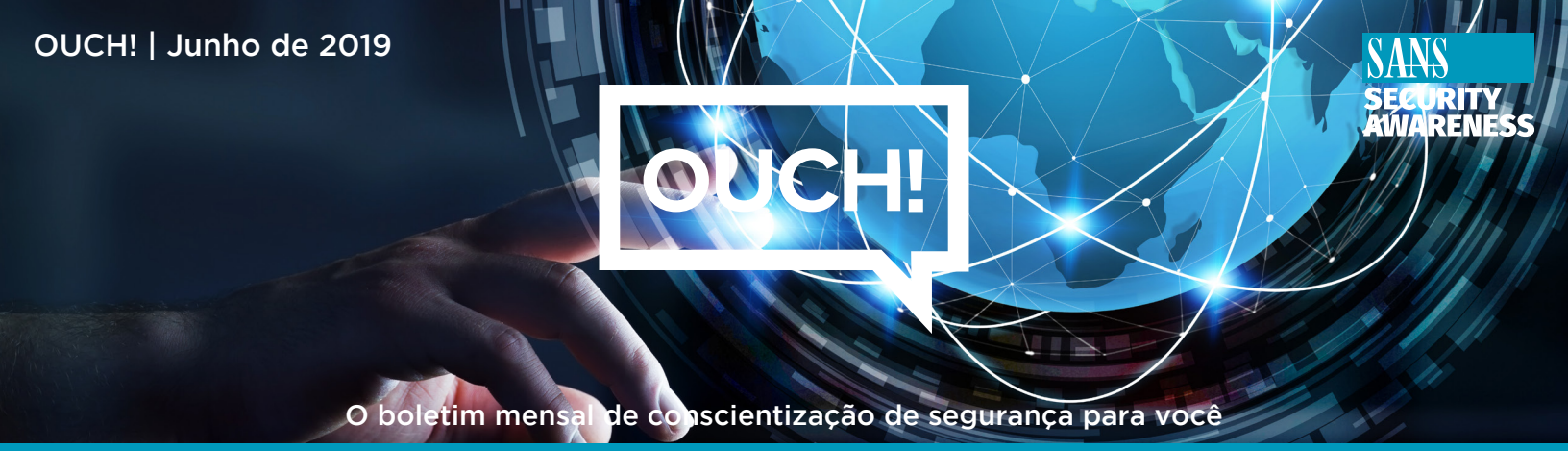

O boletim mensal de conscientização de segurança para você

Dark Web

Visão geral

Você pode ter ouvido falar da “Dark Web” por meio de outras pessoas ou na mídia e se perguntou “o que é a Dark Web?” Ou “eu deveria estar fazendo alguma coisa a respeito?”. Hoje explicaremos o que é a Dark Web e o que isso significa para você.

O que é isso?

A Dark Web consiste em sistemas na Internet feitos para comunicação ou compartilhamento de informações de forma segura e anônima. Não há somente uma “Dark Web”; não é como o Facebook, que é administrado por uma única organização. Pelo contrário, a Dark Web é uma coleção de sistemas e redes diferentes gerenciados por diferentes pessoas, usados para diversas finalidades. Esses sistemas ainda estão conectados e fazem parte da Internet, no entanto, você geralmente não os encontrará usando seus motores de busca normais. Você também precisa de um software especial no seu computador para encontrá-los ou acessá-los. Um exemplo é o Projeto Tor. Para acessar essa Dark Web, baixe e instale o Navegador Tor. Ao se conectar a servidores online usando o Navegador Tor, seu tráfego criptografado viaja através de outros computadores utilizando também o Tor. Conforme passa por esses computadores, o endereço IP de origem está mudando, o que significa que, quando você acessa o site, sua atividade online está anônima. Outros exemplos de Dark Webs são Zeronet, Freenet e I2P.

Quem usa isso?

Os criminosos cibernéticos usam frequentemente a Dark Web. Eles mantêm sites e fóruns na Dark Web para viabilizar suas atividades criminosas, como comprar drogas ou vender gigabytes de dados hackeados - tudo de forma anônima e segura. Por exemplo, quando um criminoso cibernético invade um banco ou uma loja de compras online, roubam o máximo de informações possível e depois vendem essas informações a outros criminosos cibernéticos em sites da Dark Web.

Há também usos legítimos da Dark Web. Por exemplo, pessoas em países onde a censura é excessiva podem acessar as redes Dark Web para compartilhar informações e ver o que mais está acontecendo no mundo, enquanto protegem sua privacidade e permanecem anônimas. Jornalistas, informantes e pessoas que adoram privacidade podem usar a Dark Web para aumentar

seu anonimato e driblar a censura. Além disso, indivíduos como esses podem usar tecnologias como o Navegador Tor, não só para acessar a Dark Web, mas para navegar anonimamente na Internet normal.

O que eu deveria fazer?

Se você não tiver um motivo específico para acessar a Dark Web, recomendamos não acessá-la. Alguns sites da Dark Web são utilizados para atividades ilegais, muitos dos sites usarão seu computador em uma rede ponto a ponto para atingir suas metas e, em certos casos, seu computador poderá ser investigado ou atacado. Algumas empresas oferecem serviços de monitoramento para informá-lo se seu nome ou outros dados foram roubados por criminosos cibernéticos e encontrados na Dark Web. O valor real desses serviços é questionável. O melhor jeito de se proteger é assumir que algumas das suas informações já estão na Dark Web sendo usadas por criminosos cibernéticos. Sendo assim . . .

- **Suspeite de telefonemas ou e-mails fingindo ser uma organização oficial e pressionando você a tomar uma ação, como pagar uma multa. Os criminosos podem até mesmo usar informações que encontraram sobre você para elaborar um ataque personalizado.**
- **Monitore seu cartão de crédito e extratos bancários. Talvez até mesmo configure alertas diários sobre quaisquer transações que aconteçam. Desse modo, você pode detectar se está acontecendo alguma fraude financeira. Se você detectá-lo, denuncie imediatamente à sua empresa de cartão de crédito ou banco.**
- **Congele sua pontuação de crédito. Isso não afeta como você pode utilizar seu cartão de crédito e é uma das medidas mais eficazes que você pode tomar para se proteger do roubo de identidade.**

Editor convidado

Micah Hoffman *(@WebBreacher) é o Pesquisador Principal na Spotlight Infosec LLC, um Instrutor Certificado pelo SANS Institute e autor dos cursos OSINT do SANS. Micah demonstra toda sua paixão pela inteligência cibernética e de código aberto por meio de seus projetos, cursos e estilos de ensino.*

Recursos

Ataques Personalizados: https://www.sans.org/u/RfW
Engenharia Social: https://www.sans.org/u/Rg1
Roubo de identidade: https://www.identitytheft.gov
Congelamento de crédito: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Navegador Tor: https://www.torproject.org/
Curso OSINT do SANS: https://sans.org/sec487