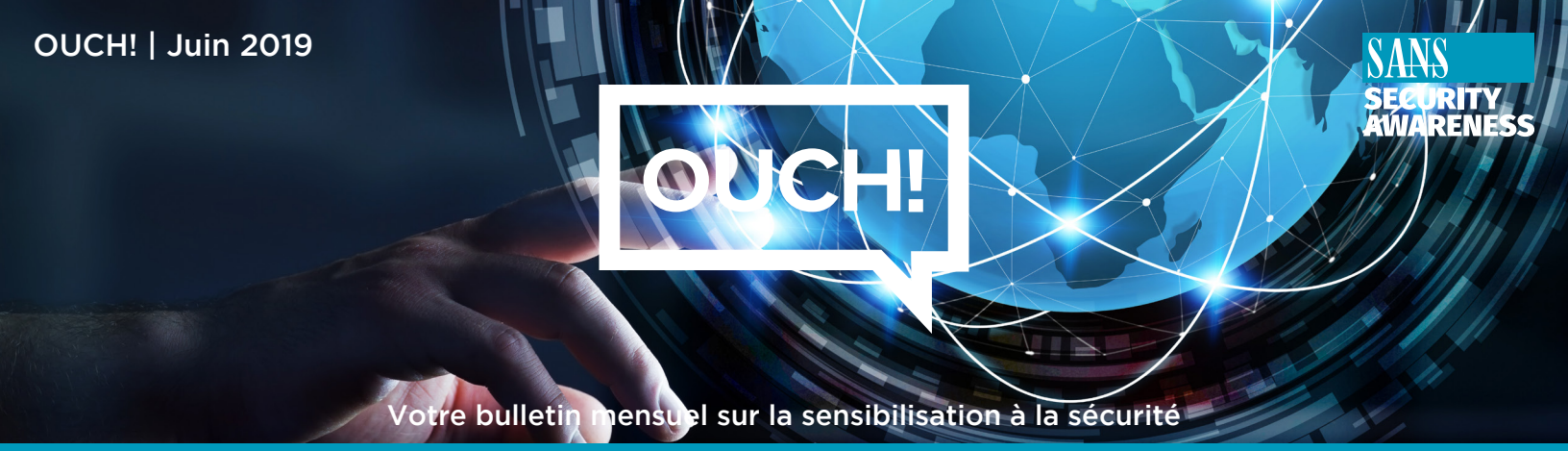

Votre bulletin mensuel sur la sensibilisation à la sécurité

Dark Web

Aperçu

Vous avez peut-être entendu parler du terme “Dark Web” dans l’actualité et vous êtes demandé “*qu’est-ce que le Dark Web ?*” ou “*dois-je faire quelque chose à ce sujet ?*” Aujourd’hui, nous expliquons ce qu’est le Dark Web et en quoi cela vous concerne.

Qu'est-ce que c'est ?

Le Dark Web est constitué de systèmes sur Internet conçus pour communiquer et partager de l’information de manière sécurisée et anonyme. Il n’y a pas un seul “Dark Web” : ce n’est pas comme par exemple Facebook, qui est exécuté par une seule organisation. En fait, le Dark Web est un ensemble de systèmes et réseaux différents gérés par différentes personnes et utilisés à des fins variées. Ces systèmes sous toujours connectés et font parti d’Internet, mais vous ne les trouverez généralement pas en utilisant les moteurs de recherche habituels. En général, vous avez besoin de logiciels spécifiques sur votre ordinateur pour les trouver et y accéder. Un exemple est Tor Project. Pour accéder à ce Dark Web, vous téléchargez et installez le navigateur “Tor Browser”. Quand vous vous connectez à des serveurs utilisant Tor Browser, votre trafic crypté voyage à travers d’autres ordinateurs qui utilisent aussi Tor. Alors que cela passe à travers d’autres ordinateurs, l’adresse IP de base change, donc quand vous arrivez sur le site, votre activité en ligne devient anonyme. D’autres exemples de Dark Web inclus Zeronet, Freenet et I2P.

Qui l’utilise ?

Les cybercriminels utilisent beaucoup le Dark Web. Ils maintiennent les sites et forums du Dark Web afin de faciliter leurs activités criminelles, telles qu’acheter de la drogue ou vendre des gigabytes de données piratées - tout ça de manière anonyme et sécurisée. Par exemple, quand un cybercriminel pirate une banque ou un magasin en ligne, il vole autant d’information que possible, puis la revend sur le Dark Web à d’autres cybercriminels.

Le Dark Web est aussi utilisé de manière légitime. Par exemple, dans certains pays où la censure est omniprésente, le Dark Web est utilisé pour partager de l’information et voir ce qu’il se passe dans le monde, en protégeant la vie privée et en restant anonyme. Journalistes, lanceurs d’alerte et autres soucieux du droit à la vie privée peuvent utiliser le Dark Web pour conserver

l'anonymat et contourner la censure. De plus, ces personnes peuvent utiliser des technologies comme Tor Browser pour non seulement accéder au Dark Web, mais aussi naviguer sur Internet de façon anynome.

Que puis-je faire ?

À moins que vous n'ayez des raisons bien précises, nous vous déconseillons d'accéder au Dark Web. Certains sites sur le Dark Web sont utilisés à des fins illégales. Ils utiliseront votre ordinateur en réseau pour atteindre leur but et pourront même sonder ou attaquer votre ordinateur. Certaines entreprises offrent leurs services pour contrôler si votre nom ou d'autre information a été volé par des cybercriminels et trouvé sur le Dark Web. La valeur réelle de ces services est discutable. La meilleure façon de se protéger est d'assumer que vos informations sont déjà utilisées par les cybercriminels sur le Dark Web. En conséquence . . .

- **Prenez garde des appels ou e-mails qui prétendent venir d'organisations officielles et qui vous poussent à agir, comme payer une amende. Les criminels peuvent même utiliser l'information qu'ils trouvent sur vous pour créer des attaques personnalisées.**
- **Contrôlez vos cartes bancaires et relevés de comptes. Peut-être même, mettez en place une alerte sur toutes vos transactions. Ainsi, vous pourrez détecter une fraude financière directement. Si cela arrive, reportez-la à votre banque immédiatement.**
- **Mettez votre cote de crédit en gel. Cela ne changera pas la manière dont vous utilisez votre carte bancaire, mais c'est une des étapes la plus efficace pour vous protéger du vol d'identité.**

Rédacteur Invité

Micah Hoffman *(@WebBreacher) est chercheur principal à Spotlight Infosec LLC, instructeur certifié SANS Institute et auteur pour les formations SANS OSINT. La passion de Micah pour l'intelligence du cyber et de l'open source se ressent dans ses projets, ses contenus de formation et son style d'enseignement.*

Ressources

Attaques personnalisées : https://www.sans.org/u/RfW
Ingénierie sociale : https://www.sans.org/u/Rg1
Vol d'identité : https://www.identitytheft.gov
Gel de crédit : https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor Browser : https://www.torproject.org/
Formation SANS OSINT : https://sans.org/sec487