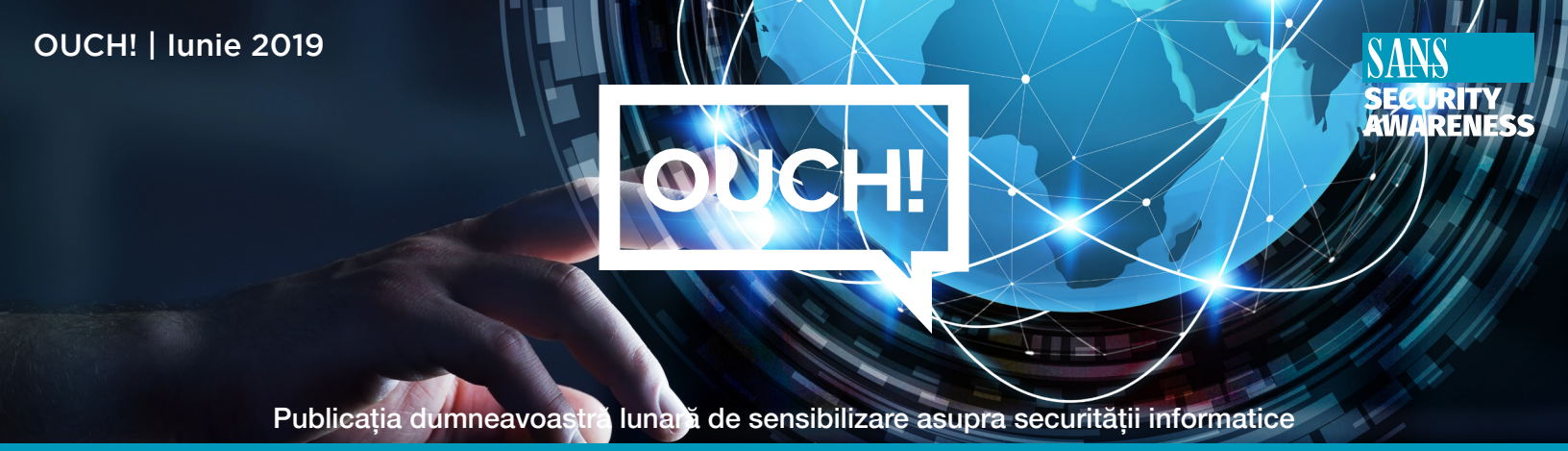

Publicația dumneavoastră lunară de sensibilizare asupra securității informatice

Dark Web

Prezentare generală

Este posibil să fi auzit termenul “Dark Web” folosit de alții sau în mass-media și să vă fi întrebat “*ce este Dark Web?*” Sau “*ce ar trebui să fac in privința lui?*”. Astăzi va explicăm ce este Dark Web și ce înseamnă pentru dumneavoastră.

Ce este?

Nu există un singur Dark Web; nu este ceva gen Facebook, condus de o singură organizație. În schimb, Dark Web-ul este o colecție de sisteme și rețele diferite, gestionate de persoane diferite, utilizate pentru diverse scopuri. Aceste sisteme sunt conectate și fac parte din Internet, dar, în general, nu le veți găsi utilizând motoarele de căutare normale. De asemenea, e posibil sa aveți nevoie de software special pentru a le găsi sau accesa. Un exemplu relevant este Proiectul Tor. Pentru a accesa acest Dark Web, trebuie sa descărcați și instalați motorul de căutare Tor. Când vă conectați la servere folosind Tor, traficul dvs. criptat se deplasează între computere care folosesc același motor de căutare. Pe măsură ce trece prin aceste computere, adresa IP sursă se modifică, ceea ce înseamnă că atunci când ajungeți pe site-ul dorit, activitatea dvs. online este anonimizată. Alte exemple de Dark Web includ Zeronet, Freenet și I2P.

Cine îl folosește?

Criminalii cibernetici sunt mari utilizatori de Dark Web. Administrează site-uri web și forumuri în Dark Web pe care își desfășoară activitățile lor criminale, cum ar fi cumpărarea de droguri sau vânzarea de date personale furate – totul anonim și securizat. De exemplu, atunci când un infractor cibernetic sparge o bancă sau un magazin online, fură cât mai multe informații posibil, apoi vinde informațiile respective altor infractori cibernetici pe site-urile Dark Web.

Există, de asemenea, utilizări legitime ale Dark Web. De exemplu, cei care locuiesc in țări unde cenzura este agresivă pot utiliza rețelele Dark Web pentru a împărtăși informații și pentru a vedea ce se mai întâmplă în lume, păstrând-și în același timp confidențialitatea și rămânând anonimi. Jurnaliști, denunțători („whistleblowers”) și persoane care doresc să își protejeze

intimitatea pot utiliza Dark Web pentru a spori anonimatul și a ocoli cenzura. În plus, acești oameni pot folosi tehnologii precum motorul de căutare Tor nu numai pentru a accesa Dark Web, ci și pentru a naviga în mod anonim pe Internetul obișnuit.

Ce ar trebui să fac?

Cu excepția cazului în care aveți un motiv întemeiat pentru a accesa Dark Web-ul, vă recomandam sa nu o faceți. Unele site-uri Dark Web sunt utilizate în scopuri ilegale, multe dintre ele vă vor folosi computerul în rețea pentru a-și atinge obiectivele, iar în unele cazuri computerul dvs. poate fi chiar detectat sau atacat. Unele companii oferă servicii de monitorizare pentru a vă informa dacă numele sau alte informații despre dvs. au fost furate de infractori cibernetici și găsite pe Dark Web. Valoarea reală a acestor servicii este însă discutabilă. Cea mai bună modalitate de a vă proteja este să presupuneți că unele dintre informațiile dvs. sunt deja pe Dark Web, fiind folosite de infractorii cibernetici. In consecință . . .

- **Fiți suspicios în legătură cu orice apeluri telefonice sau e-mailuri care pretind că vin de la instituții oficiale și vă presează să faceți o acțiune, cum ar fi plata unei amenzi. Infractorii folosesc informații găsite despre dvs. pentru a crea un atac personalizat.**
- **Monitorizați-vă cardurile și extrasele bancare. Dacă aveți opțiunea, setați-vă alerte zilnice cu privire la orice tranzacție care se întâmplă pe conturile bancare. În acest fel, puteți detecta tentativele de fraudă. Iar dacă le detectați, luați imediat legătura cu banca dvs.**

Versiunea în limba română

Ubisoft este o companie de jocuri. Un creator de lumi, dedicat îmbogățirii vieților jucătorilor cu experiențe de joc originale și memorabile. Aflați mai multe la: https://www.ubisoft.com/en-us/.

Editor invitat

Micah Hoffman *(@WebBreacher) este investigator șef la Spotlight Infosec LLC, un instructor certificat al Institutului SANS și autor al cursurilor SANS OSINT. Pasiunea lui Micah pentru cibernetică și sursele deschise de informație (open source) se observă în proiectele, cursurile și stilul său de predare.*

Resurse

Escrocherii personalizate:	https://www.sans.org/sites/default/files/2019-02/201902-OUCH-February-Romanian.pdf
Ingineria socială:	https://www.sans.org/sites/default/files/newsletters/ouch/issues/OUCH-201701_ro.pdf
Furtul de identitate:	https://www.identitytheft.gov
Motorul de căutare Tor:	https://www.torproject.org/
Cursul OSINT de la SANS:	https://sans.org/sec487