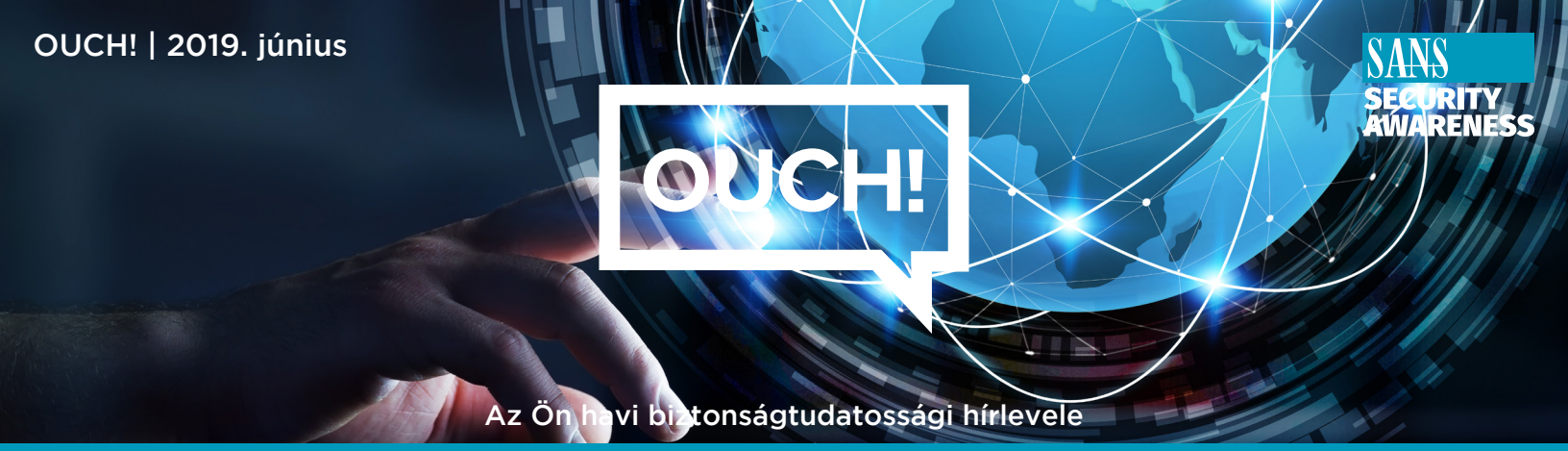
OUCH! | 2019. június



Az Ön havi biztonságtudatossági hírlevele

Sötét Web

Áttekintés

Valószínűleg hallotta már másoktól vagy a médiából a „Sötét Web” kifejezést, és csodálkozott azon, *hogy mi is az a Sötét Web*, *„kellene tudnom róla valamit?”*. Ma elmagyarázzuk, hogy mi a Sötét Web és ez mit is jelent az Ön számára.

Mi ez?

A Sötét Web olyan, az Interneten lévő rendszerekből áll, amelyeket biztonságos és névtelen kommunikációra, információ megosztásra terveztek. Nincs egyetlen egy „Sötét Web”, ez nem olyan, mint a Facebook, amit egyetlen szervezet működtet. Ehelyett a Sötét Web különböző rendszerek és hálózatok összessége, amelyeket több személy irányít és eltérő célokat szolgálnak. Ezek a rendszerek is az Internethez kapcsolódnak, részei annak, azonban a hagyományos kereső motorokkal nem találhatja meg őket. Felfedezésükhöz és elérésükhöz gyakran speciális szoftverre van szükség. Egy példa erre a Tor projekt. Ahhoz, hogy hozzáférjen a Sötét Webhez, le kell töltenie és telepítenie kell a Tor böngészőt. Amikor a Tor böngészőt használva kapcsolódik egy webszerverhez, a titkosított adatforgalom más Tor böngészőt használó számítógépeken is keresztülfolyik. Ezeken a számítógépeken ugrálva a forrás IP cím megváltozik, így amikor eléri a weboldalt, az Ön online tevékenysége teljesen anonimmá válik. További példák a Sötét Webre a Zeronet, a Freenet és az I2P.

Kik használják?

A Sötét Web jellemző felhasználói a kiberbűnözők. Weboldalakat és fórumokat tartanak fenn a Sötét Weben, hogy hátteret biztosítsanak az olyan bűnözői tevékenységeikhez, mint például a drogkereskedelem vagy több gigabyte-nyi feltört adat eladása – mindezt névtelenül és biztonságosan. Például amikor egy kiberbűnöző megtámad egy bankot vagy online boltot, annyi adatot lop el, amennyit csak tud, majd ezeket az adatokat eladja más kiberbűnözőknek a Sötét Web oldalain.

A Sötét Weben vannak legitim felhasználók is. Például, azok az emberek, akiknek az országában cenzúra uralkodik, információ megosztásra, hírek megismerésére használhatják a Sötét Web hálózatát, védve magánéletüket és megtartva névtelenségüket. A cenzúra megkerülésére újságírók, informátorok és a személyes adatuk védelméért aggódó emberek is használhatják a Sötét Webet, hogy megtarthassák névtelenségüket. Ráadásul az ilyen személyek a Tor böngészőhöz hasonló technológiát nemcsak arra használhatják, hogy elérjék a Sötét Webet, hanem arra is, hogy a hagyományos Interneten is névtelenül böngésszenek.

Mit kellene tennem?

Hacsak nincs különleges oka a Sötét Web használatára, óva intjük tőle. Néhány Sötét Webes oldalt illegális célból üzemeltetnek, ezek közül számos oldal céljai elérése érdekében használni fogja a számítógépét egy peer hálózatban; egyes esetekben pedig számítógépe támadás áldozatává is válhat. Néhány cég monitorozási szolgáltatásokat kínál, amelyek során értesítik Önt, ha nevét vagy más adatait kiberbűnözők ellopták és az megtalálható a Sötét Weben. Ezeknek a szolgáltatásoknak a valós értéke megkérdőjelezhető. A legjobb út, hogy megvédje magát, ha azt feltételezi, hogy néhány adata már fent van a Sötét Weben, amit kiberbűnözők használnak. Ennek eredményeként...

- **Legyen gyanakvó minden olyan telefonhívásnál, e-mail-nél, amikor hivatalos szervezetek arra próbálják rávenni, hogy cselekedjen, például adott összeget utaljon el. A bűnözők az Önről talált adatokat akár ahhoz is felhasználhatják, hogy személyre szabott támadást indítsanak.**
- **Ellenőrizze bankkártyáját és banki kimutatásait. Állítson be napi értesítést a banki tranzakciókra, így észlelheti, ha bármilyen pénzügyi csalás történik. Amennyiben ilyet tapasztal, haladéktalanul értesítse bankját vagy a kártya kibocsátóját.**
- **Fagyassza le hitelkeretét. Ez nem befolyásolja a hitelkártya használatát és a leghatékonyabb lépés, hogy megvédje magát a személyazonosság-lopásoktól.**

Magyar Kiadás

A Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet (NBSZ NKI) látja el Magyarországon az állami és önkormányzati szervek vonatkozásában az elektronikus információbiztonsági hatósági, eseménykezelési, valamint a sérülékenység-vizsgálati feladatokat. Az NKI rendeltetése, hogy előmozdítsa a kormányzati szektor elektronikus informatikai rendszerei biztonsági szintjének emelését, valamint, hogy fejlessze a közigazgatásban dolgozó felhasználók biztonságtudatos viselkedését a kibertérben. A nemzetközi és hazai partnerkapcsolatai révén az NKI hozzájárul a magyar kibertér biztonságának erősítéséhez. További információ az Intézetről a https://nki.gov.hu oldalon olvasható.

A szerzőről

Micah Hoffman *(@WebBreacher) a Spotlight Infosec LLC fő kutatója, SANS tanúsítvánnyal rendelkező oktató, valamint a „SANS OSINT" - „SANS – Nyílt forrású információszerzés" tanfolyamok szerzője. Micah kiber és nyílt forrású információszerzés iránti szenvedélye megmutatkozik projektjeiben, oktatási anyagaiban, valamint tanítási stílusában.*

Források

Személyre szabott támadások:	https://www.sans.org/u/RfW
Pszichológiai manipuláció:	https://www.sans.org/u/Rg1
Személyazonosság-lopás:	https://www.identitytheft.gov
Hitel fagyasztás:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/
Tor böngésző:	https://www.torproject.org/
SANS nyílt forrású információszerzés:	https://sans.org/sec487