infojegyzet

ORSZÁGGYŰLÉS HIVATALA
KÖZGYŰJTEMÉNYI ÉS KÖZMŰVELŐDÉSI IGAZGATÓSÁG
KÉPVISELŐI INFORMÁCIÓS SZOLGÁLAT

2021/14.
2021. április 16.

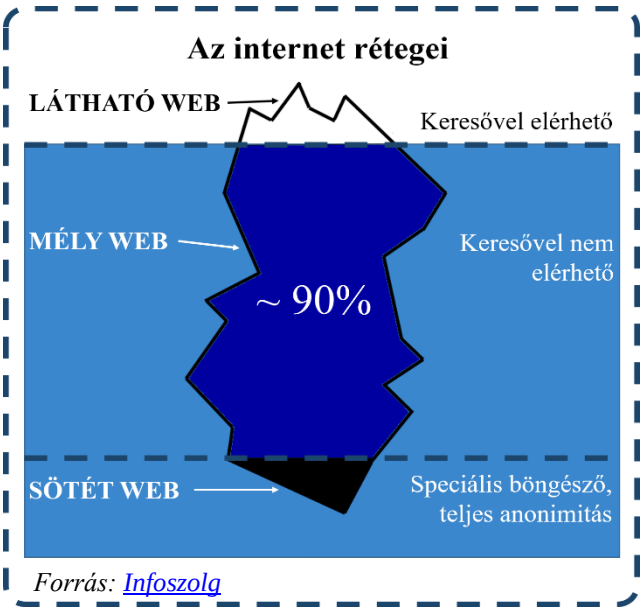
A SÖTÉT WEB

- **Az internet jelentős része a hagyományos böngészők által elérhetetlen, ennek a tartománynak azonban csak a "legalsó" részét szokás sötét webnek nevezni.**
- **A sötét web csak speciális böngészővel érhető el, s az itt böngészők, eladók, vevők, valamint az oldalak fenntartóinak kiléte nem beazonosítható.**
- **A sötét weben történő böngészés önmagában nem törvénytelen, diktatúrákban élő polgárok számára az információhoz jutást és a véleményszabadság lehetőségét nyújtja.**
- **A sötét weben piacterek kínálnak tiltott és lopott árukat, s különféle oldalak törvénytelen szolgáltatásokat.**
- **A kínálat jelentős részben kábítószerekből, fegyverekből, hamis okmányokból és lopott adatokból áll.**
- **Jelentős a sötét weben a gyermekpornográf oldalak száma is.**
- **A sötét web fizetőeszköze a bitcoin, mert ez is garantálja az anonimitást.**
- **Mind a piacterek és látogatóik száma, mind a termékkínálat folyamatosan nő.**
- **A rendőri szervek összehangolt és összetett nyomozása vezethet egyes illegális piacterek sikeres kiiktatásához.**

A Képviselői Információs Szolgálat alábbi Infojegyzete a világháló titkosított, úgynevezett sötét részét mutatja be, amely a tiltott és hamis termékek piactereinek is otthont ad. Áttekinti ennek a sötét webnek a működését, tartalmát, méreteit, végül pedig az ellene folytatott küzdelem sajátosságait.

Az internetes böngészés a korlátlanság érzetét kelti, hiszen információk kimeríthetetlen tárházát nyújtja a Föld bármely pontjáról. Pedig a világháló bárki által hozzáférhető, nyilvános része, amelyen a keresőmotorok keresnek, csak a teljes internet töredékét, legfeljebb a 3–5 százalékát teszi ki. A többi része "láthatatlan", vagyis tartalmukra nem lehet rákeresni, azok nem elérhetőek bárki számára. A világhálónak erre a részére használják a **mély web** (deep web) kifejezést, s ez teszi ki annak mintegy 90 százalékát, mások szerint a látható web 400–500-szorosát (Serbakov, 2020).

Ide tartoznak a jelszóval elérhető, illetve tűzfallal védett személyes tartalmak, a levelező-fiókok, a netbankok, a munkahelyi felhőszolgáltatások, elektronikus ügyintézési lehetőségek, s azok a régen feltöltött tartalmak, amelyek mára már láthatatlanná váltak a keresőszolgáltatások számára.



Forrás: Infoszolg

Végül az internet "legalsó" rétege a **sötét web** (dark web) elnevezést kapta. Itt a felhasználók anonimitása a nyílt interneten megszokottnál sokszorosan védettebb, a böngészés titkosított. Éppen ezek a tulajdonságok tették a sötét webet a bűnözés és az illegális tartalmak gyűjtőhelyévé, ugyanakkor ennek a szférának a méretét illetően a legnagyobb a bizonytalanság is. Egyesek szerint a világháló 1–2 százalékát foglalja el, mások szerint már meghaladta a nyilvános web méreteit.

A SÖTÉT WEB SAJÁTOS MŰKÖDÉSE

A sötét web eléréshez elegendő egy ingyenes, ám speciális böngésző le-

töltése, a legelterjedtebb közülük a TOR (The Onion Router) nevet viseli. A böngésző nevében szereplő angol "onion", azaz hagyma szó arra utal, hogy a böngészést és az üzenetküldést ugyanolyan sokszorosan rétegzett titkosítás védi, ahogyan a hagyma is egymást fedő rétegekből áll. A weboldalak címei is "onion" végződéssel rendelkeznek például "com" vagy "org" helyett.

A hagyományos internetes böngészés közben a keresések, a kommunikáció, a vásárlások nyomon követhetők, általuk a felhasználó beazonosítható. Ugyanez a TOR esetében nem lehetséges, itt csak annyi látható, hogy a felhasználó a TOR hálózatot használja. Ez a böngésző ugyanis saját hálózatot tart fenn, amely szerverek láncolatából áll. Ezek között véletlenszerűen halad a küldő fél üzenete szerverről szerverre, míg meg nem érkezik a céljához. S a lényeg, hogy sem a "menet közben" érintett szerverek, sem a "célállomás" nem tudja beazonosítani a küldő felet. Utóbbi is csak az üzenet tartalmát, mint a "hagyma" belsejét tudja kibontani.

A teljes anonimitást biztosító rendszert az Egyesült Államok Tengerészeti Kutató Laboratóriuma fejlesztette ki 2002-ben azért, hogy a haditengerészet egységei a felderítés veszélye nélkül kommunikálhassanak egymással. 2006-tól vált a különleges hálózat bárki számára elérhetővé abból a megfontolásból, hogy a hálózaton keresztül böngészők számának növekedése a kommunikáció – a haditengerészet számára az információszerzés – hatékonyságát fogja növelni, miközben az anonimitás továbbra sem sérül.

A TOR böngésző használata önmagában nem törvénybe ütköző cselekedet, sokan a magánéletük megóvása érdekében használják böngészésre. Fontos szerepe van a **szólás- és véleményszabadság biztosításában** a diktatórikus berendezkedésű országok polgárai számára, hiszen lehetővé teszi, hogy bárki a lelepleződés veszélye nélkül széleskörű információkat szerezzen, illetve osszon meg a világ közvéleményével, netán segítséget kérjen. A Facebook, a Youtube is megtalálható a sötét weben éppen azért, hogy olyan országok polgárai számára is hozzáférhető legyen, ahol korlátozzák a működését. Hasonlóképpen a The New York Times is saját oldalt nyitott a sötét weben.

Tényfeltáró és oknyomozó újságírók is előszeretettel használják a sötét webet, hiszen itt tudnak a lelepleződés veszélye nélkül találkozni informátoraikkal. A kiszivárogtatott titkos kormányzati dokumentumokat nyilvánosságra hozó Wikileaks nemzetközi szervezet is alkalmazta a sötét webet informátorai névtelenségének megőrzése érdekében.

Az anonimitás azonban az alvilág számára is csábító, ezért a sötét web hamar a lopott vagy **tiltott áruk és törvénytelen szolgáltatások piacterévé** vált. Ellentmondásos helyzet keletkezett: az Egyesült Államok rendőrségének olyan bűnözői csoportok ellen kell küzdenie, akik a kormányzat által fejlesztett és támogatott technológiát használják működésük terepeként.

A SÖTÉT WEB ILLEGÁLIS TARTALMA

A sötét web piacterei működésükben a látható weben megszokott olyan nemzetközi online kereskedelmi oldalakhoz hasonlítanak, mint az eBay vagy az Amazon, ám azokkal ellentétben itt mindent árusítanak, amely az egyes országokban tiltottnak számít; **kábítószerek, fegyverek és hamis vagy lopott okmányok, hamis bankjegyek** a legkelendőbb árucikkek, a választék pedig rendkívül széles. Amikor 2017-ben az Alphabay nevű feketepiaci oldalt a hatóságok felszámolták, az oldal 250 ezernél is több illegális drog és más vegyi anyagok hirdetéseit tartalmazta (FBI, 2017).

Nagy a választék számítógépek megtámadására, feltörésére alkalmas szoftverekből, továbbá bankfiókok **ellopott** bejelentkezési adataiból, mások bankkártyájának használatához szükséges adatokból, s általában **felhasználónevekből és jelszavakból**. Mi több, árusítják egyes személyek teljes személyes adatkészletét: nevét, születési adatait, társadalombiztosítási azonosítóját, számlaszámát és számos egyéb azonosítóit (Bitport, 2019). 2020-ban mintegy 500 millió Facebook-felhasználó adatait árusította egy hacker-csoport a sötét weben, közülük 370 ezren magyarok voltak (Quadron-HVG, 2020). Egy kutatás szerint összesen mintegy 15 milliárd felhasználónév és a hozzá tartozó jelszó kering a sötét weben (Digital Shadows, 2020).

Illegális és lopott áruk kereskedelme mellett bűncselekményekkel felérő szolgáltatásokat is kínálnak az internet "sötét részén": tiltott szerencsejátékokat, embercsempészetet, sőt, szervkereskedelmet és bérgyilkosságot kínáló oldalak is várják megrendelőiket (Hurtony, 2018).

Hatalmas mennyiségben találhatók **gyermekpornográf oldalak** is a sötét weben. A Porthsmouthi Egyetem 2014-ben végzett kutatásai szerint a sötét web internetes forgalmának akár több mint 80 százalékát ilyen anyagok tehetik ki (Business Insider, 2014).

A termékek és szolgáltatások ellenértékét kriptovalutával, jellemzően **bitcoinnal** engedik kiegyenlíteni, mert a vásárló ennek költése során is megőrzi anonimitását. A bitcoin használatának árnyoldalaihoz tartozik továbbá, hogy terroristák és más bűnözők is használják, s nemcsak fizetőeszköz gyanánt, de pénzmosásra is (Serbakov, 2020).

A COVID-19 hatása a sötét web piacára

A sötét web piacainak kínálatában 2020-ban hamar megjelentek a koronavírus járvánnyal összefüggő termékek.

A londoni City Egyetemen végzett kutatás 2020 első tizenegy hónapjában vizsgálta az illegális online piacterek hirdetéseit, s azt találta, hogy a védőeszközök és a hatásosnak hirdetett gyógyszerek mellett megjelentek a választékban csalóknak szánt oktatóvideók, vírusteszt, hamis orvosi dokumentumok, hamis negatív tesztek, sőt lélegeztetőgépek is (Baronchelli, 2020).

Később koronavírus elleni vakcinákkal, és hamis, védettséget igazoló kártyákkal bővült a repertoár (Wired, 2021), ezek kínálata 2021 január és március között a háromszorosára nőtt (BBC, 2021).

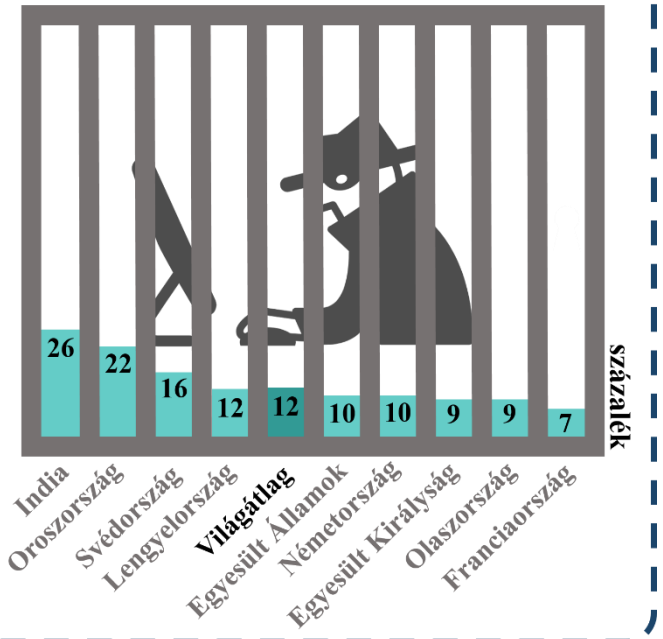
A SÖTÉT WEB HASZNÁLATÁNAK ADATAI

Rendkívül nehéz a sötét web szerteágazó volta miatt a használat méreteit meghatározni. Az első itteni piactér a Silk Road (Selyemút) nevet viselte, s eleinte kifejezetten a kábítószer-kereskedelem terepéül szolgált. Első változatában 2011 és 2013 között működött, ezekben az években mintegy 150 ezer vásárlója és 4000 eladója volt, mindkét szerepben az Egyesült Államokban élők voltak jelentős túlsúlyban (Lacson&Jones, 2016). Ehhez képest a DarkMarket nevű online piactér 2019-ben indult a sötét weben és 2021 januárjában számolták fel. Ez idő alatt mintegy 500 ezer vásárlója volt, s több mint 2400 eladó árusított itt. A két év alatt 320 ezer üzletet bonyolítottak le, ezek összértéke több mint 140 millió euró volt (Europol, 2021).

A nyomozó hatóságok leggyakrabban az oldalak felszámolásakor nyernek információt a piacok méreteiről. 2020-ban egy vizsgálat összesítette 31 illegális piactér 2011 és 2019 közötti adatait, melyek közül 24-et lekapcsoltak. Eszerint a nyolc év során körülbelül 8,3 millió felhasználó lépett érintkezésbe valamelyik oldallal a sötét weben, s eközben 4,2 milliárd amerikai dollárt cserélt gazdát (Scientific Reports, 2020).

A piaci forgalom folyamatosan emelkedő tendenciát mutat, **2020 folyamán** a sötét web piacterein **1,7 milliárd dolláros forgalmat** bonyolítottak, a legtöbbet Oroszországban és az Egyesült Államokban élők költötték itt el (Chainanalysis, 2021).

A sötét web használatához szükséges technológiával rendelkezők aránya az internethasználók között, 2019 február



Forrás: Infoszolg/Statista

Egy 2019 év elején készült vizsgálat országonként mérte a teljes, internetet használó közösségben a sötét web használatához szükséges böngészőt alkalmazók, azaz a vélhetően sötét webet látogatók arányát. Azt találták, hogy világviszonylatban India állt az élen 26 százalékkal, de Oroszországban is az internetező lakosság 22 százaléka böngészik a sötét weben (Statista, 2019). Elsősorban utóbbiak számára működik a Hydra elnevezésű, orosz nyelvű piactér, melynek 2021 elején 2,5 millió regisztrált látogatója volt (Gemini Advisory, 2021).

Bűnüldözés a sötét weben

Jelenleg becslések szerint **legalább 38 online piactér** működik a sötét weben, de a számuk az ellenük indított összehangolt rendőri akciók miatt folyamatosan változik (Scientific Reports, 2020).

Egy-egy piactér működtetőjének és eladóinak beazonosítása azonban éppen a titkosítás magas szintje miatt rendkívül nehéz. Bevett módszer a **beépülés**, amikor a rendőrség ál-vevőként próbál az eladókról információt szerezni.

Az első jelentős piactér, a kábítószer-kereskedelemre szakosodott Silk Road működetőjének kilétét úgy sikerült felfedni, hogy az oldal indulása táján egy bitcoin fórumon beazonosítható e-mail címet tett közzé. 2013 októberében sikerült az oldalt felszámolni, az üzemeltetője pedig életfogytig tartó börtönbüntetést kapott.

Öt héttel a felszámolást követően azonban megjelent a Silk Road 2.0, mely megjelenésében és működésében is csaknem azonos volt az elődjéhez. Ennek az oldalnak a felszámolására több más piactérrel együtt 2014 novemberében került sor egy összehangolt, az amerikai Szövetségi Nyomozó Iroda (FBI) és 15 további ország bűnüldöző szervének az összehangolt akciója következtében (Serbakov, 2020).

Minden sikeres rendőri akciót követően azonban újabb piacterek keletkeztek, s a méretük is egyre terebélyesebb lett. A 2017-ben felszámolt Alphabay feketepiac például tízszer nagyobb volt, mint az első Silk Road.

2015-ben az FBI nem kapcsolta le azonnal az egyik legnagyobb, 250 ezer regisztrált taggal működő gyermekpornográf oldalt, hanem még két hétig tovább működtette, hogy közben egy kémprogram segítségével megkísérelje minél több felhasználó beazonosítását (ORIGO, 2016).

A feketepiacok elleni sikeres akciók évről évre folytatódnak. Az európai rendőrség (Europol) 2018-ban külön csoportot állított fel, hogy a sötét web elleni küzdelem szereplőinek munkáját összehangolja (Dark Web Team).

Források:

- Wesley Lacson – Beata Jones: The 21st Century DarkNet Market: Lessons from the Fall of Silk Road – International Journal of Cyber Criminology, 2016/1.
- Hurtony Alexandra: Rémségek bazára – ArsBoni, 2018. július 16.
- Ennyiért adják-veszik legkényesebb személyes adatainkat a Dark Weben – Bitport, 2019. május 31.
- Serbakov Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem – Büntetőjogi Szemle, 2020/1
- Abeer El Bahrawy – Laura Alessandretti – Leonid Rusnac – Daniel Goldsmith – Alexander Teytelboym – Andrea Baronchelli: Collective dynamics of dark web marketplaces – Scientific Reports, 2 November 2020
- From Exposure to Takeover – Digital Shadows Report, 2020
- DarkMarket: World's Largest Illegal Dark Web Marketplace Taken Down – Europol Press Release, 12 January 2021
- The Dark Web Is Teeming With Vaccine Listings Right Now – Wired, 25 March 2021

Készítette: Dr. Samu Nagy Dániel
Képviselői Információs Szolgálat
E-mail: infoszolg@parlament.hu

infoszolg

Internet: www.parlament.hu/infoszolg
Intranet: intra.parlament.hu/infoszolg/
Tel.: (1) 441-6486