CTI Jelentés

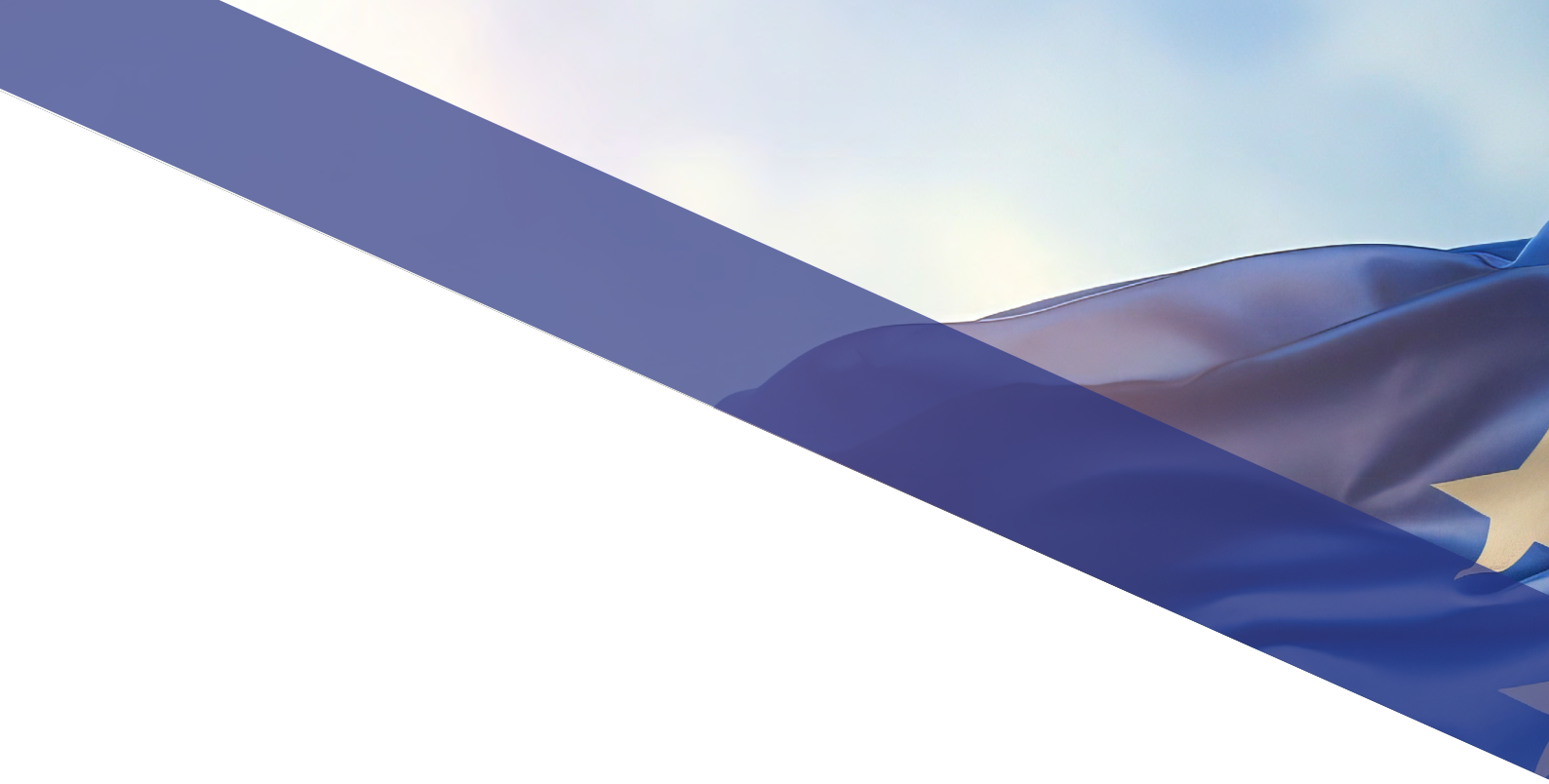
DoS-támadások

Az ENISA Threat Landscape for DoS Attacks című tanulmánya nyomán

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

enisa



Tartalomjegyzék

Mi az a Denial of Service Attack?

Közismert kibertámadási módszer, a köznyelvben gyakran csak **DoS-támadás**ként hivatkoznak rá, amely a definíció szerint olyan rendelkezésre állási támadásokat jelent, amelyek során a támadók részben vagy teljesen akadályozzák a célpont szolgáltatásának jogszerű használatát azáltal, hogy egy bizonyos időn keresztül kimerítik vagy kihasználják a célpont eszközeit.

A fogalom magyar megfelelője **szolgáltatásmegtagadással járó** vagy **túlterheléses támadás**.

A többi támadási típushoz képest kifejezetten kevés „nyomot" hagyó támadási formáról van szó, így már az észlelése is gyakran nehézségekbe ütközik. Gyakorlatban ez azt jelenti, hogy a támadók célja az, hogy megbénítsanak egy szolgáltatást – például egy weboldal elérését – oly módon, hogy a szolgáltatást kiszolgáló szervert elárasztják nagyszámú csatlakozási kérelemmel valós csatlakozási szándék nélkül. Az említett nagyszámú fals csatlakozási kérelem a hálózatot olyan mértékben igénybe veszi, hogy a valós kérelmeket **már nem tudja kiszolgálni** a rendszer, így a szolgáltatás **lelassul**, esetenként **teljesen elérhetetlenné** válik.

Kihangsúlyozandó, hogy a támadó **célja** ezekben az esetekben nem az illegális hozzáférés, hanem az, hogy a megtámadott szerver által nyújtott **szolgáltatás a többi, jóhiszemű felhasználó számára elérhetetlen legyen**. Ez a kibertámadási forma egyáltalán nem újkeletű, a kibervédelemmel foglalkozó tanulmányok rendszerint említést tesznek róla. Annak ellenére, hogy régi a módszer, még nem tűnt el, továbbra is gyakran használják, sőt egyes esetekben **emelkedő tendencia** figyelhető meg.

Mit mond az ENISA?

Az **Európai Unió Kiberbiztonsági Ügynökség**ének (**ENISA**) egyik legfontosabb célkitűzése a tudásmegosztás, melynek keretében az Ügynökség rendszeresen publikál tanulmányokat különféle kiberbiztonsági témákban. 2023 novemberében kiadásra került az ENISA Threat Landscape for DoS Attacks (January 2022 to August 2023) című kiadvány, melynek konkrét célkitűzése, hogy egy átfogó tudásanyagot adjon át a legújabb DoS-támadásokról, beleértve a támadások **motivációjának elemzését** és a támadások **hatását** is. Mindezzel természetesen elő kívánja segíteni a szervezetek kibertudatosságát, azáltal, hogy **jobban megérthetik** a támadások **hatásmechanizmusát,** valamint **elősegíthetik a védekezést**.

Jelen CTI jelentés a fent említett tanulmány feldolgozásával kíván mélyebb betekintést nyújtani a legújabb támadási trendekről.

Továbbra is fenyegetést jelentenek a DoS-támadások

A DoS-támadások jelenleg is állandó problémát jelentenek a szervezetek számára, mivel az ilyen támadások az utóbbi években egyre egyszerűbbé, olcsóbbá és agresszívabbá váltak. Tapasztalat szerint a világban kirobbanó új fegyveres konfliktusok világszerte új DoS-támadási hullámokhoz vezettek.

Az ENISA jelentés célja, hogy a támadások motivációjának és a fenyegetések alapos elemzésén keresztül segítsen a fenyegetett szervezeteknek a hatékonyabb védekezésben. A jelentés a 2022 január és 2023 augusztus között bekövetkezett incidenseket vizsgálja. Tapasztalat szerint az összes szektort érinti valamilyen szinten a probléma, azonban leginkább a **kormányzati szolgáltatások**hoz kapcsolódó szektorok az elsődleges célpontok, ugyanis ellenük intéznek leginkább politikai okokból támadásokat.

Az ENISA jelentés főbb pontjai

- **Kidolgozásra került egy újszerű osztályozási rendszer** a DoS-támadások kategorizálására a támadásokról rendelkezésre álló információk és a célpontok alapján, mely így egy szisztematikusabb elemzési megközelítést tesz lehetővé.
  Az osztályozás részeként különös hangsúlyt érdemes fektetni a **támadások motivációjára és céljára**, ugyanis a támadások technikai fejlődésén túl érdemes ezeket is elemezni.

- A 2022 januári és 2023 augusztus közötti időszakban **összesen 310 DoS-incidens** került elemzésre. (Ez nem az összes incidens ebben az időszakban).
- A leginkább érintett ágazat a **közigazgatás** volt, mely a támadások **46%-át szenvedte el**.
- A támadások **66%-át politikai okok**ból követték el.
- Összességében az incidensek **50%-a az ukrán-orosz háborúhoz köthető**.
- A tanulmány szerint a támadások **56,8%-a okozott teljes fennakadást** a megtámadott szervezetnél.

*A tanulmány is definiálja a **DoS fogalmát**: ezek olyan támadások, amelyek során a támadók részben vagy egészben akadályozzák egy célpont jogos használatát a célpont szolgáltatásainak kimerítésével vagy kihasználásával egy bizonyos időn keresztül.*

TUDTAD?

DoS-támadások azonosításának nehézségei

A DoS-támadások ugyan már jól ismertek a nagyközönség és a szervezetek előtt is, azonban mégis kihívást jelent a támadást ténylegesen azonosítani, mérni és ezáltal jelenteni is.

Ennek több oka is van:

1. *A szervezetek **nem biztosak abban, hogy DoS-támadás érte őket**, vagy akár **abban sem, hogy szándékos támadásról van szó vagy csak valamilyen technikai probléma áll fenn**.*

2. *A támadások **mérete nehezen mérhető**, mivel ugyanazok a számítógépek, amelyek a mérést végzik, egyúttal a támadások célpontjai is lehetnek.*

3. *Nehéz felmérni, hogy **milyen pénzügyi hatása** van annak, hogy egyes ügyfelek számára lassúak a szolgáltatások, vagy ha egyes weboldalak nem működnek.*

4

*A támadások után **jellemzően nincsenek hátrahagyott kódok**,vagy bináris fájlok,amelyek segítenék a mélyebb elemzést, ugyanis az a kevés rendelkezésre álló adat,ami hátramarad, mint például IP címek, általában nem megbízhatóak.*

5

*Előfordul, hogy **az efféle támadásokat elterelésként használják** a támadók, akiknek nem egy szolgáltatás – például weboldal – elérhetetlenné tétele a fő célja, hanem jogosulatlan hozzáférés szerzése vagy valamilyen egyéb károkozás, ugyanis efféle túlterheléses támadássokkal el tudják fedni ezeket az akciókat.*

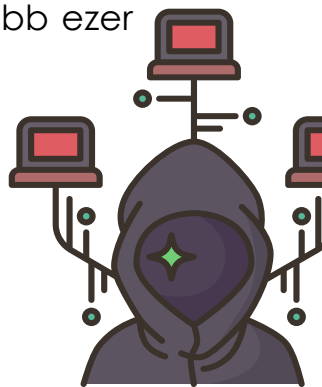
A fentiek miatt nincsenek hivatalos adatbázisok a megerősített DoS-támadásokról és azok jellemzőiről.

Maga a tanulmány is emiatt három fő nyilvános forrásra támaszkodik: a **hírmédiára**, az **ilyen jellegű támadásokat mérő szervezetekre** és a **támadók állításaira**. Összeségében elmondható, hogy kevés olyan nagyszabású hivatalos jelentés létezik, amely a DoS-eseményeket, azok motivációit és hatásait elemzi.

A tanulmány kitér arra is, hogy időként milyen egyéb nehézségekbe ütközik a támadás azonosítása. A leggyakoribb nehézségek a fent említetteken túl:

- A DoS-támadást **ellenőrző rendszerek vagy számítógépek maguk is a támadás célpontjának részei** lehetnek, így akadályozva van a forgalom figyelés, és támadás észlelés. A támadássok így kevés nyomot hagynak.
- A DoS-támadások **kezdeti időpontja nehezen megállapítható**, mivel rendszerint fokozatosan növekszik a forgalom melynek eredményeképp problémát jelenthet egyértelműen megállapítani, hogy az a bejövő támadásból származik-e.
- A támadások során **nehéz beazonosítani a támadás elejét és végét,** valamint **számszerűsíteni, hogy egy vagy több** támadásról van szó.
- Mivel a webes szolgáltatások gyakran megosztják az IP-címeket, **egy támadás több webhelyet is leállíthat**.
- A DoS-zavarok **tovább élhetnek, mint maga a támadás**, mivel a számítógépek vagy rendszerek leállhatnak, így a támadás időtartamát emiatt is nagyon nehéz megbecsülni.

A szolgáltatás megtagadással járó támadások elemzését az is nehezíti, hogy ezek a támadások különböznek más típusú kibertámadásoktól, mivel alapvetően hálózati alapú támadásról van szó, így nem maradnak hátra szoftveres „nyomok”, csak több ezer elemezhető, egymástól független hálózati csomag.



Az információforrások kategorizálása

Az információforrások minősége alapján három kategóriát állít fel a tanulmány. Meglepő módon kifejezetten...

Jó minőségű (good-quality information)

és megbízható adatokat szolgáltatnak maguknak a támadóknak a jelentései és nyilatkozatai. Értelemszerűen ezen információk megerősítésre szorulnak egyéb felhasználók, szervezetek vagy éppen a célpontok nyilatkozatai alapján. Maguk a támadók a különféle csoportok Telegram-csatornáin osztják meg ezeket a támadási

Rossz minőségű (bad-quality information)

adatok állnak csak rendelkezésre egyes esetekben: ezek a közepesen megbízható adatok általában olyan DoS-védelmi szolgáltatóktól származnak, amelyek támadásokat állítottak meg.

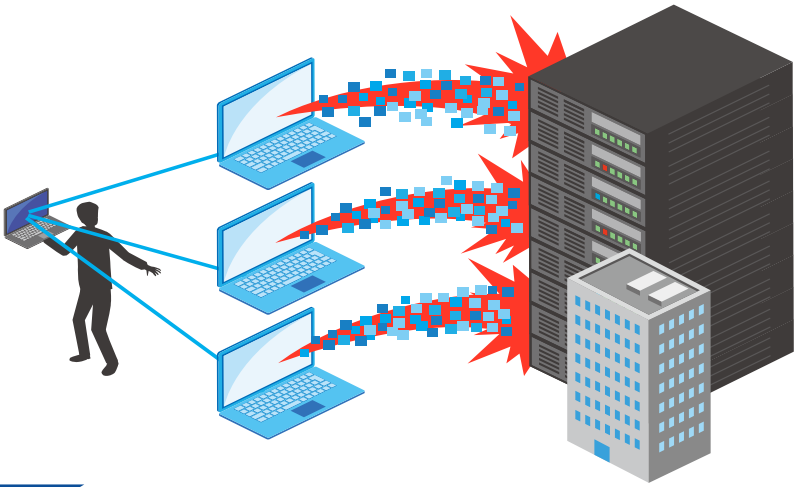
Ezek a jelentések magas szintű jelentésként hasznosak, de rossznak minősülnek, mivel nem használhatóak a célpontok vagy a motivációk értékelésére. Ezek a szolgáltatók általában több ezer ügyféllel rendelkeznek, így nehéz megérteni, hogy ki kit, miért és hol támadott meg. Ráadásul az esetek többségében szerződés köti a feleteket, ezáltal jogi okokból kifolyólag nem hozhatóak nyilvánosságra a célpontok nevei. Amennyiben a célpont nem erősíti meg a jelentést, a támadó pedig nem vállalja a felelősséget, akkor a szolgáltatók jelentései nehezen ellenőrizhetők.

Csúnya minőségű (ugly-quality information)

információk pedig azok, amelyek azon alacsony megbízhatóságú adatok, melyek a célpontok által készített jelentésekből származnak. Problémát jelent ezekkel az adatokkal kapcsolatban, hogy a harmadik fél megerősítése nélkül felhasználhatósága nem biztosított, mivel a célpont eltúlozhatja vagy elegendő bizonyíték nélkül egy fenyegető csoportnak tulajdoníthatja a támadást.

Az efféle jelentés megbízhatatlanságára jó példa, amikor a DoS támadások célpontjai a támadást lehetőségként használják fel népszerűségük növelésére *(„fontosak vagyunk, mert megtámadtak minket")* vagy hamisan állítják, hogy nagyobb hatást gyakorolt a támadás a valósnál, így jogi lépéseket tehetnek, vagy adott esetben mindenfajta bizonyíték nélkül állítják, hogy támadás érte őket, ezzel pedig igazolni tudják a jövőbeli lépéseiket.

A különböző megbízhatóságú jelentéstípusok legjobb kihasználása érdekében **alapos keresztellenőrzési és validálási folyamatokat vezettek be** annak biztosítására, hogy az incidensekkel kapcsolatos információk felhasználhatók legyenek.



ENISA elemzési módszertan

A jelentés a DoS-incidensek elemzésére összpontosít az ENISA Cybersecurity Threat Landscape módszertan alapján, amely 5 lépésből áll:

01

Nyílttforrású adatszerzés a különféle jelentett biztonsági incidensekre vonatkozóan. *A keresés minden régióra kiterjedt, és magában foglalta a média- és hírszervezetek, biztonsági cégek nyilatkozatait, a DoS-védelemre szakosodott cégek által bejelentett incidenseket, a megtámadott szervezetek nyilatkozatait.*

02

Manuálisan ellenőrizni szükséges az incidens idejét*, hogy a bejelentés tárgyát képezi-e a jelentésnek.*

03

A jelentés hatálya alá tartozó valamennyi incidens esetében ***további, harmadik féltől származó jelentések felkutatása****, amelyek megerősítik, hogy támadás történt.*

04

A támadást ***részletes elemzés alá vonják a jellemzőik alapján****: célpont neve, ágazata, országa, incidens kezdő időpontja, valamint a támadók motivációja, célja, támadás módszere vagy technikája. Továbbá a célpontról szóló információk: célzott szolgáltatás, erőforrás,*

05

A támadás egyénileg ***vizsgálatra kerül az adott társadalmi-politikai kontextusban****.*

Az elemzés alapvetően a sikeres DoS-támadásokra koncentrál, azonban magasfokú látencia jellemző, ugyanis számos kísérlet a hatékony védelmi mechanizmus miatt kudarcot vallott. Ugyanakkor az elemzés során ezek a sikertelen, de jól azonosított támadások is felhasználhatók, köszönhetően a kifejezetten DoS-védelemre szakosodott vállalatoknak.

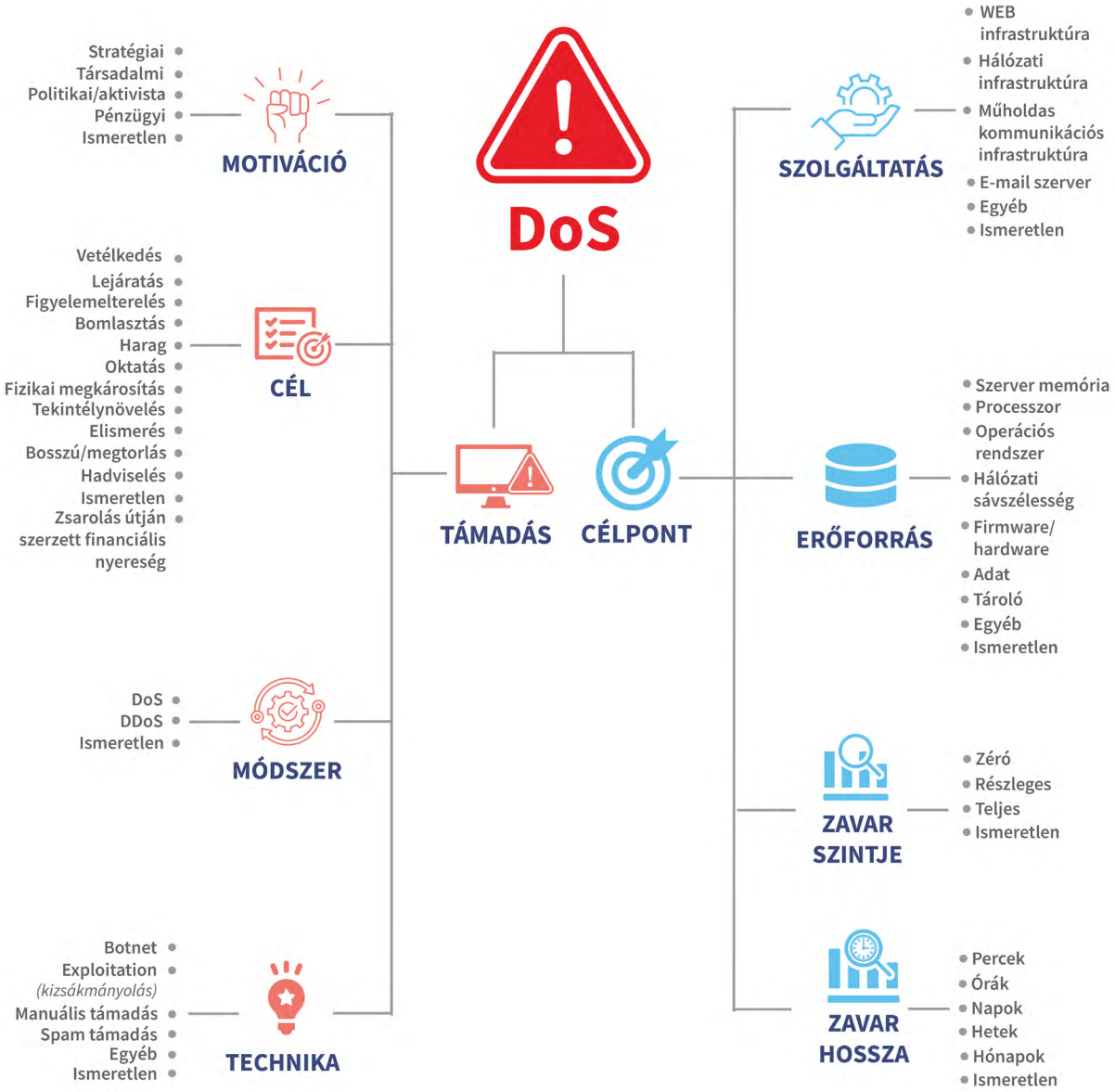
A DoS-támadások besorolásai

Az ilyen jellegű támadások kategorizálására több osztályozásos módszertan létezett eddig is, azonban ezek mind a támadás technikai jellemzőire, illetve a lehetséges védekezési módokra támaszkodott. Ezek alapján eddig 3 gyakori típus volt: **volumetrikus támadás** (bit per másodpercenként), **protokolltámadások** (másodpercenkénti csomagokban mérve) és **alkalmazási rétegbeli támadások** (másodpercenkénti kérésekben mérve).

A forrás ENISA jelentés egy újabb megközelítést alkalmaz, ami motivációra és a célpontra támaszkodik, ugyanis ezek a paraméterek szinte minden DoS-támadást jellemeznek. Az új osztályozási módszertan előnye, hogy fokozza a stratégiai hírszerzést, segíti a fenyegetések jobb megértését és segíthet megtervezni a lehetséges ellenintézkedéseket. Ezen felül a témában egyfajta szabványosítás a cél, ezáltal elősegítve az együttműködést és a kommunikációt, mivel ez a megoldás egy közös nyelvet kínál a vonatkozó megoldások megvitatásához és egyúttal meghatározza a fejlesztendő területeket is.

A támadások osztályozási sémája

Az új osztályozási rendszer szerint két fő kiindulópont van: a támadásra és a célpontra vonatkozó információk. Mindkét kategória további 4-4 pontra osztható, mely szerint a támadás **motiváció, cél, módszerek** és **technikák** alpontból áll, míg a célpontra vonatkozó információk a **szolgáltatás, erőforrás, zavar szintjére** és **zavar hosszára** oszthatóak. Ezt a 4-4 elemet tovább bővíthetjük. A fentieket az alábbi ábra szemlélteti:



1. ábra

A DoS-támadások osztályozási sémája

Kiemelkedő incidensek

Az ENISA tanulmány öt konkrét incidenst emel ki a vizsgált időszakból és osztályoz az új ENISA módszertan alapján, melyből jelen tanulmány is bemutat kettőt. Bár a legtöbb információ angol nyelven áll rendelkezésre, számos más nyelvű incidenst lefordítottak angolra az elemzéshez.

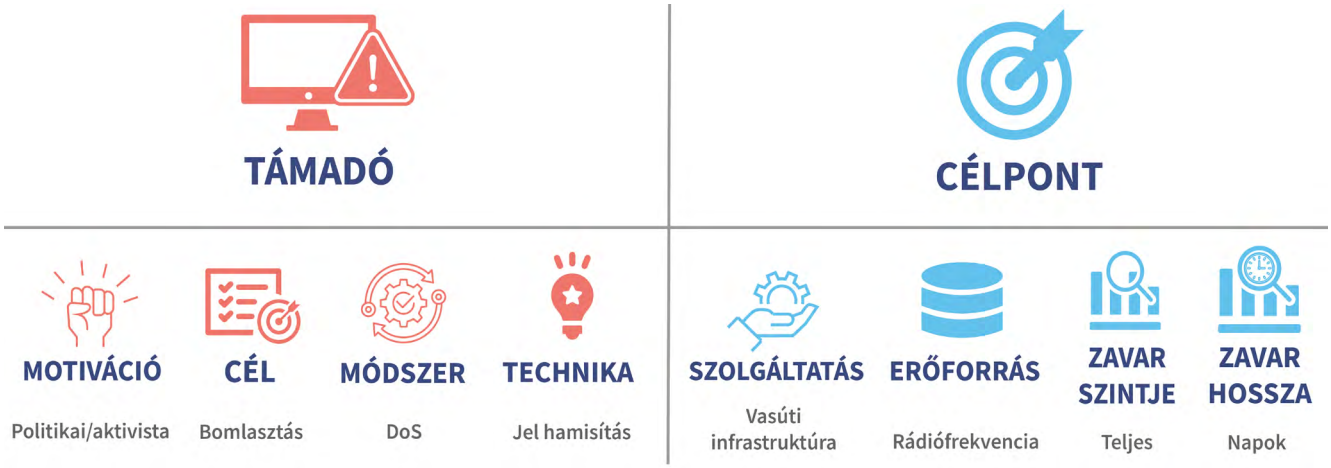
A lengyel vasúti rendszer elleni támadás

2023. augusztus 25-én Lengyelországban leállt a teljes vasúti közlekedés, ugyanis a vasúti hálózat által használt vészleállító rendszer általhasznált rádiójelek nem voltak megfelelően titkosítva, így ***két lengye hacker olyan hamis rádiójelet tudott küldeni, amit éles vészjelzésként észleltek a vonatok.*** *Ez egy a vonatok vészleállító mechanizmusa elleni DoS-támadásként értékelhető.*

Ez a támadás azért emelendő ki a többi közül, mert ez **kritikus infrastruktúra ellen irányult**, nem "csak" egy webes infrastruktúra ellen. Amikor aktív katonai konfliktus van a háttérben, akkor gyakran megfigyelhető ez a tendencia.

A támadás mögött egyértelműen politikai motiváció volt, mert a lengyel vasút stratégiai jelentőségűvé vált a Nyugat-Ukrajna támogatása szempontjából az orosz invázióval szemben.

Az incidensről készült elemzést az alábbi ábra szemlélteti:



2. ábra

A lengyel vasúti rendszer elleni DoS-támadás elemzése az új osztályozási rendszer alapján

Kórházak elleni támadás az Egyesült Államokban

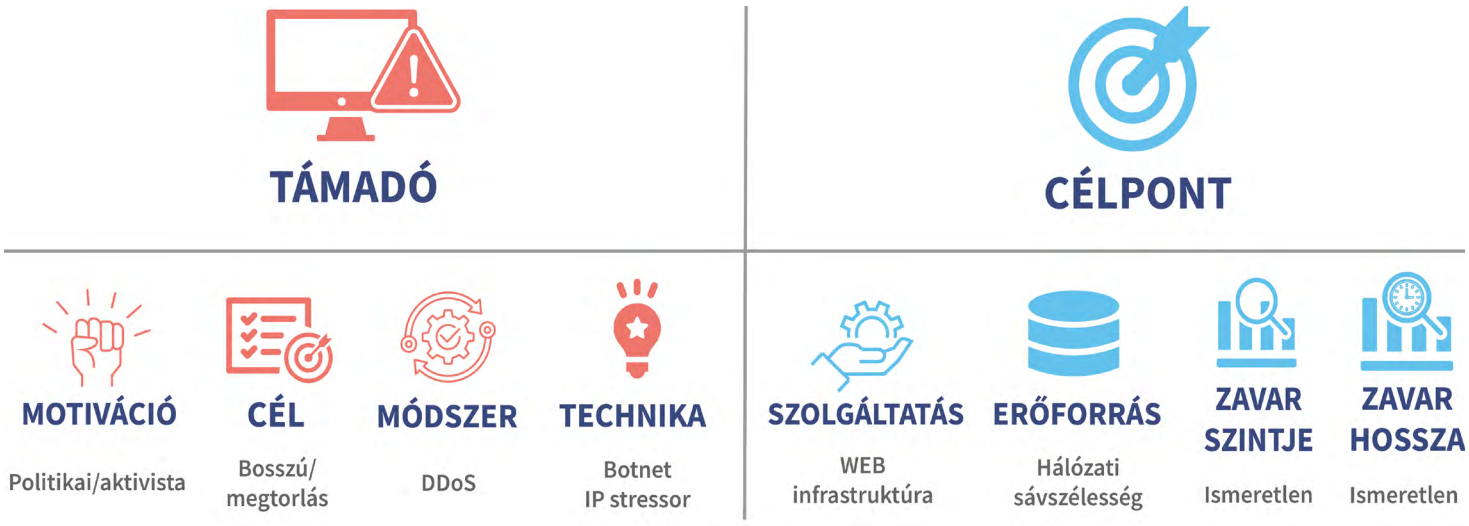
*2023. január 30-án egy Oroszországhoz köthető csoport **DDoS-támadást indított az Egyesült Államokban található kórházak ellen**. Az összehangolt támadás több mint egy tucat kórház webes infrastruktúráját célozta meg. A csoport bejelentette a támadást és azt állította Telegrammon, hogy a támadást megtorlás céljából követték el, mert az Egysült Államok támogatást nyújtott Ukrajnának az Oroszország inváziója követően.*

A támadás jól mutatja, hogy milyen kockázatot rejtenek ezek a támadások az egészségügyi rendszert illetően, még akkor is, ha nehéz pontosan meghatározni azt, hogy milyen konkrét kárt okozott az ellátásba a támadás.

Jól szemlélteti a támadások veszélyességét az, hogy nincsenek tekintettel a Genfi Egyezményre sem, holott az rendelkezést tartalmaz a háborús időszakban az egészségügyi intézmények ellen elkövetett támadások vonatkozásában is.

Az ENISA módszertan alapján az alábbi módon lehet osztályozni a támadást: **motivációja politikai/aktivista**, a **célja bosszú**, a módszer DDoS, a technika pedig botnet és IP-stresszorok. A célzott szolgáltatás webes infrastruktúra volt, az erőforrás hálózati sávszélesség volt, a zavar szintje és hossza pedig ismeretlen.

Az incidensről készült elemzést az alábbi ábra szemlélteti:



3. ábra
A kórházak elleni támadások (az Egyesült Államokban) elemzése az új osztályozási rendszer alapján

Az incidensek globális elemzése

Az incidensek száma és a mintavétel

Az ENISA jelentés kihangsúlyozza, hogy a tanulmányban szereplő mintavételi módszer az incidensek kiválasztására elfogult, mivel számos olyan incidenst hagy ki, amelyet nehéz volt nyomon követni vagy semmilyen formában nem került be a hírekbe. A DoS-támadások tényleges mérésének nehézségét növeli, hogy a védelmet nyújtó szervezetek gyakran számolnak be arról, hogy naponta több ezer DDoS-támadást blokkolnak, ugyanakkor ezekről a támadásokról a negyedéves mérési dokumentumokon kívül többnyire nem számolnak be, és nem adnak konkrét részleteket a támadások jellegéről, illetve arról, hogy az ő szempontjukból mi számít támadásnak.

Ezért az ENISA jelentés eredményeit leginkább **iránymutatásnak kell tekinteni**, **nem** pedig **a támadások teljes számának pontos ábrázolásának**. Az osztályozási módszertant kizárólag erre a tanulmányra szabták, hogy segítse az elemzést.

Célzott ágazatok

Általánosságban elmondható, hogy **egyetlen iparág sem immunis** a DoS-támadásokkal szemben. A globális elemzés rávilágított, hogy a támadások **46%-a a közigazgatási ágazat**ot célozza, de jelentős számú támadásnak van kitéve a **közlekedési**, a **média szórakoztatás**i, valamint a **digitális-infrastruktúra** ágazat is. A megfigyelt incidensek száma alapján a nyolc leginkább érintett ágazatot az alábbi ábra szemlélteti:

4. ábra

A top 10 érintett szektor a 2022 január és 2023 augusztusa között bekövezett incidensek száma alapján

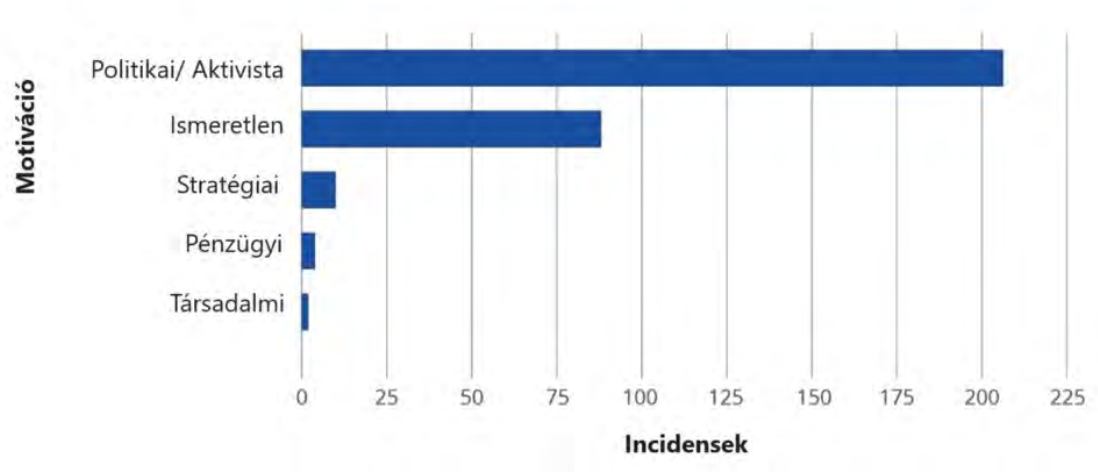
A közigazgatási ágazatot célzó támadások drasztikus emelkedésének oka főként az, hogy a folyamatban lévő – orosz-ukrán – háborús konfliktushoz kapcsolódóan **számos megtorló akciót indítottak** a támogatásukat kifejező országok kormányzati intézményei ellen. Az online média elleni támadások jelentős része szintén a fennálló háborús konfliktusra vezethető vissza, hiszen háborús időszakban elementáris fontosságú a média ellenőrzés alá vonása.

Motivációk és célok

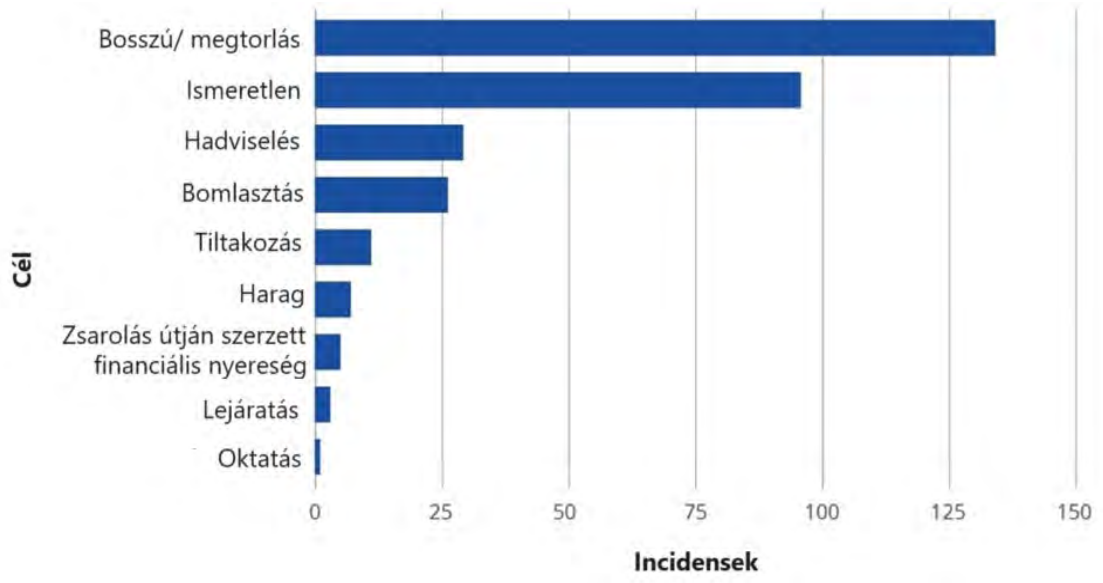
A motiváció szempontjából megállapítható, hogy a megfigyelt incidensek **66%-át a politikai vagy aktivista célokból** követték el. Meglepő módon csupán **5%-ban volt azonosítható a stratégiai és pénzügyi cél,** ugyanakkor az esetek **28%-ában támadás motivációja ismeretlen** maradt.

Fontos megjegyezni, hogy a fent ismertetett módszertan okán sok incidens marad látenciában, mert egyes célpontok annyira „kicsik" piaci szempontból, hogy a média nem tesz róluk említést. Megfigyelhető, hogy **a támadások célja 43%-ban megtorlás** volt. Erre jó példák az orosz-ukrán háború kapcsán elszaporodó oroszbarát hacktivista támadások.

A motivációk és a célok számadatait az alábbi grafikonok szemléltetik:



5. ábra:
A támadók motivációjának eloszlása a 2022 január és 2023 augusztusa között bekövezett incidensek száma alapján



6. ábra
A támadók célpontjainak eloszlása a 2022 január és 2023 augusztusa között bekövezett incidensek száma alapján

Hogyan mérhető a DoS-támadás hatása?

Egy ilyen típusú támadás valódi hatása számtalan tényezőtől függ, és hatást nem könnyű számszerűsíteni. Ugyanakkor meg kell próbálni meghatározni, hogy milyen paraméterek alapján lehet mérni egy támadást. Miután leggyakoribb hatások a **leállási idő** és a **nyilvánosság**, így érdemes a fókuszt ezekre a mérőszámokra helyezni.

A leállási idő a célszolgáltatás tényleges, valós elérhetetlenségére utal a támadás következtében, mely minél hosszabb, annál súlyosabb a támadás. A nyilvánosság a támadás által a médiában keltett figyelem mértékére vonatkozik. Minél nagyobb a támadás médiavisszhangja, annál nagyobb a lehetséges hatása a hírnévre. Ez a támadók gyakran igen fontos motivációja.

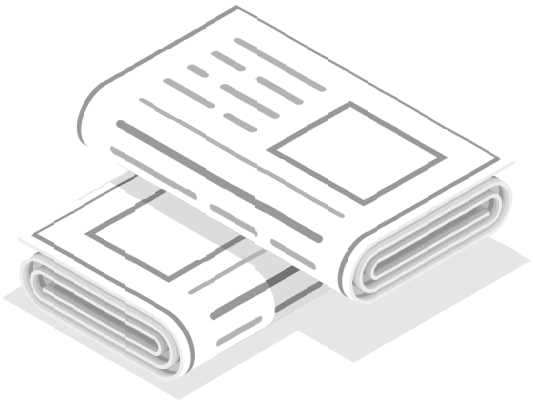
A fentiek **egyik ritkán tárgyalt melléktermék a FUD**, amely szintén a támadás hatásának mérésére szolgál. A FUD angol mozaikszó a **fear (félelem)**, **uncertainty (bizonytalanság)** és a **doubt (kétség)** szavakból áll össze, amely tulajdonképpen a támadásnak a lakosságra gyakorolt pszichológiai hatására utal.

A DoS-támadásoknak természetéből fakad, hogy FUD-ot generálnak, mivel a támadások kiszámíthatatlanok és a célpontra gyakorolt hatásuk gyakran ismeretlen.
A valóban hatásos támadások melléktermékként FUD-ot generálnak. Értelemszerűen a nyilvánosság és a leállási idő együttes szintje befolyásolja a támadás által generált FUD szintjét.

DoS-támadások a fegyveres konfliktusok során

Általánosságban elmondható, hogy a nagyobb fegyveres konfliktusok az ilyen jellegű támadások újabb hullámainak **legjelentősebb kiváltó okai**, melyre jó példa az Ukrajna elleni orosz agressziós háború, valamint az izraeli-palesztin konfliktus. A támadások többsége katonai célpontok ellen irányul, többnyire egy stratégia részeként. Emellett a DoS-t a háborúban részt vevő felek el nem ismert támogatói is felhasználhatják az ellenség támogatói elleni megtorlás vagy bosszú eszközeként.

A támadások általában a média figyelmét kívánják felkelteni, ezért ismert szolgáltatásokat és weboldalakat céloznak. A fentieket támasztja alá, hogy több jelentés is beszámolt a DoS-támadások számának növekedéséről az Ukrajna elleni orosz offenzíva kezdete után, valamint több újonnan alkalmazott technikáról tesz említést. Az azonosított új technikák között szerepelnek a különböző felhőszolgáltatók segítségével végrehajtott egyidejű, valamint a Tor használatával elkövetett támadások.



A háborús összefüggéseket jól mutatja egy adatforgalomról szóló jelentés, mely szerint az orosz-ukrán háború első hónapjában az **.ua** domainekre irányuló teljes internetes forgalom több mint 80%-át tette ki a DDoS-támadások forgalma 2022. március elején, mely később fokozatosan csökkent. Összeségében 2022 első negyedévében **a forgalom 12,6%-a DDoS tevékenyég** volt.

Ajánlások megelőzésre és helyreállításra

A tanulmány jól mutatja, hogy a DoS-támadások világszerte elterjedtek és egyetlen szervezet sem tud mentesülni az alól, hogy potenciális célponttá váljon. A fenyegetés jellege egyértelművé teszi, hogy nem lehet könnyen megjósolni, hogyan válnak a szervezetek célponttá, tekintve, hogy a támadások különféle tényezőkben gyökerezhetnek, kezdve a személyes sérelmektől egészen a hadviselésig. A tanulmányban szereplő ajánlás két kategóriára osztható: **megelőzésre** és **helyreállításra**.

A megelőzés szempontjából a tanulmány – a korábbi módszereken túl - legjobb eszközként kiemeli a prevenciót: **szükséges készíteni egy fenyegetettségmodellt**. Fel kell mérni a lehetséges kockázatokat, az adott szervezet és infrastruktúra sebezhetőségét. A felmérés egyik legfontosabb pontja, hogy azonosítsuk be a szervezet „értékét" mint lehetséges célpont. Jellemzően a legértékesebb célpontok a kritikus infrastruktúrák és a kormányzati ügynökségek.

A DoS-támadások elleni legelterjedtebb védelem a **CDN** (Content Delivery Networks – tartalom szállító hálózat), az **internetszolgáltató által nyújtott védelmi megoldások** (upstream internet service provider protection), a **felhőszolgáltatók DoS-védelmi megoldásai** és a **helyi telepítésű/ üzemeltetésű megoldások** (on-premise solution) alkalmazása. Ezek a különféle megoldások különféle előnyökkel és hátrányokkal bírnak, így maguknak a szervezeteknek kell eldönteniük, hogy melyik a legoptimálisabb a szervezetük szempontjából.

A tanulmány felhívja a figyelmet arra is, hogy egy DoS-támadás kockázata nem csökkenthető a nullára, emiatt fontos egy **„helyreállítási terv”** elkészítése, amely többek között tartalmazza a lehetséges védelmi intézkedés működésének ellenőrzését, a védelmét ellátó szervértesítésének rendjét, a partner szervezetek értesítésének rendjét a szolgáltatás leállásáról, valamint az esetleges sajtónyilatkozatra vonatkozó protokollt.

Mindemellett a támadás bejelentése a megfelelő hatóságoknál kiemelt fontosságú.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2024