CTI jelentés

Éves kiberbiztonsági jelentés

Az ENISA Threat Landscape 2023 című tanulmánya nyomán

1996

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

Fortes fortuna adiuvat

NEMZETI KIBERVÉDELMI INTÉZET

enisa

Tartalomjegyzék

Az ENISA az Európai Unió Kiberbiztonsági Ügynökségét jelenti, melyet 2004-ben alapítottak az unió kiberbiztonságának egységes, magas szintű biztosításának érdekében.

Bevezetés

Az **Európai Unió Kiberbiztonsági Ügynöksége** (European Union Agency for Cybersecurity - ENISA) minden évben kiadja az ENISA Threat Landscape című éves jelentését, hogy átfogó képet adjon az elmúlt év kiberfenyegetettségi helyzetéről. A jelentés tartalmazza a legjelentősebb fenyegetettségeket, a fennálló trendeket, a fenyegetettségi szereplőket, támadási technikákat, valamint támadási hatás- illetve motivációelemzést.

A **Nemzeti Kibervédelmi Intézet** jelen CTI jelentése a fenti 2023-as évben, immár tizenegyedik alkalommal, 2023 október 19. napon online publikált ENISA kiadvány feldolgozása nyomán készült, annak legelementárisabb részeit emeli ki.

Áttekintés

A kiadvány a 2022-es év második és a 2023-as év első felét értékeli, melynek kapcsán kiemeli, hogy a kiberbiztonsági szektor mind mennyiségi, mind minőségi szempontból növekedést tapasztalt a kibertámadások vonatkozásában, mely főként a jelenleg is fennálló orosz-ukrán háború kapcsán egyre aktívabbak oroszbarát hacktivistáknak róható fel.

A jelentés legfontosabb megállapításai az alábbiak:

- Egyre inkább megfigyelhető **a kiberbűnözők professzionalizálódása**, egyre újabb taktikákat és módszereket alkalmaznak, hogy beszivárogjanak egyes környezetekbe, vagy az áldozatok nyomás alá helyezése és zsarolása érdekében.

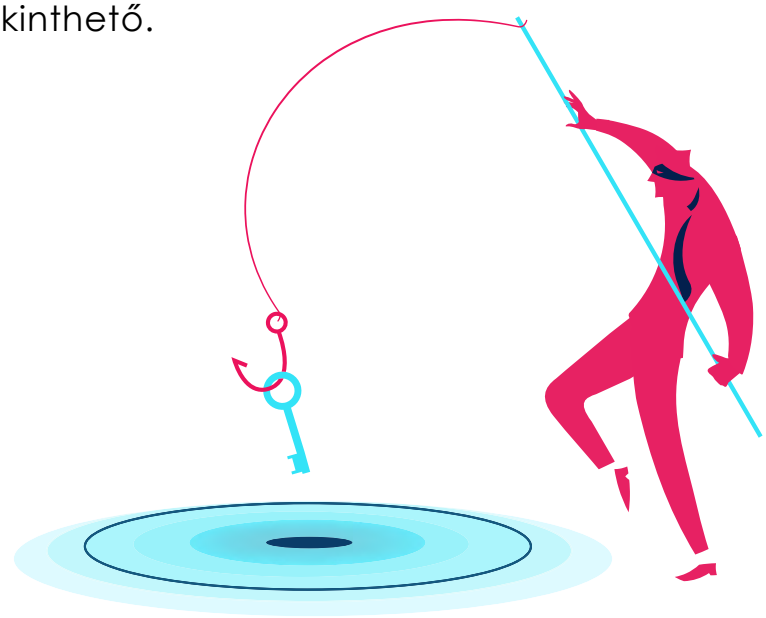
- Jelenleg is **elsődleges célpontnak számít - 19% - a közigazgatási szektor**, őket követik a célzott egyéni célpontok elleni támadások – 11% -, de jelentősek az egészségügyi szektorral, a digitális infrastruktúrával, termelési szektorral, pénzügyi és közlekedési szektorral szembeni támadások is.

- Az **információ manipuláció** kulcsfontosságú eleme volt Oroszország Ukrajna elleni háborújának.

- A kiberbűnözők egyre inkább **a felhő alapú infrastruktúrákat veszik célba**, valamint egyre jobban megfigyelhető a **geopolitikai motiváció**. A támadások agresszivitását mutatja, hogy a zsarolások már nem csupán ransomware-ek útján történnek, hanem jellemzően egyes felhasználókat vesznek célba.

- Ahogy várható volt, 2023-ban **a social engineering támadások során is megjelent az AI felhasználása.**

- Az **adathalász tevékenység továbbra is a legfontosabb** támadási vektornak tekinthető.



Elsődleges fenyegetések

Az ENISA Threat Landscape 2023 jelentés nyolc elsődleges fenyegetettségi csoportot emel ki, melynek oka, hogy tapasztalat szerint ezeknek volt a legnagyobb jelentőségük, széleskörű előfordulásuk és a hatásuk.

A nyolc csoportot az alábbi ábra szemlélteti:

1. ábra

Elsődleges fenyegetések

Az egyes csoportok kapcsán a CTI jelentés a továbbiakban részletesebb megállapításokat tesz.

Fenyegetettségi trendek

A fejezet összefoglalja a vizsgált időszak alatt bekövetkező kiberfenyegetések terén megfigyelt főbb tendenciákat:

A jelentési időszakban a **zsarolóvírusok álltak az elsődleges helyen** a fenyegetettségek tekintetében.

Megfigyelhető, hogy **gyakran használnak fel legális eszközöket** különféle kiberkémkedési műveletek elfedésére. A legális szoftverek felhasználásával hosszabb ideig elkerülhető a felderítés, mivel nehezebb azokat azonosítani, valamint nem keltenek gyanút.

A **geopolitika** továbbra is nagy hatással van a kiberműveletekre.

A kiberbűnözői csoportok egyre inkább **jól kidolgozott „as-a-Service" programokat használnak**, ezáltal sokkal hatékonyabban tudnak nyomást gyakorolni az áldozatokra.

A támadásokkal párhuzamosan **egyre nő a rendvédelmi szervek aktivitása is**, így például sikeresen felszámolták a Hive zsarolóvírust üzemeltető csoportot.

A jelenleg még mindig leghangsúlyosabb malware az információ lopásra felhasznált **Agent Tesla, Redline Stealer és a FormoBook**.

Ugyan folyamatosan csökken a „klasszikus" mobil kártevők száma, azonban **az adware-ek és a kémprogramok száma továbbra is jelentős**.

A social engineering támadásokra egyre inkább jellemző, hogy **az áldozatokat a fizikai világban tévesztik meg.**

Az anyagi haszonszerzésnek továbbra is az **egyik legkedveltebb módszere az üzleti e-mailek kompromittálása** (business e-mail compromise - BEC).

10

A kiberbiztonsági fenyegetettségekre **hatással vannak az AI chatbotok**.

11

A **DDoS támadások egyre nagyobbak és összetettebbek**, jellemzően most már a mobilhálózatok és az IoT felé mozdulnak el.

12

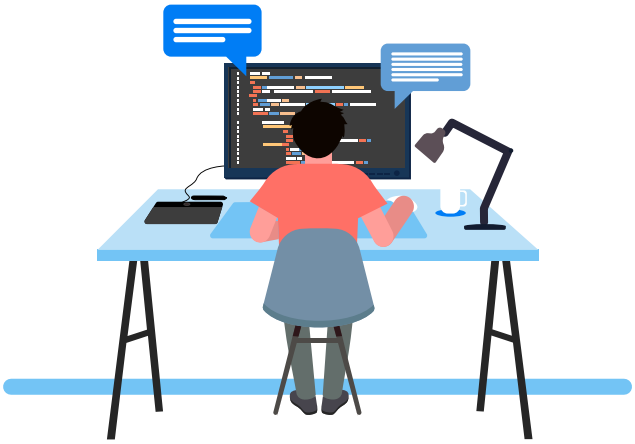
A "**Cheap fakes**" és az **információk AI-val történő manipulálása** továbbra is aggodalomra ad okot.

13

A fenyegető csoportok **növekvő érdeklődést tanúsítanak az ellátási láncokat érintő támadások iránt is**. Ezen támadások során főként a magasabb jogosultságokkal rendelkező alkalmazottakat veszik célba, például fejlesztőket és a rendszergazdákat.

Új fenyegetettségi trendek a kiberbűnözésben

Az elemzés kitér rá, hogy kiberbűnözők előszeretettel használnak programjaikhoz relatíve ritkábban használt programozási nyelveket, mint a Rust vagy a GO. Ezzel egyrészt nehezítik az elemezhetőséget, másrészt hasznos a támadók szempontjából az is, hogy a GO nyelven íródott forráskód fordítást követően aránylag nagyobb méretű fájlokat eredményez, amit a malware scannerek többsége figyelmen kívül hagy, mivel azok rendszerint kisebb fájlokra lettek optimalizálva.



A nagyobb méret oka, hogy a Go könyvtárak statikusan linkeltek, ami azt jelenti, hogy az összes szükséges könyvtárat, függőséget tartalmazza a lefordított bináris állomány. Gyakorlatban például a klasszikus „Hello World!" program bináris fájljának mérete – Linux alatt - GO nyelven kb. 2-3 MB, ugyanez Rust nyelven kb. 300-500 KB, míg a dinamikus linkelést használó – vagyis ahol a futtatási időben szükséges könyvtárak külön vannak tárolva - C és C++ nyelvek esetében csak kb. 20-30 KB méretűek.

Továbbra is **jelentős a felhőinfrastruktúra szerepe** a kiberbűnözés tekintetében, mivel többnyire maga az infrastruktúra is részét képezi a social engineer kampányoknak is, például phishing e-mailek terjesztéséhez használják fel a fájlmegosztó szolgáltatást.

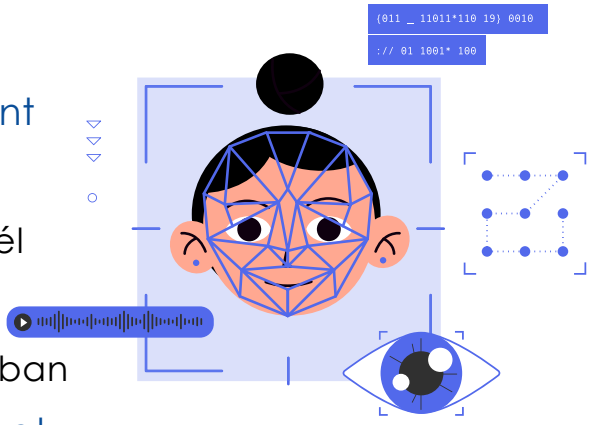
Ezen kívül a kiberbűnözők előszeretettel fordulnak az áldozatok felhő-infrastruktúrájához abból a célból, hogy kárt okozzanak, elsősorban a felhő hibás konfigurációjával visszaélve.

Az új technikák mellett ugyanakkor még mindig jelentős számban vannak jelen a régi technikák is, mint a **keresőoptimalizálás mérgezése**, valamint a **rosszindulatú reklámok (malvertising)**.

Az **FBI is figyelmeztetést adott ki**, hogy a bűnözők keresőmotor-hirdetési szolgáltatásokat használnak arra, hogy márkának adják ki magukat, és a felhasználókat adathalász vagy ransomware-eket tartalmazó oldalakra irányítsák.

A módszer lényege, hogy a kiberbűnözők olyan hirdetéseket vásárolnak, amelyek az internetes keresési találatokban jelennek meg egy olyan domain-nel, amely egy tényleges vállalkozáshoz vagy szolgáltatáshoz hasonlít. Amikor a felhasználó rákeres az adott vállalkozás nevére, ezek a hirdetések a keresési találatok legelején jelennek meg, miközben a hirdetés és a keresési eredmény között minimális a különbség. Ezek a hirdetések egy olyan weboldalra mutatnak, amely **azonosnak tűnik** a megszemélyesített vállalkozás hivatalos weboldalával, ugyanakkor **a valóságban kártékony kódot tartalmazó oldal**ra irányítják a felhasználót.

Ezen kívül továbbra is „népszerű" – bár már nem újkeletű – technika a **cryptojacking**.



Az elemzés általánosságban felhívja rá a figyelmet, hogy ugyan valóban megjelent a deepfake és az AI a kiberbűnözők eszköztárában, amikkel minden eddiginél kifinomultabb social engeneering támadásokat tudnak végrehajtani, azonban még többségében a régebbi technikákat használják.

Ennek oka, hogy a régi technikák sokkal kevesebb erőfeszítést igényelnek, de még mindig komoly haszonnal kecsegtetnek. A kémprogram-iparág jelenleg is virágzik, emiatt egyre nagyobbak az aggodalmak a magánélet védelmével kapcsolatban.

A jövőben várható, hogy bővülnek a CaaS-piacok (*Crime-as-a-Service*), vagyis a különféle kibertámadások, illetve azok „tervrajzai" gyakorlatilag szolgáltatásként bárki által megvásárolhatóvá válnak.

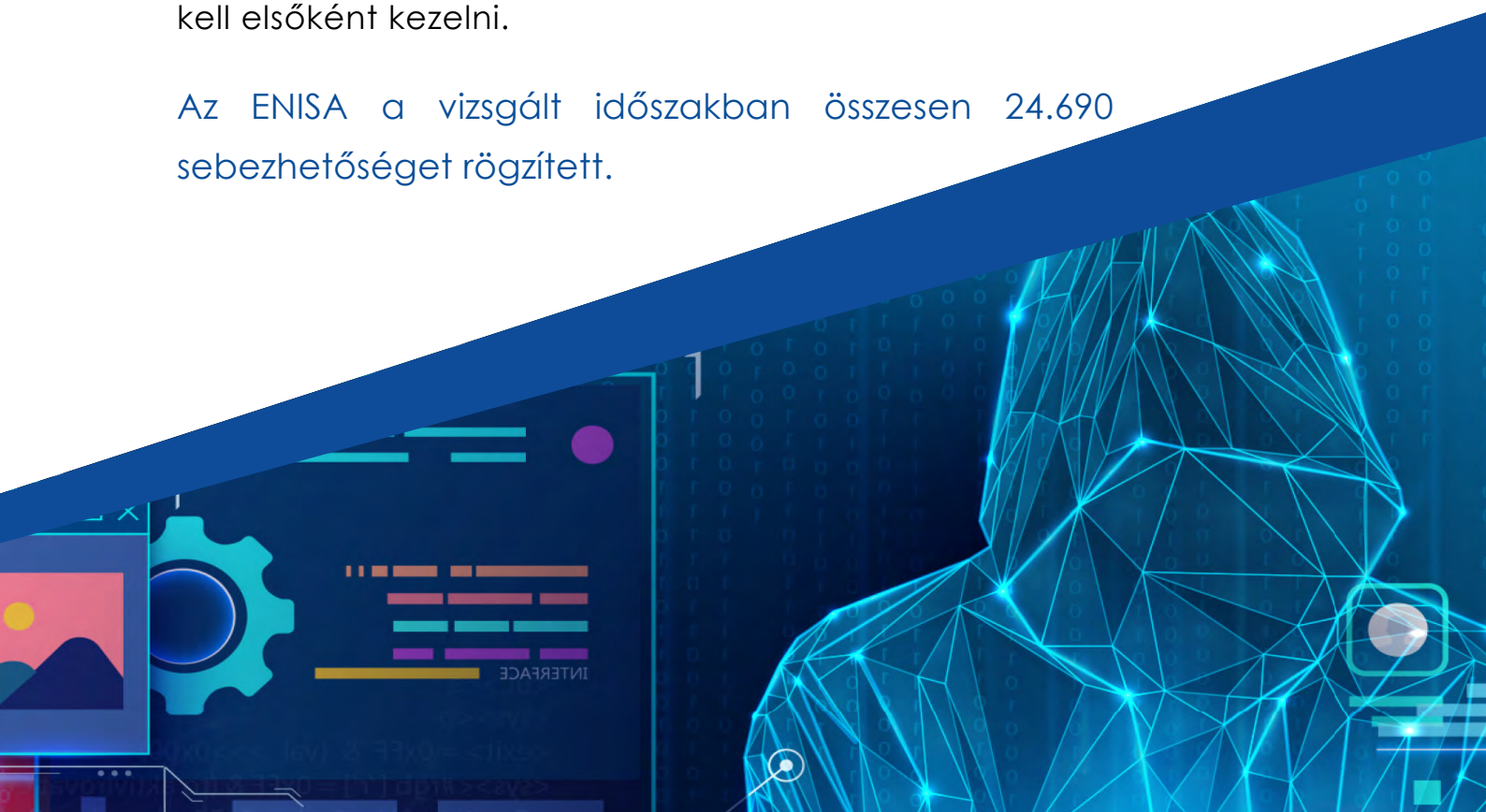
Az orosz-ukrán háború kapcsán láthatóan fokozódnak az oroszbarát hacktivista tevékenységek. A NoName057 nevű csoport egyenesen toborzási tevékenységet végez, melynek keretében olyan programok letöltésére buzdítják az embereket, melyekkel laikusok is könnyedén indíthatnak túlterheléses támadásokat.

A sérülékenységek elemzése (2022-2023)

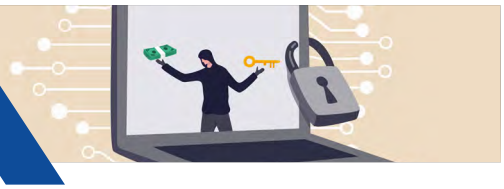
A kiadvány bemutatja – a kiberbiztonság területén már jól ismert – **CVE** (*Common Vulnerablities and Exposures)* szabványosított rendszert, amit a **különböző szoftver- és hardvertermékek biztonsági réseinek azonosítására és megnevezésére terveztek**. A rendszer minden egyes sebezhetőséghez egyedi azonosítót rendel, ami megkönnyíti a nyomon követésüket és a rájuk történő hivatkozást a különböző rendszerekben és adatbázisokban.

A **CVSS** (*Common Vulnerability Scoring System*) a **biztonsági sebezhetőségek súlyosságának értékelésre használt keretrendszer**. Előnye, hogy pontszámok alapján megadja a sebezhetőség hatását és kihasználhatóságát, ezzel pedig segíti a szervezeteket annak rangsorolásában, hogy mely sebezhetőséget kell elsőként kezelni.

Az ENISA a vizsgált időszakban összesen 24.690 sebezhetőséget rögzített.



Zsarolóvírusok



A tanulmány kiemeli a kibertámadások közül a zsarolóvírusokat. Korábbihoz képest újabb definíció nem került meghatározásra. A vizsgált időszakban jelentős növekedés volt tapasztalható a zsarolóvírusokkal kapcsolatos incidensekben, mely támadások főként az Európai Unió országaira összpontosítottak.

*A **zsarolóvírusok** meghatározása: a támadások olyan típusa, amelyben a fenyegető szereplők átveszik az ellenőrzést a célpont eszközei felett, és váltságdíjat követelnek az eszközök rendelkezésre állásának visszaállításáért cserébe.*

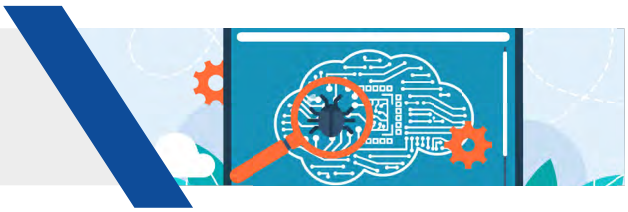
TUDTAD?

A tanulmány kutatásai alapján a vizsgált időszakban a **20 leggyakrabban előforduló zsarolóvírus csoport** a következő: 8base, Akira, BianLian, Black Basta, BlackByte, BlackCat (más néven ALPHV), CL0P, Hive, Karakurt, LockBit 3.0, LV, Mallox, Medusa, nokoyawa, PLAY, qilin, Ragnar Locker, RansomHouse, Royal, Snatch, STORMOUS valamint a Vice Society.

Tendencia továbbá, hogy 2022-ben 40%-ot csökkentek a korábbihoz képest a ransomware-es támadásokból származó bevételek (765 millió dollár helyett 456 millió dollár), ami azonban nem az incidensek számának csökkenésének, hanem az áldozatok fizetési hajlandóságának drasztikus csökkenésének tudható be.

A támadások tendenciája az adatlopások irányába mutat a titkosításos zsarolások helyett.

Malware



A malware egy átfogó kifejezés, amelyet minden olyan szoftver vagy firmware leírására használnak, amelynek célja olyan jogosulatlan folyamat végrehajtása, amely káros hatással van a rendszer titkosságára, integritására és rendelkezésre állására (pl. vírusok, férgek, trójai vírusok stb.).

Ezek a malware-ek lehetnek saját fejlesztésűek, de mint szolgáltatás is – *Malware-as-a-Service* – megvásárolhatóvá váltak. Mivel egyes esetekben kifejezetten olcsó szolgáltatásról van szó, a MaaS modell gyakorlatilag egy önálló előfizetéses üzletággá kezd válni.

Malware témában kiemelésre került, hogy az információ lopó programok közül a vizsgált időszakban az AgentTesla, a FormBook és a RedLine bizonyult a legelterjedtebbnek. A klasszikus mobil kártevők (pl: banki trójaiak) visszaszorulóban vannak, azonban a reklámszoftverek jelenleg is nagyon elterjedtek.

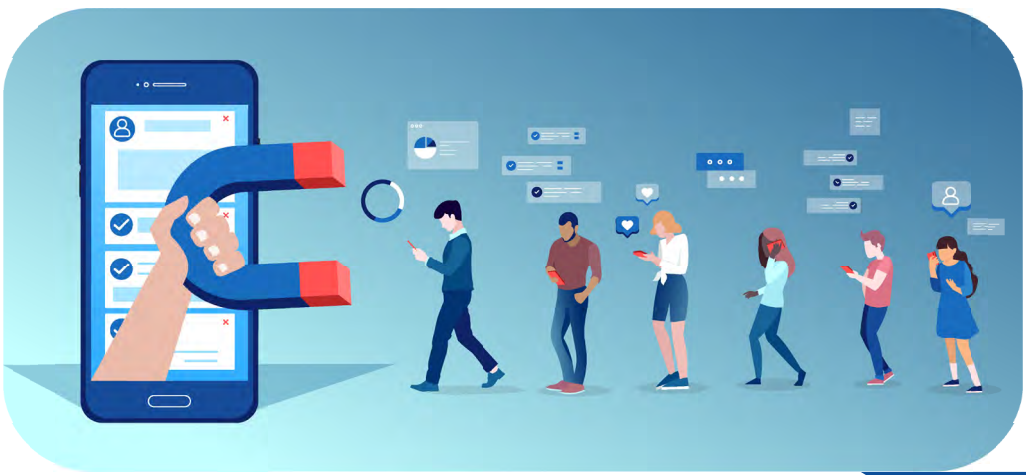
Kiemelték továbbá, hogy a kattintásmentes kémprogramokkal való visszaélés egyre inkább növekszik. Fokozott kockázattal bírnak a kínai gyártmányú Android operációs rendszerrel ellátott okostelefonok is, mivel azokon olyan előre telepített szoftverek találhatóak meg, amelyek túlzott hozzáférési jogosultságokat adnak a harmadik féltől származó alkalmazásoknak. Ennek eredményeképpen olyan adatok is továbbításra kerülnek értesítés nélkül, mint a geolokáció, profil vagy kapcsolati adatok.

Social Engineering

A social engineering olyan tevékenységek széles körét foglalja magában, amelyek az emberi hibát vagy emberi viselkedést próbálják kihasználni azzal a céllal, hogy hozzáférjenek információkhoz vagy szolgáltatásokhoz. A manipuláció legkülönbözőbb formáit használja arra, hogy az áldozatokat hibákra kényszerítse, illetve érzékeny vagy titkos információk átadására csábítsa.

A felhasználókat dokumentumok, fájlok, vagy e-mailek megnyitására, weboldalak meglátogatására, illetve rendszerekhez vagy előfordulhat az is, hogy szolgáltatásokhoz való hozzáférés engedélyezésére próbálja rávenni. Bár a módszer alapvetően a technológián alapszik, mégis a sikerének az **emberi tényező** a kulcsa.

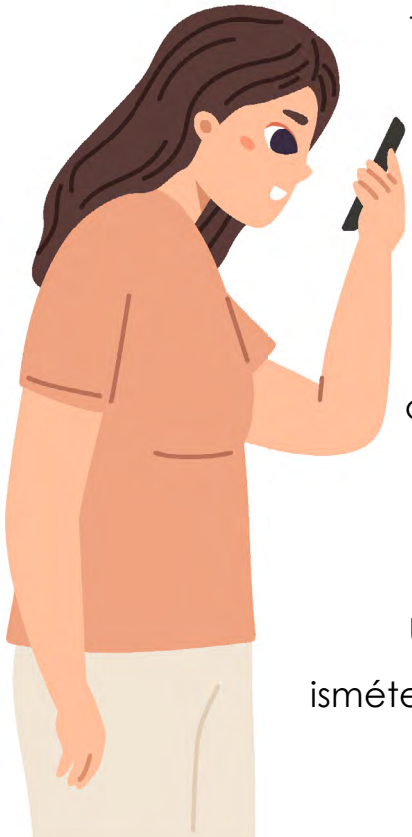
A social engineering technikákat gyakran használják „eszközcselekményként", például kezdeti hozzáférés megszerzésére egyéb módszerek részeként, például e-mail kompromittálás (BEC) módszerével elkövetett csalásoknál.



A social engeneering témában újszerű problémaként jelentkezett az AI térhódítása, ugyanis ezáltal egyre szofisztikáltabbá váltak a támadások. A ChatGPT által írt adathalász üzenetekben már nehezebben észrevehetőek az eddigi gyanús helyesírási hibák, valamint pontatlanságok. Ezen felül a hangklónozással vagy a deepfake-kel végrehajtott támadásoknak drámai módon javult a hatékonysága.

A jövőben az AI-val támogatott támadások emelkedése várható.

Ugyanakkor már több olyan eset történt az USA-ban, ahol a már közismert, magyar szakmai zsargonban csak „unokázós csalásnak" nevezett módszert finomítják még tovább olyan hívással, ahol az áldozat hozzátartozójának hangját klónozzák. Mivel az hangklónozáshoz szükséges egy minta az adott személy hangjából, így csökkenthető a támadás esélye, ha a közösségi médiában közzétett tartalmakat korlátozzuk. Jelenleg még a valós idejű deepfake videók nem elég hatékonyak a technológia fejletlensége miatt, azonban ezen a téren gyors fejlődés várható.



Ugyanakkor a régi, jól bevált módszerek sem tűntek el: ismételten kezd megjelenni a social engineering támadások azon fajtája, ahol a fizikai világban hajtják végre a

megtévesztést: gyakorivá váltak azon hamis QR kódok terjesztése, amelyek fertőzött weboldalakra mutatnak. Ezeket sokszor plakátokon vagy különféle szórólapokon terjesztik.

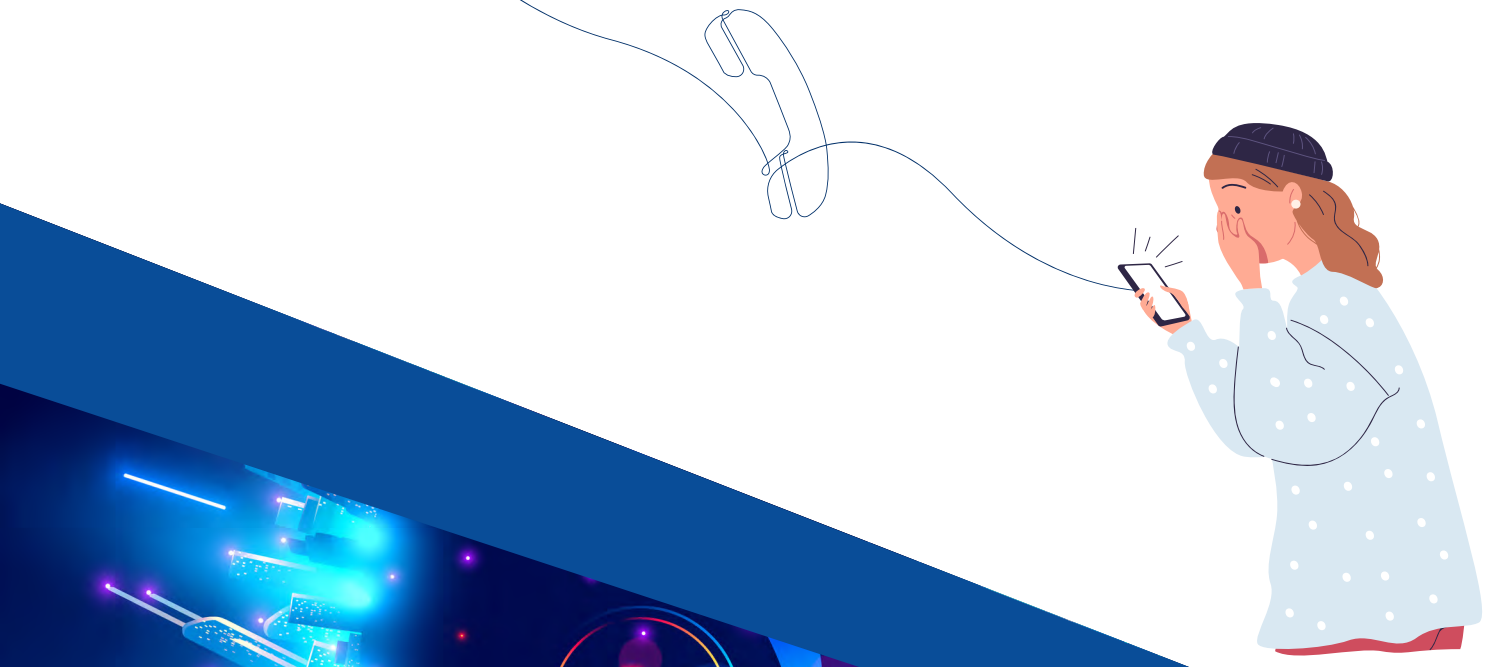
A QR-kódos csalásokról többet is megtudhat, ha elolvassa egy korábbi CTI jelentésünket.

De újfent megjelenőben vannak a klasszikus „elhagyott" USB pendrive-os támadások is. Növekedést mutatnak a kriptotárcák elleni közvetlen támadások, valamint az NFT-k ellen intézett támadások is, melyet leginkább egy fertőzött NFT-vel követnek el.

Újszerű jelenség az is, hogy a kiberbűnözők egyre gyakrabban követnek el zsarolást, viszont már ransomware-ek nélkül. Teszik ezt úgy, hogy felveszik a kapcsolatot a sértett szervezetekkel, és DDoS-támadással fenyegetik meg őket vagy éppen az eltulajdonított adatok nyilvános hozzáférhetővé tételét vagy egy esetleges jogsértés ügyfelek vagy hatóságok részére történő közzétételét helyezik kilátásba.

Ez ellentmond a korábbi tapasztalatnak, mely szerint a korábbi adathalász támadások során a támadók maximum a kezdeti szakaszban kommunikáltak a sértettekkel, egyéb alkalmakkor viszont elenyésző volt az interakció.

Ennek a fejlődésnek a hozadéka, hogy a kiberbűnözők szabályos helpdesk-et működtetnek, hogy sikeresen tudjanak egyeztetni a sértettekkel. Annak érdekében, hogy kellő pressziót tudjanak a célzott szervezetekre helyezni, sok esetben még attól sem riadnak vissza a támadó csoportok, hogy magánszemélyek családtagjait is bevonják a fenyegetésekbe.



Adatok elleni fenyegetések

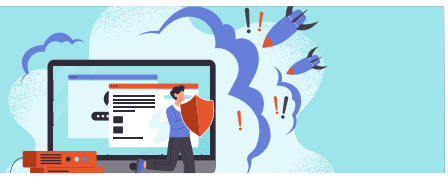
Az „**adat az új olaj**” kifejezés előrevetítette az adatvezérelt forradalmat, amelyet az elmúlt években megfigyelhettünk. Ma ugyanis egy olyan összekapcsolt társadalomban élünk, ahol a felhő, valamint az IoT technológiák és alkalmazások másodpercenként hatalmas mennyiségű adatot termelnek.

Az utóbbi években folyamatosan nagyobb teret hódító gépi tanulás (ML) és a mesterséges intelligencia (AI) modellek a rendelkezésre álló nagy mennyiségű adatok alapján találják meg egy-egy probléma megoldását. Ennek tükrében kulcsfontosságú, hogy megfelelő minőségű adatok álljanak rendelkezésre.

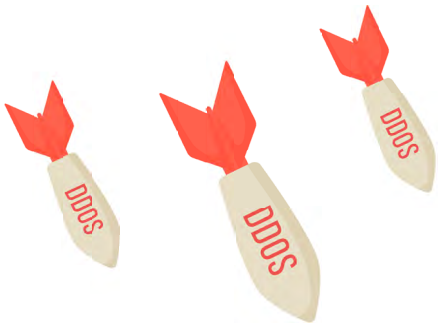
Például az AI chatbotok maguk is támadásnak vannak kitéve, mivel ezek a nyelvi modellek adathalmazokra támaszkodnak, így fennáll az adatmérgezés lehetősége. Ebben az esetben a chatbot hamisított adatok alapján fog válaszolni. Az efféle támadások célja az, hogy a modell pontossága csökkenjen, vagy a mérgezést követően téves következtetéseket vonjon le. Az így kapott modell ezután a célrendszer valós viselkedésétől eltérő viselkedést tanul meg, ami a célrendszert rossz döntések meghozatalára kényszeríti.

A gazdasági szempontok itt is előtérbe kerültek: Florian Tramér nevű kutató például aggályosnak nevezte azt a gyakorlatot, mikor a szöveges modelleket – mint például ChatGPT, Microsoft Bing, Google Bard – olyan alkalmazásokban használják, mint a keresőmotorok. Ugyanis ilyen esetekben a keresőmotorok esetében manipulálni lehet a modellek beviteli adatait, így például a modell azt hiheti, hogy egyik termék jobb, mint a másik.

Hozzáférés elleni fenyegetések (DoS-támadások)



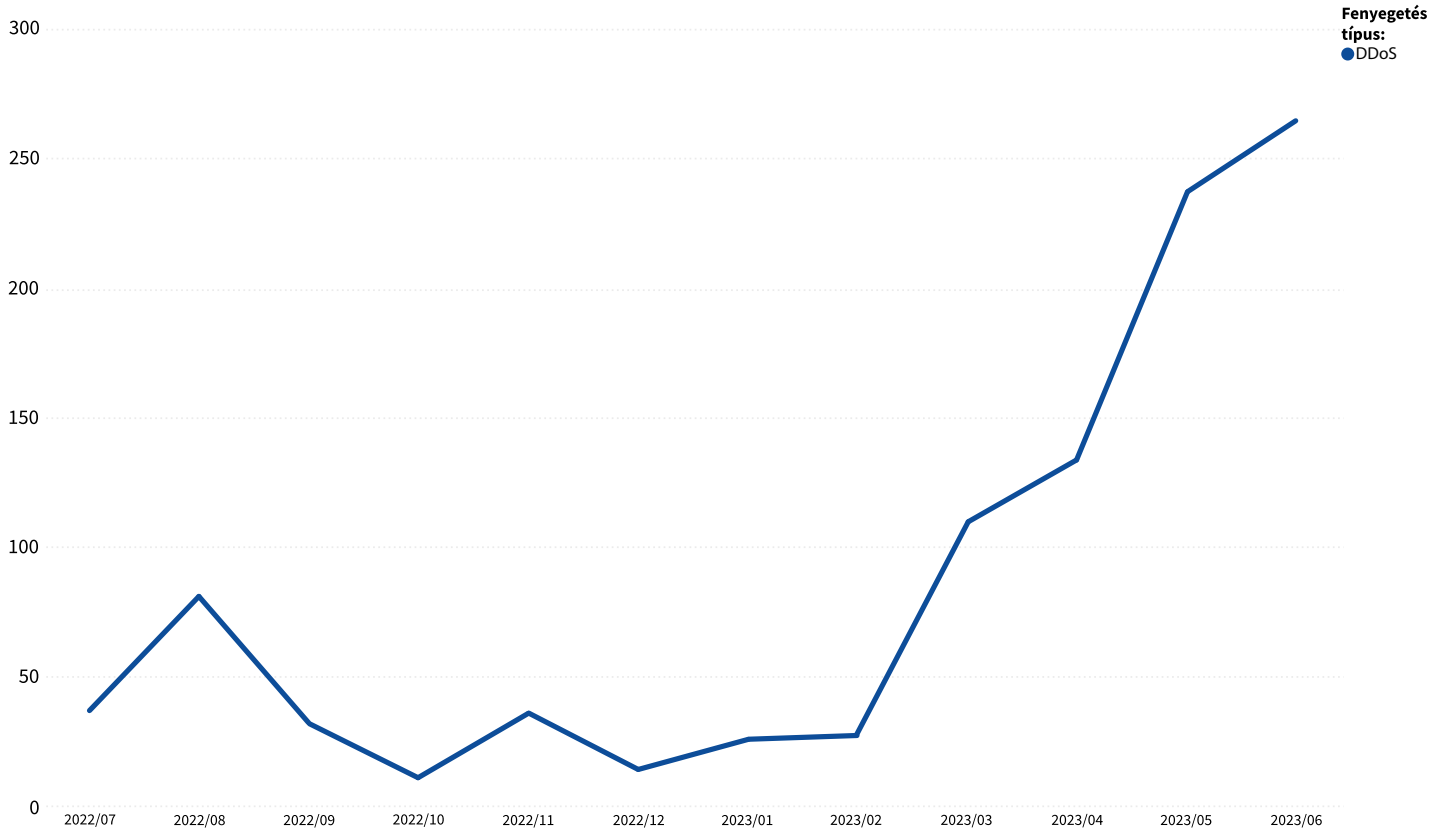
A hozzáférés számos fenyegetés és támadás célpontja lehet, amely támadási formák közül kiemelkednek a DoS-támadások. A DoS-támadások egyáltalán nem új keletűek, azonban még most is komoly fenyegetést jelentenek. A támadások akkor következnek be, amikor egy rendszer vagy szolgáltatás felhasználói nem tudnak hozzáférni a releváns adatokhoz, szolgáltatásokhoz vagy egyéb erőforrásokhoz. Ez történhet a szolgáltatás és erőforrásainak kimerítésével vagy a hálózati infrastruktúra túlterhelésével.



A jelentés által vizsgált időszakban jelentősen megnőtt a DoS-támadások száma, melynek főként aktuálpolitikai motivációi vannak, így például Oroszország Ukrajna elleni inváziója, melynek során a kritikus infrastruktúra elleni támadások száma a háború ötödik dimenziójaként megnőtt.

Ezen felül megszaporodtak a különféle hacktivista célból elkövetett DoS-támadások, rendszerint például az Ukrajnát támogató országok rendszerei ellen. Megjegyzendő ugyanakkor, hogy nem csupán az orosz-ukrán konfliktus hozadéka a fellendülő kibertámadási tendencia, hanem egyéb (globális) konfliktusok is – például Tajvan-Kína, USA-Izrael-Irán – összefüggésbe hozhatóak vele.

Az emelkedő tendenciát az alábbi grafikon szemlélteti:



2. ábra

A jelentési időszakban az ENISA által megfigyelt főbb incidensek időgrafikonja

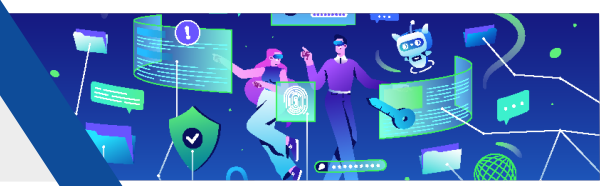
A 2022-es éves ENISA jelentés már felhívta rá a figyelmet, hogy jelentősek a Ransom Denial of Service támadások hatásai is, mely tendencia folytatódott. Az RDoS-támadások a DDoS-támadások egy speciális fajtája, melynek lényege, hogy előzetes elemzés alapján kiválasztanak a támadók egy lehetséges célpontot – például egy vállalkozást -, majd feltérképezik a rendszereinek a gyengeségeit, ezt követően pedig egy zsarolólevél útján megfenyegetik ezeket a vállalkozásokat, hogy váltságdíj ellenében nem fogják őket megtámadni DDoS-támadással.

A módszer elterjedtségének oka, hogy a DDoS-as-a-Service-nek köszönhetően a támadás csekély erőforrás ráfordítással nagy anyagi haszonnal kecsegtet.

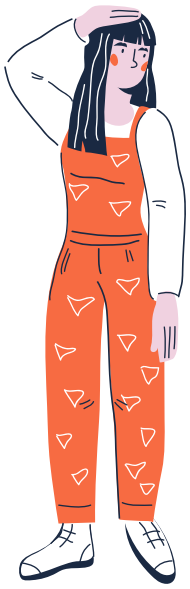
Összeségében elmondható, hogy DDoS-támadások egyre nagyobb méreteket öltenek, egyre komplexebbek és egyre olcsóbbak is. Itt is már gyakorlatilag egy kiforrott üzleti modell – DDoS-for-Hire – jelent meg, mely azt jelenti, hogy megrendelhetővé váltak a támadások, így annak kivitelezéséhez már gyakorlatilag semmilyen technikai előképzettség nem szükséges.

Megfigyelhető az is, hogy a hagyományos DDoS-támadások a mobilhálózatok és az IoT felé mozdultak el. Az érzékelők és az eszközök valójában könnyű célpontok, mivel gyengébb védelemmel – például nem megfelelő konfiguráció, vagy a ritkább szoftverfrissítés okán – vannak ellátva. Ezt követően már ezek az eszközök rendre egy botnet részévé válnak, hogy aztán azokkal további támadások hajtsanak végre.

Hozzáférés elleni fenyegetettség (internetes fenyegetések)



Az internet elérését fenyegető támadások egyre inkább előtérbe kerülnek, mivel már egy olyan alapvető szolgáltatásról van szó, amely már szinte nélkülözhetetlen a mindennapi élethez. Az internet elérhetőségét fenyegető veszélyek az internet vagy az elektronikus kommunikáció szándékos vagy éppen nem szándékos megszakítását jelentik, amelyek rendszerint a webes kapcsolat megszakadását vagy áramszüneteket eredményeznek.



Az internetkapcsolat megszakadása hátterében sokféle ok lehet: esetenként szándékos, kormányok által irányított vagy megrendelt leállítás, áramkimaradás, kábelszakadás, kibertámadás, egyéb műszaki probléma, természeti katasztrófa vagy éppen katonai akció. A támadás célja leginkább az információáramlás feletti ellenőrzés átvétele.

A szolgáltatás elleni támadások 2022-ben 323%-kal növekedtek meg 2021-hez képest. Összesen 35 országban 187 ilyen – regisztrált – esemény történt. Megfigyelhető, hogy a leállások mögött sok esetben valamilyen szándékos destruktív magatartás áll, jól felismerhetően valamilyen társadalmi eseménnyel összefüggésben, például humanitárius válság idején, tömegtüntetés közben, vagy éppen a háborús konfliktus alatt.

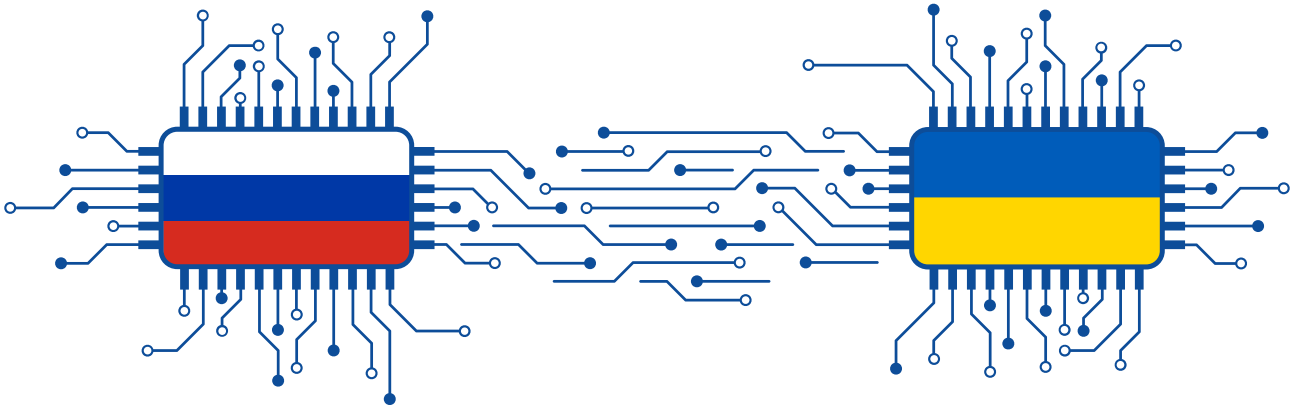
Az internet leállítása érdekében egyre kifinomultabb, célzott támadásokat alkalmaznak. Megfigyelhető, hogy a szolgáltatáskiesések egyre hosszabbak, egyes esetekben az 500 napot is meghaladták. Ezen felül megfigyelhető egyes weboldalak célzott tiltása, főként a közösségi oldaláké. A három leginkább érintett közösségi weboldalak a Facebook, az Instagram és a TikTok voltak.

Kiemelték a támadások közül a Border Gateway Protocol támadásokat (BGP), amelyek az internetes kommunikáció és a csomagok útválasztásának megzavarására szolgálnak. A BGP eltérítés az internetes hálózatokban egy olyan technika, amely során egy rosszindulatú támadó manipulálja a BGP útválasztási táblákat annak érdekében, hogy forgalmat irányítsanak át az általa ellenőrzött rendszerekre vagy hálózatokra.

Ennek eredményeként a támadó képes lehet közvetlen hozzáférést szerezni a forgalomhoz: ellenőrizni vagy megfigyelni azt, vagy akár hamisított adatokat is elhelyezhet a kommunikációban. Mindez azért jelent komoly veszélyt, mert a BGP az internetes forgalom irányításának alapvető protokollja, így hatalmas károkat tud okozni az internetes infrastruktúrákban.

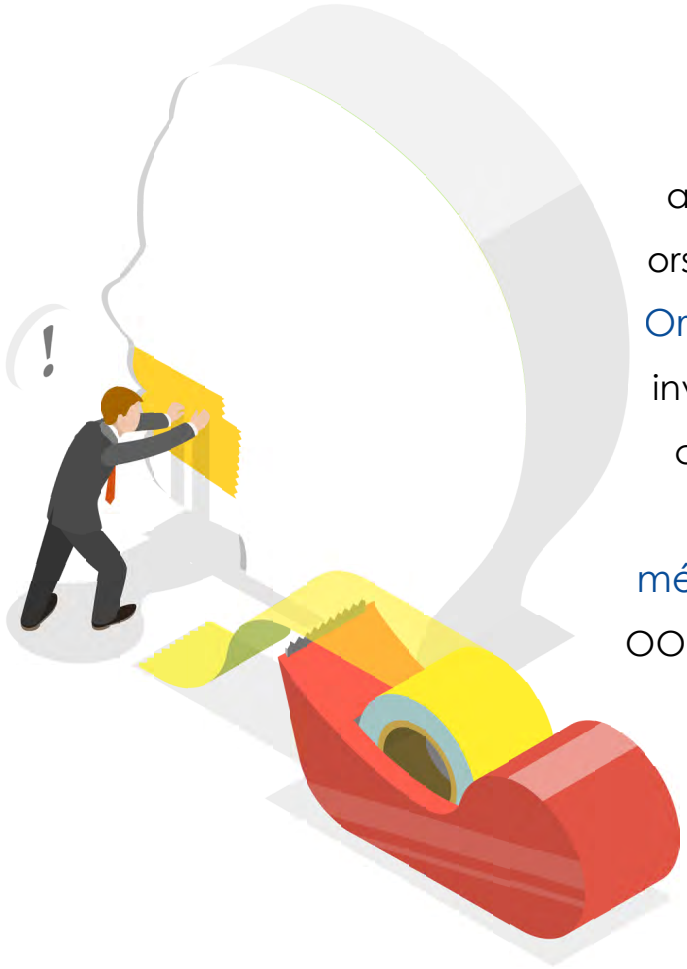
Ugyanakkor megjegyzendő, hogy nem minden BGP-ről szóló bejelentés mögött van szándékos BGP elterelés, hanem előfordulhat az is, hogy a hálózati eszközök egyszerűen rosszul vannak bekonfigurálva.

Az orosz-ukrán háború során megfigyelhető volt, hogy az orosz haderő számos támadást intézett alapvető fontosságú ukrán internetes infrastruktúrák ellen, abból a célból, hogy a teljes internet elérést ellehetetlenítsék, vagy éppen átvegyék a hálózatok feletti ellenőrzést.



Ez történt Herszon városának elfoglalása során, mikor az orosz fél arra kényszerítette a helyi internetszolgáltatókat, hogy adják át a hálózatok feletti ellenőrzést, majd fizikailag átirányította a mobil- és internetforgalmat az orosz tulajdonú hálózati infrastruktúrán keresztül. Ez lehetővé tette Oroszország számára, hogy blokkolja a közösségi médiához való hozzáférést, akadályozza az információk kiszivárgását és nagyobb kontrollt gyakoroljon a háborús narratíva felett.

Az internetes cenzúra is egyre elterjedtebb eszköz, akár politikai, akár katonai okokból. Ez főként a nemzeti vagy regionális kormányzatok szándékos akcióit jelenti, amelyek célja a nyilvánosság hozzáférésének korlátozása bizonyos weboldalakhoz vagy online információkhoz. A cenzúra többfélemódon valósulhat meg, mint például DNS-manipulálással, az IP-címek blokkolásával és a kulcsszavak szűrésével.



Az OONI, a Freedom House és a Riporterek Határok Nélkül nevű szervezetek aktívan figyelik az internetes cenzúra tendenciáit, amelyek közül a legrosszabb helyzetben lévő országok közé tartozik Kína, Mianmar, Irán és Oroszország. Az oroszok 2022 februári ukrajnai inváziója jelentősen befolyásolta az internetes cenzúra tendenciáit, Oroszországban több ezer weboldalt blokkoltak és a közösségi médiához való hozzáférést is korlátozták. Az OONI átfogó elemzése szerint Oroszországban széles körben korlátozták az internetes szabadságot, míg Délkelet-Ázsiában egyetlen ország sem érte el a szabad internet státuszát.

Információmanipuláció és zavarás

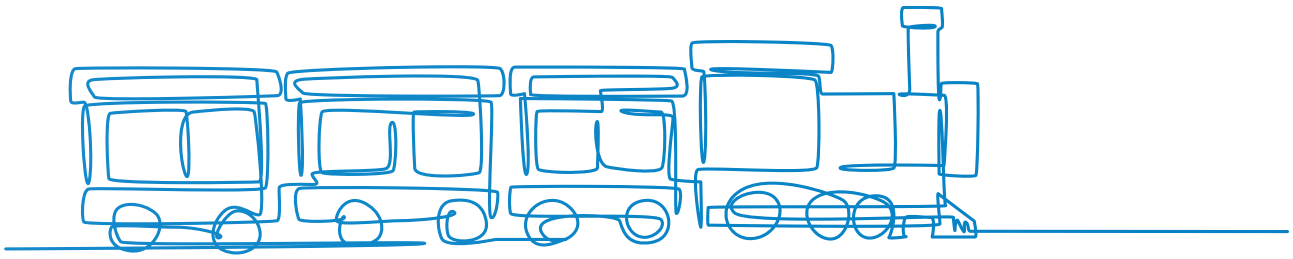
Az információmanipuláció és a kiberbiztonság közötti kapcsolatot gyakran vitatják. Az ENISA Threat Landscape álláspontja szerint azonban az információmanipulációt és a rá vonatkozó műveleteket kiberbiztonsági fenyegetésnek kell tekinteni, mivel ezek a műveletek közvetlenül érintik az információbiztonsági modell három összetevőjének legalább az egyikét, különösen az információ sértetlenségét.

Az információmanipuláció tekintetében az AI megjelentése szintén hatalmas lendületet hozott, ugyanis az így generált tartalmak már rendkívül hitelesnek tűnnek, és a folyamatos tartalomellátás is könnyedén biztosított. Ezeknek a manipulált tartalmaknak a kiszűrése egyre több erőforrást emészt fel, és tulajdonképpen elérik a céljukat, mely szerint már nehezen állapítható meg egyértelműen a tartalmakról, hogy valós tényeken alapulnak-e vagy sem.

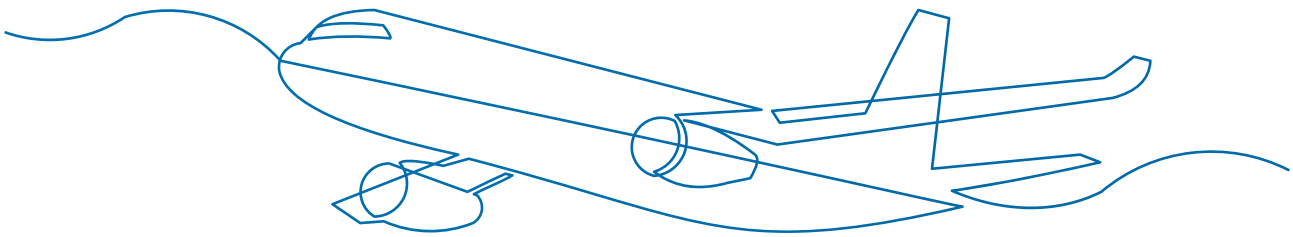
Az információmanipuláció – vagy dezinformálás - ugyanakkor már önálló üzletággá nőtte ki magát (*Desinformation-as-a-Service*). Több esetben kiderült már, hogy egyes vállalkozások fő tevékenységi köre, hogy a közösségi médiában automatizált dezinformációt hajtanak végre hírszerző ügynökségek, politikai kampányok, vagy akár magáncégek megbízásából. Ennek egyik módja például a hamis közösségi média profilok olyan tömeges felhasználása, mellyel már ténylegesen befolyásolni lehet a „közvéleményt".

Ellátási lánc elleni támadások

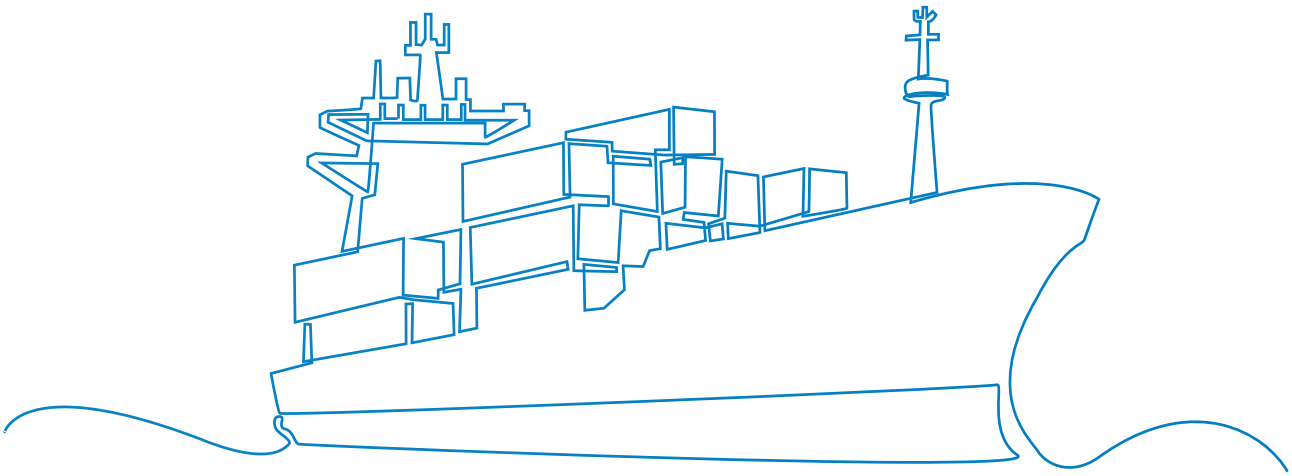
Az ellátási lánc elleni támadás a szervezetek és a beszállítók közötti kapcsolatot veszi célba. Az ellátási lánc azt a folyamatsort jelöli, ami egy termék létrehozásának gondolatától annak fogyasztóhoz való eljuttatásáig lezajlik. Ebbe beletartozik az összes szereplő, aki bármilyen módon részt vállal a termék létrejöttében és logisztikájában, függetlenül attól, hogy hozzájárulása mekkora és milyen jellegű.



Az ENISA jelentés definíciója szerint akkor beszélhetünk ellátási lánc elleni támadásról, ha legalább két támadás kombinációjából áll, pontosabban egy első támadás egy beszállítót céloz, amelyet utána a célpont megtámadására használnak fel azért, hogy hozzáférjenek annak eszközeihez. Tehát a definíció szerint mind a szállítónak, mind a vevőnek célpontnak kell lennie. Ez a meghatározás tehát kizárja azokat az eseteket, amikor például fejlesztői könyvtárakat támadnak meg, de nem célzottan egy konkrét áldozat ellen.



Az ilyen támadások „praktikuma” abban áll, hogy egyetlen beszállító elleni támadással több szervezetre is lehet hatást gyakorolni. Az ukrajnai háború az ellátási láncok biztonságára is negatív hatással volt. Az oroszpárti hacker-ek többnyire ukrán és európai ellátásokat vettek célba azért, hogy ellehetetlenítsék a humanitárius szállítmányok áramlását.



Ajánlás

A tanulmány végén részletesen bemutatásra került a **Mitre Att&ck** nevű globális tudásbázis, mely tartalmazza a különféle kiberfenyegetési modelleket és támadási módszereket, valamint ajánlási megoldásokat tesz az ellenük történő védekezésre, így annak megismerése kifejezetten ajánlott az iparági szereplőknek.

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2024