9. fejezet

A katonai információs rendszerek elleni műveletek – az informatikai megsemmisítés a valós szőnyegbombázástól a precíziós *malware*-ig

Üveges András József

Bevezetés

A digitális társadalom gyors előretörésének következtében felmerülő kiberbiztonsági kockázatok a mindennapi élet mellett számos ágazatot érintenek. Napjainkra a védelempolitikai nyilatkozatokban és elgondolásokban alapvetővé vált az, hogy a jelenlegi és jövőbeli katonai műveletekben a fizikai csapásmérő erőkkel együtt vagy önállóan alkalmazott kiber- és hibrid hadviselési módszerek dominanciája emelkedő tendenciát mutat. A NATO álláspontja szerint ez már a negyedik dimenziója a hadviselésnek. Mint minden katonai műveletet, a kiberműveleteket is fegyverekkel vívják meg. Ilyen eszközök a rosszindulatú szoftverek is, amelyek napjainkra a kiberhadviselés egyik alapeszközévé váltak, amelyekkel az egyes reguláris vagy irreguláris erők sikeres műveleteket képesek végrehajtani a katonai információs rendszerek ellen.

A NATO 2007-től kiemelt figyelmet fordít a kibervédelemre és a kiberhadviselésre. A 2012-es évben a kibervédelem mint koncepció vagy elgondolás bekerült a NATO védelmi tervezési folyamatába is. A legjelentősebb esemény viszont a 2014-es walesi csúcs[1] egyik döntése volt, amellyel elfogadták a NATO kibervédelmi szakpolitikai irányait.[2]

Ezt követően 2016-ban a varsói csúcsértekezleten a szövetséges erők amellett, hogy megerősítették a NATO védelmi jellegét, műveleti területté nyilvánították a kiberteret is.[3]

[1] NATO e-Library: *Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales*. 2014.

[2] *Wales Summit Declaration* (2014): i. m. 72–73.

[3] NATO e-Library: *Warsaw Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw.* 2016.

https://doi.org/10.36250/01079_09

https://orcid.org/0000-0002-5860-2405

Általánosan elmondható, hogy a kiberhadviselés vonatkozásában a műveleteket állami szereplők, jellemzően hírszerzésre, disztruptív vagy destruktív céllal, közvetlenül – vagy proxyfelhasználó segítségével – hajtják végre. A kiberhadviselés témaköréhez tartozik minden olyan kibertérben végrehajtott offenzív művelet is, amelynek a támadást végrehajtó ország – tágabb értelemben szélsőséges szervezet – szemszögéből katonai vagy politikai értelemben véve értékelhető (hasznos) eredménye van.

Az előbbiekben említett támadásokat rosszindulatú szoftverek segítségével lehet a leghatékonyabban végrehajtani a kibertérben, ahol használhatjuk ezeket széleskörűen (globálisan vagy mondhatjuk, szőnyegbombázás formájában) vagy csak konkrétan egy adott célpont ellen, testre szabva. Utóbbi esetben kifejezetten a célba vett rendszerre írt kártékony szoftverrel hajtják végre a támadást.

A *malware*-eket hatékonyan alkalmazzák egymás ellen akár békeidőszakban is az ellenérdekeltségű országok. Ezek a műveletek a kibertérben követik a valóságban fennálló geopolitikai ellentéteket. Ilyen geopolitikai ellentét húzódik például Kína és India viszonylatában, illetve India és Pakisztán vonatkozásában. A szemben álló felek előszeretettel alkalmaznak precíziós *malware*-eket arra, hogy a kibertérből támadva megbénítsák vagy rombolják az ellenérdekeltségű ország infrastruktúráját, gyengítve ezzel annak gazdaságát. Rosszabb esetben destabilizálják annak alkotmányos rendjét egy nagyobb támadással. Ezekkel az eseményekkel a sajtóban többször is találkozhatunk.

Egy jól időzített *malware*-támadással (*fake news, defacement* stb.) hiteltelenné lehet tenni egy kormányt vagy egy szervezetet is. Akár választásokat is befolyásolhatunk velük. Azaz a *malware*-kampányok kiválóan alkalmasak az információs műveletek kivitelezésére a kibertérben.

A kínai kormány és az indiai vezetés között 2021-ben többször kiújult az ellentét egy határvita miatt. A kasmíri térséghez tartozó Ladakban a kínai kormány 90 ezer négyzetkilométeres területet követel magának. Az indiai rezsim szerint a kínai fennhatóság alatt álló Akszai Csin-fennsík 38 ezer négyzetkilométere Ladak eredeti része, amelynek ezért Indiához kell tartoznia.

2021 márciusában a *The Hindu* sajtóinformációi szerint a kínai kormányhoz köthető hackercsoport kártékony szoftvert juttatott be az indiai villamosenergia-elosztó rendszer egy részét kiszolgáló infrastruktúrába.

A támadást az amerikai érdekeltségű Recorded Future kiberbiztonsági vállalat fedte fel. A támadást 21 IP-címről indították 10 energetikai vállalat ellen.[4]

Rosszindulatú szoftverek

Mielőtt a témát részletesen tárgyalnánk, szükséges pontosítani a *malware* fogalmát. A *malware* kifejezés alapvetően és döntően gyűjtőfogalom. Magába foglal számos rosszindulatú szoftvert, mint például a trójai programok, a zsaroló vírusok, a klasszikus értelemben vett vírusok, férgek és banki kártevők. A médiában többször szinonimaként használják a kártevő szoftver, a kártékony szoftver és a káros szoftver fogalmát is.

Fajtájukat tekintve részletes leírást lehet olvasni Kovács László *A kibertér védelme* című művében, ahol a szerző részletesen kifejti az egyes csoportok jellemzőit.[5]

A káros szoftverek közös tulajdonsága az, hogy a készítőik rosszindulatú szándékkal, károkozás, illegális anyagi haszonszerzés vagy hírszerzés céljából készítették el ezeket. Ha még pontosabban megpróbáljuk definiálni, akkor mondhatjuk azt is, hogy olyan szoftverek, amelyek más szoftverek vagy rendszerek üzemszerű működését megakadályozzák,[6] onnan illegális módon adatokat tulajdonítanak el további felhasználás céljából.

Általánosságban az is elmondható róluk, hogy gyakran az elavult rendszerek sebezhetőségeit, a nem naprakész biztonsági rendszabályok okozta biztonsági réseket kihasználva terjednek, vagy a memóriában elfedve várakoznak, és csak egy előre programozott esemény során aktiválják magukat. Egyes esetekben ismert alkalmazásokat utánozva maradnak észrevétlenek. De az sem ritka, hogy a pszichológiai manipulációs módszerek segítségével emberi mulasztás vagy figyelmetlenség során jutnak be a célba vett rendszerekbe.

A *malware*-ek másik tulajdonsága, hogy kiválóan alkalmasak arra, hogy hatékony eszközei legyenek a korszerű kiberműveleti tevékenységeknek.[7]

[4] Regionális árufeladó központ *(regional load despatch centres)* és állami együttműködők, két tengeri kikötő.

[5] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 122. 5. táblázat.

[6] Simon Kramer – Julian C. Bradfield: A General Definition of Malware. *Journal in Computer Virology,* (2010), 6. 105–114.

[7] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 271.

A téma relevanciája és nagysága miatt alapvetően a *malware*-ek két típusával foglalkozunk. Az egyik csoportba azok tartoznak, amelyeket széles körben terjesztenek a készítőik, és céljuk, hogy úgynevezett széles merítést alkalmazva nagy mennyiségű adatot gyűjtsenek az internetről. A folyamatban nincs konkrét célpontja a *malware* alkalmazójának. Célja, hogy globális méretekben fertőzzön meg informatikai rendszereket, majd a befolyt adatokat szintetizálva, szűrve felhasználja a későbbiekben. Azaz a nagy adattömegben olyan részinformációkat keresnek az elkövetők, amelyek egy későbbi támadás során felhasználhatóak. Természetesen egyes esetekben az ilyen fajta támadás során is lehet célirányosan adatokat keresni.

A védelmi szektor esetében ilyen adatok lehetnek például csoportos e-mail-címek, amelyek köthetőek valamilyen hadiipari vállalathoz. Vagy ilyen módszer alkalmazása során nagy méretű adathalászatból származó, nem rendszerezett adatokban olyan e-mail-címeket keresnek, amelyek köthetőek valamilyen kormányzati vagy hatósági szervezethez. Ebben az esetben akár a keresés (szűrés) paramétere lehet az, hogy az e-mail-cím tartalmazzon olyan tartománynevet mint például a gov.xxx.[8] A közelmúltban kitudódott SolarWinds-botrány is példa egy ilyen tevékenységre. A kormányzati intézmények és nagyvállalatok által is előszeretettel és széles körben használt rendszerfelügyeleti programokat fejlesztő SolarWinds 2020. december elején bejelentette, hogy nagyon komplex és megtervezett módon, vélhetően egy állami támogatású hackercsoport rosszindulatú kódot helyezett el az Orion nevű szoftverük frissítésében. Itt fontos hangsúlyozni azt, hogy ez érintette többek között az amerikai energiaügyi minisztérium nukleáris laboratóriumait is.

A másik csoportba pedig olyan szoftverek tartoznak, amelyeket célirányosan alkalmaznak egy adott célpont ellen. Mivel ezek a szoftverek az információs műveletek részét is képezik, ezért a későbbiekben mindenképpen tisztázni kell röviden az információs műveletekben betöltött szerepüket, valamint magukat az információs műveleteket is.

[8] Konkrét országhoz köthető kormányzati weboldal, amely a legfelső szintű tartománynév alá berendelt második szintű tartománynév.

Katonai információs rendszerek

A *malware*-ek definiálása után érdemes röviden megemlíteni, mit is értünk katonai információs rendszereken.

A katonai információs rendszereket alapvetően és meghatározóan az információs térben értelmezzük, ahol „az információs környezet a fizikai, az információs és a kognitív dimenziót magában foglaló információs műveleti tartomány, amelyben a különféle információkezelési és döntési folyamatok zajlanak, illetve az információs képességek megvalósulnak”.[9]

A katonai információs rendszerek alapvető célja, hogy biztosítsa az információáramlást a vezetési és irányítási, valamint a felderítési rendszerek részére, valamint, hogy biztosítsa a katonai műveletek vezetéséhez szükséges információkat. Ezeken a rendszereken strukturálatlan és strukturált adatok cseréje zajlik, valamint már megvalósul az automatizált adatkezelés, az automatizált adatmegosztás és az alkalmazott információmegosztás is.

Egy korszerű haderő számos ilyen rendszert üzemeltet béke-, valamint különleges jogrendi időszakban. Ilyen például a NATO SECRET WAN, a NATO UNCLASSIFIED WAN, illetve a NATO WWW.[10] Az egyik legkomplexebb és legjobb példa a NATO BICES-rendszer,[11] amely számos katonai információs rendszert egyesít. Természetesen ide értendők az egyes haderők által működtetett C4ISR-rendszerek[12] is.

De nemcsak a műveleteket támogató rendszereket kell idesorolni, hanem még idetartoznak a védelmi szektorbeli kormányzati intézmények (védelmi minisztérium szintű szervezetek, katonai felderítő és elhárító szolgálatok) minősített rendszerei, a minősített haditechnika beszállítói, hadigazdasági információs rendszerek (állami érdekeltségű hadigazdasági vállalatok, állami tulajdonú haditechnikai cégek stb.), valamint a haderőt támogató infrastruktúra (energiahordozók szállításáért és elosztásáért felelős rendszerek, logisztikai, egészségügyi hálózatok stb.) működéséért felelős információs rendszerek is.

A legfontosabb és közös jellemzőjük az, hogy ha működésükben hiba lép fel, akkor kiemelt biztonsági kockázatot jelentenek a katonai és nemzetbiztonsági műveleti tevékenységekre, valamit a rutinszerű napi tevékenységre egyaránt.

[9] Haig (2018): i. m. 211.

[10] *World Wide Web,* WWW.

[11] BICES: *Battlefield Information Collection and Exploitation System.*

[12] C4ISR: *Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance* (vezetés, ellenőrzés, kommunikáció, számítógépek, hírszerzés, megfigyelés és felderítés).

Ezek a rendszerek napjainkban már korszerű informatikai rendszerek, amelyek rejtjelező eszközökön keresztül továbbítják a vezetési szintek közötti információkat. Ezek az informatikai rendszerek a polgári életben megtalálható rendszerekhez hasonlóan sérülékenyek, egy megfelelő időben és helyben alkalmazott kártékony szoftverrel jelentős károkat lehet okozni bennük. Működésük és céljuk hasonló a klasszikus értelemben vett létfontosságú infrastruktúrához.

Információs műveletek

Az információs hadviselés jelenleg gyorsan fejlődő és egyelőre nehezen definiálható terület. A katonai műveletek tervezése és szervezése során napjainkban egyre nagyobb figyelmet fordítanak erre a területre a katonai felsővezetők és a politikai döntéshozók is. A digitális ökoszisztéma gyors fejlődése és az információs környezet térnyerése következtében a katonai és politikai döntéshozók egyre több lehetőséget látnak az információs műveletekben.

Kiberműveletek

A *malware*-ek alkalmazását az információs műveleteken belül elsősorban a kiberműveletek vonatkozásában érdemes vizsgálni.

Ennek egyik oka, hogy a kiberműveletek egyik eszköze lehet a kártékony szoftver, amelynek segítségével viszonylag gyorsan, költséghatékonyan és célirányosan lehet bénítani, lerombolni, megzavarni az ellenérdekeltségű ország információs rendszereit, és nem mellesleg információt szerezni. Azaz megkímélhető a haderő humánerőforrása, valamint már a kinetikus műveletek megkezdése előtt meg lehet kezdeni az ellenség vezetési rendszerének lerombolását, az ellenség befolyásolását.

Az előbbiekben említett előnyök érvényesítésének eszközei lehetnek a kártékony szoftverek, amelyeket két csoportba lehet osztani: olyan *malware*-ek, amelyek alkalmazása széles spektrumban hatékony, valamint a precíziós csapáshoz előre elkészített kártékony szoftverek.

Malware-ek széles spektrumú alkalmazása (szőnyegbombázás)

Az információs műveletek során végrehajtott kiberműveleteknek több célja lehet. Ezek közé tartozik a megtévesztés, a katonai hálózatok üzemszerű működésének megakadályozása, az informatikai rendszerek ideiglenes megbénítása, valamint ugyanezen rendszerek fizikai rombolása és az információ gyűjtése.

A *malware*-ek széles spektrumú használatát az alábbiak szerint érdemes csoportosítani:

– érzékeny adatok gyűjtése;
– véletlenszerű és nagy méretű rombolás (kiberterrorizmus);
– esetleges későbbi kibertámadás előkészítése.

Érzékeny adatok gyűjtése

Honvédelmi vonatkozásban az információgyűjtés esetében értelemszerűen csak a honvédelemmel kapcsolatos információk a relevánsak. Az adatgyűjtésnek több ismert módszere létezik, viszont katonai viszonylatban a legcélravezetőbb az, ha nagy mennyiségű adatot begyűjtünk az ellenérdekeltségű célpontról, majd a megszerzett adatokat szintetizáljuk és szűrjük. A tisztított adatot a későbbiekben relevancia szerint klaszterekbe rendezzük,[13] vagy az általunk meghatározott struktúrába csoportosítjuk a gyors és hatékony kereshetőség érdekében.

Ennek a folyamatnak a terjedése növekvő tendenciát mutat az elmúlt időszakban. Elég csak felfigyelni arra, hogy erre a tevékenységre szolgáltatási iparág is épült. A kártékony szoftverek üzemeltetését egyes hackercsoportok már szolgáltatják is, és ezt általában a számítógépes támadások végrehajtására szolgáló szoftver és hardver bérbeadásaként is nevesítik (MaaS).[14] A MaaS-szerverek tulajdonosai fizetett hozzáférést biztosítanak egy rosszindulatú programokat terjesztő botnethez.[15] Az ilyen szolgáltatások ügyfeleinek általában személyes fiókot kínálnak, amelyen keresztül irányíthatják a támadást, valamint technikai támogatást nyújtanak részükre. Ez a szolgáltatás kiemelten alkalmas a katonai

[13] A klaszteranalízis során olyan dimenziócsökkentő eljárást alkalmazunk, amely által megpróbáljuk a klasztereket tartalmi relevanciájuk szerint csoportosítani. Az automatizált osztályozást követően viszont ilyenkor sajnos manuálisan kell ellenőrizni a csoport homogenitását.

[14] KasperskyLab: Malware-as-a-service (MaaS).

[15] Más néven zombihálózathoz: olyan számítógépek hálózatához, amelyek úgy szolgálják a hackerek céljait, hogy azok tulajdonosa nem is tud róla.

információs infrastruktúra elleni támadásra is, hiszen a támadó anonim módon csak egy szolgáltatást bérel, amelyet könnyűszerrel testre szabhat.[16] A gyártó emellett műszaki segítséget nyújt a *malware* továbbfejlesztésére. De a leglényegesebb paraméter az anyagiak és az idő ráfordítása a támadásra, hiszen ilyen szolgáltatással költséghatékony és gyors dinamikájú műveleteket lehet végrehajtani.[17]

Ilyen adatszerzésre kiválóan alkalmasak a kiberhírszerzés során használt kártékony szoftverek, amelyeket kémprogramoknak vagy más néven kémszoftvernek *(spyware)* neveznek. Általában az interneten terjedő azon számítógépes programok összességét nevezik így, amelyek célja, hogy a felhasználó tudomása nélkül megszerezzék az érintett informatikai eszközök felhasználójának érzékeny adatait.

A legtöbb *spyware* a felhasználó tudomása nélkül, valamilyen megtévesztésen alapuló módszerrel kerül bele az informatikai rendszerbe. A megtévesztés egyik módja, hogy hasznos, a felhasználó számára releváns alkalmazásba kerül be.[18] A másik módszer a böngészőn keresztüli bejutás. Ebben az esetben a felhasználó egy már megfertőzött internetes felületre navigál,[19] majd lefut a fertőző kódsor, és a kártékony program a rendszerre települ.

Adattípusok

A széles spektrumú adatgyűjtés a katonai rendszerek vonatkozásában az esetek túlnyomó többségében az alábbi információkra korlátozódik:

- hadiipari és hadigazdasági vállalkozások üzleti adatai;
- hadiipari beszállítók érzékeny adatai;
- haditechnikai vállalatok műszaki megoldásai;
- katonai létfontosságú rendszerek sérülékenysége;
- létfontosságú információs infrastruktúra rendszerelemeinek sérülékenysége;

[16] Dark net C&C vezérlőpult, késleltetett indítás, *delayed encryption, mutex,* feladatkezelő/*registry editor disabler, UAC bypass, desktop wallpaper change, offline encryption, unkillable process.*

[17] EnigmaSoft: *'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline.*

[18] Például a Gator (GAIN).

[19] Például az Internet Optimizer vagy más néven DyFuCA.

- a haderő személyi állományával kapcsolatos adatok (személyes vagy akár biometrikus);
- technológiai és ipari vállalatok érzékeny adatai;
- kormányzati és hatósági rendszerek adatai;
- valamint a haderőt érintő ipari vezérlő rendszerekkel kapcsolatos információk, mint például nukleáris erőművekben működő vezérlő és irányító rendszerek adatai, hadiipari gyártók vállalatirányítási rendszerei, közfeladatot ellátó állami tulajdonú gazdasági társaságok.

Természetesen ezen rendszerek a fent felsorolt adatok mellett számos olyan információt gyűjtenek, amely közvetve érinti a haderőt, és nem alkalmas arra, hogy egy információs rendszert megbénítson.

A *malware*-ek több esetben véletlenszerűen katonai információs rendszereket kiszolgáló informatikai infrastruktúrát is rombolhatnak. Ennek oka, hogy a nem precíziós *malware*-ek széles körben terjednek. Az elmúlt évek során több esetben történt meg az, hogy ipari rendszerekbe vagy létfontosságú infrastruktúrák egyes rendszereibe kerültek be *malware*-ek. Ezek nagy része nem az ipari rendszerek elleni célzott támadáshoz kifejlesztett *malware* volt, hanem csak általános kártevő, amely bejutott az ipari vezérlő rendszerbe (*Industrial Control System:* ICS).[20] Közöttük legnagyobb számban a gyorsan terjedő *malware*-családok képviselői találhatóak meg. Ilyen például a szaúd-arábiai olajfinomítók elleni kibertámadásról híressé vált[21] Triton *malware,*[22] amelyre a későbbiekben Triton/TriSIS néven hivatkoztak. Ritkábban a különböző trójaiak is jelen lehetnek ezekben a rendszerekben, amelyek viszont már hozzáférést is adhatnak a támadóknak a megtámadott ICS-rendszerhez. Az utóbbi *malware*-ek, bár nem célzott támadások eszközei, mégis jelentős károkat okozhatnak az ipari rendszerekben.

A Dragos Inc. tanulmánya szerint éves szinten megközelítőleg 3000 ipari rendszerben tűnhetnek fel klasszikus IT-*malware*-ekre visszavezethető, nem célzott támadásból származó fertőzések.[23]

[20] Malware in Modern ICS. Understanding Impact While Avoiding Hype. *POWER,* 2017. május 1.

[21] Az amerikai NSA, az FBI, a DHS és a DARPA vizsgálatokat folytatott, mivel meg nem erősített információk szerint a támadók célja nem csupán az olajipari létesítmény működésének megbénítása volt, hanem fizikai pusztítást akartak előidézni a biztonsági rendszer kompromittálásával.

[22] Davide Franzetti: Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON. *Security Boulevard,* 2019. február 26.

[23] Dragos Inc.: *Industrial Control System Threats.* 2019. február 14.

Az adatgyűjtő módszerek célja

A *malware*-ekkel folytatott széles körű adatgyűjtés célja valamilyen előny (gazdasági, technológiai, döntéstámogató) költséghatékony és gyors megszerzése. A jelenlegi tendenciák szerint több esetet kell megkülönböztetni. Célszerű elkülöníteni a támadó entitást, a megszerzendő információkat, valamint a támadás célját. Napjainkban az autokratikus országok esetében jellemzően valamilyen haditechnikai információ, érzékeny honvédelmi adat, harcértékadat megszerzése a cél. Ezen információk részletes ismerete szükséges ahhoz, hogy a környező országokkal szemben műveleti előnyt szerezzen az érintett ország.

Erre talán a legjobb példa az észak-koreai kormány stratégiája. A nemzetközi sajtóban szinte folyamatosan egymást követik az olyan cikkek, ahol Phenjant globális méretű kiberhírszerző kampányokkal vádolják meg. Ahogy számos autokratikus kormány proxyfelhasználókat használ, Észak-Korea esetében is számos, *malware*-ekkel végrehajtott támadással hozták összefüggésbe a rezsimhez tartozónak gondolt csoportokat.[24]

Ha csak két évet vizsgálunk is, az észak-koreai kormányhoz köthetően számos hír jelent meg a sajtóban.[25] Az országot nemzetközi import- és exportkorlátozások sújtják. Korea gazdasági helyzetét mutatja az is, hogy Kim Dzsongun vezető 2021 júniusában beismerte, az ország élelmezési gondokkal küzd.[26] A kieső gazdasági forrásokat a rezsim a viszonylag fejlett, de mindenképpen globálisan jelen lévő kiberképességeivel próbálja meg pótolni. Azaz például globálisan alkalmaz kriptopénzbányász-szoftvereket illegálisan. A feltelepült *malware*-ek több milliárd amerikai dollár értékű károkat okoznak a kriptopénz-kereskedelemben.[27]

Az észak-koreai állam által támogatott Lazarus csoport 2020-ban feltételezhetően megközelítőleg 12 országban folytatott kiberhírszerző tevékenységet katonai beszállítók irányában. A KasperskyLab kutatói[28] szerint a kiberhírszerző

[24] A támadók előnye, hogy jogilag bonyolult nekik tulajdonítani a támadást, és minden ország másmás megfontolások alapján dönti el, hogy diplomáciailag felvállalja-e az elkövetők megnevezését. A célország szempontjából hátrány, hogy teljes biztonsággal aligha lehet megnevezni az elkövetőt, és nehéz ellenlépéseket is tenni, akár technikailag, akár diplomáciailag.

[25] Vyacheslav Kopeytsev – Seongsu Park: *KasperskyLab ICS CERT Lazarus targets defense industry with ThreatNeedle*. Kaspersky ICS CERT, 2021. február 25.

[26] Lin Yoon: Kim Jong Un Acknowledges Food Crisis in North Korea. *Hrv.org,* 2021. június 17.

[27] Dan Mangan: North Korean Hackers Charged in Massive Cryptocurrency Theft Scheme. *CNBC,* 2021. február 17.

[28] Kopeytsev–Park (2021): i. m.

tevékenységet adathalász levelekkel kezdték meg. A levelek túlnyomó többségének témája vagy a Covid–19-járvánnyal kapcsolatban érkezett, vagy a célba vett vállalat munkatársainak ajánlottak benne hamis munkalehetőséget a védelmi szektor területén.[29] Ezekben a levelekben a Microsoft Word makrójának segítségével az elkövetők telepíteni tudták az áldozatok informatikai eszközére a ThreatNeedle elnevezésű *malware*-t. A kártékony szoftver ezt követően hátsóajtó-alkalmazást telepített, amelynek a segítségével a támadók képesek adatokat megszerezni a megfertőzött informatikai eszközökről.

Másik eset: a Reuters londoni székhelyű világhírügynökség 2020. áprilisi cikke szerint a kínai kormányhoz köthető hackercsoport hónapokon át végzett kiberhírszerző tevékenységet amerikai hadiipari vállalatok ellen. A támadás során a virtuális magánhálózatokat (*virtual private network:* VPN) vették célba, és ezen rendszereken keresztül szerezték meg az érzékeny adatokat. Ezekre az incidensekre a *Cybersecurity and Infrastructure Security Agency* (USA CISA) is felhívta a figyelmet, miszerint a támadók a VPN-hálózatokba juttathatják a SUPERNOVA elnevezésű kártékony alkalmazást.[30]

Precíziós malware alkalmazása

Az ipari vezérlőrendszerek (*Industrial control systems:* ICS) kiberbiztonsága egyre meghatározóbbá válik a folyamatosan fejlődő és automatizálódó digitális ökoszisztémában. A létfontosságú infrastruktúrák megfelelő működése meghatározóan függ az ICS-rendszerek kiberbiztonságától. Ezek a rendszerek számos elemből állnak, idetartoznak a SCADA-rendszerek *(Supervisory Control and Data Acquisition),* a HMI-k *(Human-Machine Interface),* a programozható logikai vezérlők (*Programmable Logic Controller:* PLC), a távoli diagnosztikai és karbantartó eszközök, az ipari szenzorok.

Az informatikai hadviselés hatékony és sikeres alkalmazásának több előnye is van. Viszonylag kevés anyagi ráfordítással és az élő erő megkímélésével súlyosabb károkat lehet okozni az ellenérdekeltségű fél vezetési-irányítási rendszerében.

[29] Derek B. Johnson: Threatneedle Malware Tied to Year-Long North Korean Espionage Campaign Against Global Defense Industry. *Scmagazine,* 2021. február 25.

[30] Justin Katz: Cisa Issues Warning on Exploited VPN Flaw. *GCN.com,* 2021. április 23.

Más esetben békeidőszakban lehet a létfontosságú infrastruktúrákban kártékony szoftverekkel jelentős fizikai károkat okozni. Ezeknek az incidenseknek kiemelt jelentősége van, hiszen ezek a támadások nem kizárólag katonai létfontosságú rendszerelemek ellen irányulnak, hanem a polgári lakosságot is érinthetik. Emellett a létfontosságú rendszerek interdiszciplináris jellege miatt több rendszert is érinthet a támadás.

A precíziós *malware*-ek hatékonyan alkalmazhatóak katonai információs rendszereket kiszolgáló infrastruktúra-vezérlő rendszerek ellen. Ezen *malware*-ek egy részét célirányosan erre a feladatra készítik fel.

Az ICS-rendszerek ellen készült *malware*-ek száma viszonylag alacsony, a legjelentősebb ezek közül a Stuxnet, a Havex és a BlackEnergy2.

Természetesen azért vannak kivételek is, az ukrán áramszolgáltatók elleni 2015. decemberi támadás megmutatta azt is, hogy egy támadónak nem szükséges magas szinten specializált *malware*-t használni ahhoz, hogy súlyos üzemzavart tudjon előidézni komplexebb ipari vezérlő rendszerben. Az ICS-rendszerek ellen készített *malware*-ek egy kis csoportját a támadók olyan ICS-alkalmazásnak álcázzák, amely hivatalosan is használatban lévő vezérlő szoftver. Egy ilyen *malware* akkor hatékony, ha mögötte állami szereplő áll, ami biztosítja a szakértőket, a katonai és mérnöki tanácsadókat. Emellett rendelkezésre áll a megfelelő teszt- és laborkörnyezet, valamint a megfelelő anyagi források. A szoftver esetleges célba juttatását pedig titkosszolgálati műveleti tevékenység biztosítja. Ha az előbbiekben említett feltételek együttesen rendelkezésre állnak, akkor nagy eséllyel már számottevő károkat lehet okozni.

Létfontosságú rendszerek

A precíziós *malware*-ekkel végrehajtott támadások kiemelt célpontjai katonai viszonylatban a katonai létfontosságú rendszerelemek lehetnek. Interdiszciplináris jellegük miatt ezek a rendszerek kiemelt kockázatot jelentenek.

Fontos megjegyezni, hogy ez a probléma nem új keletű. Hasonló jelentősebb esemény bekövetkeztének lehetőségét és forgatókönyvét kifejtették a 2010-ben megjelent *Digitális Mohács* című tanulmányban is.[31] A létfontosságú

[31] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56.

infrastruktúra és a kapcsolódó információs rendszerek viszonylatába a folytatás ad részletes betekintést.[32] Ezeket az előzőekben részletesen bemutattuk.

A honvédelemmel kapcsolatba hozható létfontosságú rendszerek közül is kiemelkedően fontosak például az energetikai, valamint a fosszilis energiahordozók szállítását és elosztását biztosító információs rendszerek, esetlegesen a fegyverirányítási, illetve az előre jelző rendszerek. Ezeknek a rendszereknek az üzemszerű működéstől való eltérése különleges jogrendi, valamint békeidőszakban is jelentős problémát okozhat. Ennek oka az, hogy „[a]mennyiben ezek közül a rendszerek közül néhány kiesik, vagy működésében sérül akár időlegesen is, az beláthatatlan következményekkel jár a társadalom említett funkcióinak ellátásában. […] hogy egy-egy rendszer vagy rendszerelem kiesésének másik rendszerre gyakorolt valamennyi hatása csak nagyon nehezen jelezhető előre teljes bizonyossággal".[33]

Napjainkban erre az egyik legjobb példa a Colonial Pipeline-incidens. Egy zsaroló vírussal végrehajtott kibertámadás miatt egész üzemanyagvezeték-hálózatát lezárta a Colonial Pipeline vállalat. Ez a fosszilisenergia-hordozó rendszer az Amerikai Egyesült Államok keleti partvidékének közel felét látja el vezetékein keresztül.[34] A zsaroló vírus működése és az okozott gazdasági károk elemzése nélkül is látható, hogy egy ilyen *malware*-típus komoly károkat tud okozni, főleg, hogy a hajtóanyag, a benzin és a gázolaj kiesése jelentősen hátráltathat egy katonai műveletet. Így megállapítható, hogy a zsaroló vírusokkal is hatékonyan lehet akadályozni egy támadó katonai műveletet vagy a haderő logisztikai rendszerét. Ebben az esetben persze nem beszélhetünk szó szerinti pusztításról, de az is egyértelmű, hogy precízen kivitelezett támadás zajlott le, hiszen emiatt az üzemanyag-szállítás az egész hálózaton leállt, és a vállalat informatikai rendszerét is részben le kellett kapcsolni.[35.]

A Colonial Pipeline esetében ráadásul az információs rendszerben közvetett károk is keletkeztek, mivel nemcsak támadásról volt szó, hanem nagy méretű

[32] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16.

[33] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 212.

[34] Megközelítőleg 9000 kilométeres vezetékhálózatán benzint, gázolajat, repülőgép-hajtóanyagot és egyéb finomított kőolajszármazékokat szállít, napi mintegy 2,5 millió hordó mennyiségben.

[35] Andrew Ginter: Ransomware Targets Largest Gasoline Pipeline in USA. *Waterfall,* 2021. május 10.

adatlopásról is. Amint azt már említettem, az információs rendszerek elleni támadásnak több területet is érintő, rendszereken átívelő hatása van.[36]

A támadók jelezték közleményükben, hogy az eltulajdonított adatok között a vállalat szállításainak teljes listája, köztük a hadászati célúak is szerepeltek, amelyekből következtetni lehet az Amerikai Egyesült Államok műveleti képességeire is (katonai logisztika). A gazdasági károk szintén jelentősek voltak, hiszen az Amerikai Egyesült Államok adminisztrációja a támadás után vészhelyzeti rendelkezést adott ki, amely engedélyezi, hogy a kőolajszármazék-szállításban részt vevő logisztikusok többet dolgozzanak a normális üzemszerű időnél, a szállítás zavartalanságának biztosítása érdekében.[37] A vezetékrendszer nagyságából arra is lehet következtetni, mekkora gazdasági kár érte napi szinten a vállalatot. A támadás és a leállás ráadásul nemzetközi viszonylatban is jelentős kiesést jelentett, mert a Brent olaj[38] és más termékek ára emelkedni kezdett, ahogy a szolgáltatók igyekeztek más forrásból beszerezni a kiesést.

A támadások 2021-ben egyre nagyobb számban fordulnak elő. A közlekedési rendszerek szintén ilyen támadás alatt állhatnak, és egyes esetekben az elkövetők nem kiberbűnözők, hanem államilag finanszírozott csoportok. 2021. július 10-ei sajtóinformációk szerint például az iráni közlekedési minisztérium informatikai rendszerét kibertámadás érte. A támadás során az iráni vasúthálózat forgalomfigyelő rendszereleme nem működött üzemszerűen, valamint a vasúti forgalomban is fennakadások jelentkeztek. Az Iranian Students News Agency (ISNA) szerint viszont nem történt olyan méretű támadás, amely befolyásolta volna a személy- és teherszállítást, valamint a nemzetközi vasúti forgalmat. Ezzel szemben a Fars hírügynökség képein látható, hogy a vasúti menetrendkijelzőkön számos késést mutatnak.[39] Az eset információs műveletekhez való tartozását jelzi, hogy a késések alatti telefonszám állítólag Irán egyházi vezetőjének, az ajatollahnak a magántelefonszáma volt.

[36] Joe Panettieri: Colonial Pipeline Ransomware Attack Timeline and Status Updates. *MSSP Alert,* 2021. június 7.

[37] The White House: *Remarks by President Biden on the Colonial Pipeline Incident* (2021. május 13.).

[38] Globálisan megközelítőleg 200 féle kőolaj létezik, ezek közül egyes fajták az úgynevezett *„marker"* olajok. Ezek egyike a Brent-típusú kőolaj, amely az északi-tengeri kőolajnak felel meg.

[39] Cyber-Attack' Hits Iran's Transport Ministry and Railways. *The Guardian,* 2021. július 11.

SCADA

A létfontosságú infrastruktúrákat vezérlő rendszerek már több esetben estek áldozatul *malware*-ekkel végrehajtott támadásoknak. Az ilyen típusú támadások jellemzője, hogy magasan képzett programozók hajtják végre, akik jártasak a PLC-programozásban, valamint jól ismerik az ICT-rendszereket[40] és a támadásban érintett iparágat.

A támadások célja, hogy a rendszert üzemszerű működésétől eltérítsék, vagy olyan paramétereket adjanak meg az egyes üzemi eszközöknek, amelyek következtében fizikai károsodás éri a hálózatot vagy magát az eszközt. Például téves adatokat adnak meg a vezérlőrendszernek, vagy a szenzorok alapértékeit állítják át.

A SCADA esetében is meg kell jegyezni azt, hogy ezek a rendszerek több technológiát ötvöznek. Az ilyen rendszerek sokkal sérülékenyebbek a *malware*-ekkel szemben, hiszen a támadóknak lehetőségük van több ponton is bejutni. Ilyen lehet az ICT-sérülékenység, a tévesen beállított protokoll vagy a napjainkban egyre jobban terjedő szolgáltatási láncba beágyazott támadás is, ahogy azt a korábbiakban olvashattuk. Mivel az információs és kommunikációs technológia komplex, globálisan elosztott és összekapcsolt ellátásilánc-rendszereken alapul, ezért

> „az ICT-ellátásilánc-kockázatok magukban foglalhatják hamisítások beillesztését, jogosulatlan gyártást, hamisítást, lopást, rosszindulatú szoftverek és hardverek beillesztését, valamint az ICT-ellátási lánc rossz gyártási és fejlesztési gyakorlatait. Ezek a kockázatok azzal járnak, hogy a szervezet rálátása és megértése csökken az általuk megszerzett technológiák fejlesztésének, integrálásának és bevezetésének módjáról."[41]

Egy cikk 2009-ben már arra hívta fel a figyelmet, hogy a SCADA-rendszerek távközlési összeköttetése, valamint hálózatba szervezése súlyos biztonsági kockázatot jelent az egész infrastruktúrára nézve, valamint hogy a klasszikus értelemben vett ICT-védelmi megoldások egyáltalán nem védenek a speciálisan SCADA-ra tervezett *malware*-támadások ellen. Például egy SCADA-specifikus *malware* ellen az ICT-védelmi eljárások teljesen hatástalanok. A cikk szerint

[40] Information Communication Technologies.

[41] Deák Veronika (szerk.): *Kibertéri fenyegetések. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára*. Budapest, Nemzeti Közszolgálati Egyetem, 2020. 55.

a kísérleti tesztek alapján a rosszindulatú programok képesek voltak teljesen kijátszani a hagyományos biztonsági mechanizmusokat. A fertőzés *ad hoc* jellege miatt a program hatékonyan megfertőzte a jelentősebb szenzorokat és jelző egységeket.[42]

Hadiipari kémkedés

Míg egyes kártékony szoftvereket arra készítenek fel, hogy látványos – esetleg sajtóvisszhangot keltő – fizikai pusztítást okozzanak, addig más szoftvereket amiatt hoznak létre, hogy a megfertőzött rendszerben megbújva hosszabb ideig adatot szerezzenek. A védelmi szektor viszonylatában ezek a szoftverek nagy biztonsági kockázatot jelentenek. Az esetek többségében ezekkel a szoftverekkel hadiipari beszállítókat, honvédelmi érdekeltségű fejlesztő intézeteket céloznak meg. Itt a cél a hosszan tartó rejtett jelenlét és a maximális adatkinyerés. Kiemelten olyan technológiát érintő dokumentumok eltulajdonításáról van szó, amelyek valamilyen katonai célú fejlesztést is érintenek. Hiszen sokkal gyorsabb és költséghatékonyabb ellopni egy katonai eszköz dokumentációját és terveit, mint kifejleszteni ugyanezt.

Emellett nemcsak a fejlesztés területén jelentősek ezek az információk, hanem védelmi területen is. Hiszen egy offenzív technológiáról előzetesen megszerzett információk nagyban segítik a felkészülést a technológia ellen, ha már rendelkezünk előzetesen ellopott tervezetekkel. A FireEye 2016-os elemzése is rámutat arra, hogy az államilag finanszírozott hackercsoportok is ezeket az információkat keresik, amivel elsősorban az állam által működtetett védelmi rendszer fejlesztését tudják támogatni.

Globális viszonylatban – sajtóinformációk és internetbiztonsági vállalatok szerint – a kínai kormányhoz köthető hackercsoportok jelentik ezen a területen a legnagyobb kockázatot. Az ellopott dokumentációkat a haderőfejlesztés során használja fel a kormány, valamint ezek a támadások az úgynevezett előzetes felderítő tevékenység részét is képzik, amelyeket a későbbiekben továbbfejlesztenek, és még több érzékeny adatot tudnak eltulajdonítani.

[42] Igor Nai Fovino et al.: An Experimental Investigation of Malware Attacks on Scada Systems. *International Journal of Critical Infrastructure Protection,* 2. (2009), 4. 139–145.

A védelmi ipari szektor információs rendszereit számos kártevő veszi célba. A teljesség igénye nélkül a legjelentősebb védelmi szektort érintő *malware*-ek: a GhOst RAT, a PcClient, a ZXShell, az NS01, a WITCHCOVEN.[43]

A védelmi szektor információs rendszerei napjainkban is támadás alatt állnak.[44] A Mandiant jelentése szerint ezt a szektort 2020-ban nemcsak a kínai kormány, hanem az észak-koreai vezetés által finanszírozott csoportok is célba vették. Céljuk, hogy az Amerikai Egyesült Államok védelmi és légügyi információs rendszeréből érzékeny adatokat tulajdonítsanak el.[45]

Dél-koreai sajtóinformációk szerint feltételezhetően észak-koreai elkövetők a Korea Aerospace Industries (KAI) repülőgépipari vállalat informatikai rendszeréből eltulajdonították a KF-21 (HAWK)[46] típusú vadászrepülőgép minősített tervét.[47] A Daewoo vállalatot hasonló kár érte az elmúlt időszakban, amely során feltehetően észak-koreai hackerek érzékeny adatokat távolítottak el a vállalat szervereiről.

Kitekintés

A fokozódó kibertámadások és a kiberbűnözői tevékenység Európában és globálisan is – párhuzamosan a katonai incidensekkel – egyre gyakoribbá és egyre komplexebbé válik. Ez a tendencia várhatóan tovább fog erősödni, mivel 2024-re megközelítőleg 22 milliárd készülék kapcsolódik majd az internetre (*Internet of Things:* IoT).

Ezeknek a támadásoknak egy része közvetlenül vagy közvetve is érinteni fogja a katonai információs hálózatokat. Nem beszélve arról, hogy ezen információs hálózatok egy része a jövőben az IoT-eszközökre is épülhet. Hiszen a polgári technológiák is megjelennek a katonai technológiák között, például a DIoT- eszközök *(Defence Internet of Things)* csoportjába tartozó WINLANS-rendszer[48] a városi harcászati rendszereket támogatja majd a későbbiekben.[49]

[43] FireEye: *Cyber Threats To The Aerospace And Defense Industries.* 2016

[44] FireEye: *FireEye-Mandiant Special report: M-Trends 2021.* 2021.

[45] CuteLoop-kampány.

[46] Ismertebb nevén KF-21 Boramae.

[47] Elizabeth Shim: Maker of South Korea's Kf-21 Indigenous Fighter Hacked. *UPI.com*, 2021. június 30.

[48] WINLANS: Wireless Sensor Networks for urban Local Areas Surveillance.

[49] Ignacio Montiel-Sánchez: *Defence Internet of Things (DIOT).* European Defence Matters, (é. n.).

A hálózati és információs rendszerek biztonságáról szóló európai irányelv 2016-ban lépett életbe, és az első olyan, unió területén alkalmazandó jogalkotási intézkedést jelenti, amelynek célja, hogy elmélyítse a tagállamok közötti kiberbiztonsági tevékenységekre vonatkozó együttműködést a létfontosságú rendszerek területén.

Az irányelv meghatározza az alapvető szolgáltatásokat nyújtó gazdasági szereplők és a digitális szolgáltatók biztonsági kötelezettségeit. Az Európai Bizottság 2020 decemberében javaslatot tett a 2016-os irányelv helyébe lépő módosított kiberbiztonsági irányelvre.[50] Az új szabályok szerint szigorítani fogják a vállalkozások biztonsági kötelezettségeit, fokozzák az ellátási láncok biztonságát, szigorúbb felügyeleti intézkedéseket fognak bevezetni a nemzeti hatóságok számára, tovább fokozzák majd az információmegosztást és az együttműködést. A javaslatot a fejezet írásának idején a Tanács tárgyalja.

Az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) új uniós kiberbiztonsági stratégiát terjesztett elő 2020 decemberében. A cél, hogy megerősödjön az európai információs infrastruktúra a kiberfenyegetésekkel szemben. Az új stratégia konkrét javaslatokat tartalmaz szabályozási, beruházási és szakpolitikai eszközök bevezetésére. A tanúsítás[51] alapvető szerepet játszik az IKT-termékek és -szolgáltatások, valamint -folyamatok magas szintű kiberbiztonságának biztosításában.[52]

Az Európai Unió és tagállamai határozottan egy olyan nyitott és stabil, valamint biztonságos kibertér létrejöttét támogatják, amelyben megvalósul az emberi jogok, az alapvető szabadságok és a jogállamiság tiszteletben tartása. Emellett a társadalmi stabilitást, a gazdasági növekedést, a jólétet és a szabad és demokratikus társadalmak integritását kívánják elősegíteni.

Az EU nagy erőfeszítéseket tesz annak érdekében, hogy megvédje magát az ellenérdekeltségű országokból érkező kibertámadásokkal szemben. Erre jó lehetőséget nyújtanak a közös uniós intézkedések, azaz a kiberdiplomácia eszköztára, amelynek eleme többek között a diplomáciai együttműködés és párbeszéd, a kibertámadások megelőzését célzó intézkedések, valamint ezek szankcionálása. Az Európai Bizottság és az EKSZ által 2020 decemberében elfogadott

[50] NIS 2 irányelv.

[51] European Commission: *Shaping Europe's Digital Future. The EU Cybersecurity Certification Framework*. 2021.

[52] Az egyes uniós országok jelenleg más-más biztonsági tanúsítási rendszereket alkalmaznak, és ez a piac széttöredezettségéhez és szabályozási akadályokhoz vezet. Európai Tanács: *Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket?* 2021.

uniós kiberbiztonsági stratégia megerősíti a kibertámadásokra adandó uniós diplomáciai válaszintézkedéseket.

A Tanács 2019 májusában létrehozta a jogszabályi keretet, amely lehetővé teszi az unió számára, hogy célzott szankciókat vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek kívülről érkező fenyegetést jelentenek a tagállamokra. Ez lehetővé teszi, hogy szankciókat vessen ki olyan támadókra, akik kibertámadásokért felelősek, akik esetleg pénzügyi, technikai vagy anyagi támogatást nyújtanak ilyen támadásokhoz, vagy akik azokban egyéb módokon közreműködnek. Itt számos kérdés is felmerülhet, például, hogy a támadókat hogyan és melyik szervezet azonosítja hivatalosan, illetve hogyan bizonyítható a tényleges pénzügyi támogatás a gyakorlatban.

A kibertér védelmével kapcsolatos uniós együttműködés az Európai Védelmi Ügynökség (*European Defence Agency:* EDA) tevékenységeinek keretében, az Európai Uniós Kiberbiztonsági Ügynökség (*European Union Agency for Cybersecurity:* ENISA) és a European Police Office (EUROPOL) részvételével zajlik. Az EDA segítséget nyújt a tagállamoknak ahhoz, hogy szakképzett katonai kibervédelmi személyzettel rendelkezzenek, és biztosítja a proaktív és reaktív kibervédelmi technológia meglétét.[53]

A 2020 decemberében a Bizottság és az EKSZ által elfogadott uniós kiberbiztonsági stratégia a következőket kívánja megerősíteni:

– a kibervédelem koordinálása,
– az együttműködés és a kibervédelmi képességek kiépítése.

Összefoglalás

A szőnyegbombázás-szerű kibertámadások és a precíziós *malware*-ek elleni védekezés fokozása ma már nemcsak a polgári vagy kereskedelmi/ipari szektort érinti, hanem jelentős kockázati tényezőként jelenik meg a katonai információs rendszerek vonatkozásában is.

Emiatt szükségessé vált a kiberreziliencia növelése, a kiberbűnözés elleni fellépés, a kiberdiplomáciai tevékenység fokozása. Emellett prioritássá vált a kibervédelem folyamatos erősítése, valamint a meglévő rendszerek revíziója is. Az előbbiekben említett feladatok mellett fokozni kell a kutatást és az inno-

[53] EDA: *Cyber Defence Summary: Training & Exercises.* 2021.

vációs tevékenységet, valamint kiemelten kell kezelni a létfontosságú infrastruktúra védelmét.

Véleményem szerint a katonai információs rendszerek vonatkozásában jellemzően a precíziós *malware*-ekkel végrehajtott támadások lesznek a mérvadók az elkövetkező években. Mivel maguk a katonai információs rendszerek is egyre több elemből és alrendszerből állnak majd, valamint ezek komplex és összekapcsolt hálózatokat alkotnak, csak olyan kibertámadások lehetnek hatékonyak, amelyek olyan *malware*-eket használnak, amelyeket a célba vett rendszerre írtak.

Irodalomjegyzék

Deák Veronika (szerk.): *Kibertéri fenyegetések. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára*. Budapest, Nemzeti Közszolgálati Egyetem, 2020. Online: https://bit.ly/3I7EeVN

Dragos Inc.: *Industrial Control System Threats.* 2019. február 14. Online: www.dragos.com/resource/dragos-releases-industrial-control-systems-2018-year-in-review-reports/

EDA: *Cyber Defence Summary: Training & Exercises.* 2021. Online: https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

EnigmaSoft: *'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline.* Online: www.enigmasoftware.com/malware-service-market-booms-prices-malware-botnet-tools-decline/

Európai Tanács: *Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket?* 2021. Online: www.consilium.europa.eu/hu/policies/cybersecurity/

European Commission: *Shaping Europe's Digital Future. The EU Cybersecurity Certification Framework.* 2021. Online: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

FireEye: *Cyber Threats to The Aerospace And Defense Industries.* 2016. Online: www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf

FireEye: *FireEye-Mandiant Special Report: M-Trends 2021.* 2021. Online: https://content.fireeye.com/m-trends/rpt-m-trends-2021

Fovino, Igor Nai et al.: An Experimental Investigation of Malware Attacks on Scada Systems. *International Journal of Critical Infrastructure Protection,* 2. (2009), 4. 139–145. Online: https://doi.org/10.1016/j.ijcip.2009.10.001

Franzetti, Davide: Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON. *Security Boulevard,* 2019. február 26. Online: https://securityboulevard.com/2019/02/oil-gas-cybersecurity-and-process-safety-converge-thanks-to-triton/

Ginter, Andrew: Ransomware Targets Largest Gasoline Pipeline in USA. *Waterfall,* 2021. május 10. Online: https://waterfall-security.com/ransomware-targets-largest-gasoline-pipeline-usa/

Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.

Johnson, Derek B.: Threatneedle Malware Tied to Year-Long North Korean Espionage Campaign Against Global Defense Industry. *Scmagazine,* 2021. február 25. Online: www.scmagazine.com/news/apt/threatneedle-malware-tied-to-year-long-north-korean-espionage-campaign-against-global-defense-industry

KasperskyLab: Malware-as-a-service (MaaS). Online: https://encyclopedia.kaspersky.com/glossary/malware-as-a-service-maas/

Katz, Justin: Cisa Issues Warning on Exploited VPN Flaw. *GCN.com,* 2021. április 23. Online: https://gcn.com/articles/2021/04/23/cisa-supernova.aspx

Kopeytsev, Vyacheslav – Seongsu Park: *KasperskyLab ICS CERT Lazarus Targets Defense Industry with ThreatNeedle.* Kaspersky ICS CERT, 2021. február 25. Online: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Lazarus-targets-defense-industry-with-Threatneedle-En.pdf

Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018.

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/3780

Kramer, Simon – Julian C. Bradfield: A General Definition of Malware. *Journal in Computer Virology,* (2010), 6. 105–114. Online: https://doi.org/10.1007/s11416-009-0137-1

Malware in Modern ICS. Understanding Impact While Avoiding Hype. *Power,* 2017. május 1. Online: www.powermag.com/malware-in-modern-ics-understanding-impact-while-avoiding-hype/

Mangan, Dan: North Korean Hackers Charged in Massive Cryptocurrency Theft Scheme. *CNBC,* 2021. február 17. Online: www.cnbc.com/2021/02/17/north-korean-hackers-charged-in-massive-cryptocurrency-theft-scheme.html

Montiel-Sánchez, Ignacio: *Defence Internet of Things (DIOT).* European Defence Matters, (é. n.). Online: https://eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)

NATO e-Library: *Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales.* 2014.

NATO e-Library: *Warsaw Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw.* 2016.

Panettieri, Joe: Colonial Pipeline Ransomware Attack Timeline and Status Updates. *MSSP Alert,* 2021. június 7. Online: www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/

Shim, Elizabeth: Maker of South Korea's Kf-21 Indigenous Fighter Hacked. *UPI.com*, 2021. június 30. Online: www.upi.com/Top_News/World-News/2021/06/30/skorea-South-Korea-KAI-aerospace-hack/5591625059379/

Cyber-Attack' Hits Iran's Transport Ministry and Railways. *The Guardian,* 2021. július 11. Online: www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways

The White House: *Remarks by President Biden on the Colonial Pipeline Incident* (2021. május 13.). Online: www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/

Yoon, Lin: Kim Jong Un Acknowledges Food Crisis in North Korea. *Hrv.org,* 2021. június 17. Online: www.hrw.org/news/2021/06/17/kim-jong-un-acknowledges-food-crisis-north-korea