4. fejezet

Hírszerzés a kibertérben

Deák Veronika

Bevezetés

A technológia rohamos fejlődésének következtében a kibertámadások száma folyamatosan nő. Emellett egyre komplexebb és kifinomultabb támadások jelennek meg, amelyek eredményes elhárításához elengedhetetlen a mögöttes cél, a motiváció, valamint a támadási alternatívák mélyebb ismerete.

Az elmúlt években számos olyan eset látott napvilágot, amelyben állami szervek kerültek a kibertámadások középpontjába. A különféle elektronikus információs rendszerek vagy szolgáltatások működésének korlátozásától kezdve az anyagi haszonszerzésen át egészen a bizalmas információk megszerzéséig bezárólag számtalan motiváció azonosítható a támadások hátterében.

A központi, állami szerveket célzó támadások sok esetben az adott államra vonatkozó belső és bizalmas információk megszerzésére irányulnak, a saját nemzeti érdekek védelme, érvényesítése és támogatása céljából. Ezen támadások vonatkozásában kiemelt figyelmet kell fordítani a katonai hírszerzést megvalósító kibertámadásokra, hiszen segítségükkel számtalan hasznos információ megszerezhető az adott ország céljairól, szándékairól, alapvető működéséről, erőforrásairól és védelmi mechanizmusairól, amely a későbbiekben egy esetleges katonai művelet során eredményesen felhasználható. A hagyományos és a kiberhadviselésben egyaránt fölényt jelent a megfelelő mennyiségű és minőségű információ megszerzése, hiszen nemcsak az ellenséges félről szerezhetők meg hasznos információk, hanem a saját védelmi képességek hatékonysága és eredményessége is jelentősen fejleszthető, aminek következtében a hírszerzés stratégiai és taktikai előnyt is jelenthet a saját erők számára.

A kibertérben megvalósuló katonai célú hírszerzés már az 1980-as években megjelent, azonban a technológia fejlődésével a hírszerző módszerek is folyamatosan változnak. Így például az ötödik generációs technológia, az IoT-eszközök, a mesterséges intelligencia új hírszerző támadási technikák megjelenéséhez vezet. Éppen ezért elengedhetetlen a már rendelkezésünkre álló módszerek

https://doi.org/10.36250/01079_04

működési mechanizmusának megismerése, azok fejlődési jellemzőinek azonosítása a jövőbeli változások hatékony előrejelzése érdekében.

Jelen fejezet célja az elmúlt évtizedek legjelentősebb katonai célú hírszerző támadásainak azonosítása és elemzése. A támadások elemzése során megvizsgáljuk, hogy miért lehettek sikeres támadások, illetve mitől váltak meghatározó esetté a történelemben. Bemutatjuk, hogy az idő előrehaladtával és a technika fejlődésével miképpen változtak meg a támadások motivációi és célpontjai.

A kibertámadások természetesen válaszlépéseket indukálnak, amelyek során különböző, a kibervédelmi képességek nemzeti szintű fejlesztését nagyban befolyásoló védelmi stratégiai lépések jelentek meg. Mindezek miatt jelen fejezet további célja, hogy a nevezett hírszerzést célzó kibertámadások tapasztalatain alapuló legfontosabb kibervédelmi eszközöket, eseményeket, mechanizmusokat is bemutassa.

Végül egy esetleges előrejelzés keretében ismertetjük, hogy a katonai hírszerzés milyen irányokat és célokat tűzhet ki maga elé az elkövetkezendő néhány évben és évtizedben.

Alapfogalmak

A kibertérben megvalósuló katonai hírszerzés főbb eseményeinek feltárásához, a hírszerző, felderítő technikák elemzéséhez elengedhetetlen a hírszerzéssel összefüggő főbb definíciók áttekintése. Jelen fejezet olyan hírszerzésre alkalmas támadások feltárását és elemzését tűzte ki célul, amelyek végrehajtása a kibertérben zajlott le.

Ahogy azt az előző fejezetekben láthattuk, a kibertérnek számos definíciója létezik, aszerint, hogy milyen aspektusból vizsgáljuk azt. Szempontok lehetnek akár a kibertér térgeometriai jellemzői, az egyén, a társadalom, a gazdaság és a kibertér viszonya is. Donna Haraway szerint a kibertér nem az információ szállítására, feldolgozására van a legnagyobb hatással, hanem a társadalmi viszonyok, kapcsolatok alakulására.[1] Általában az a vélemény, hogy az egész világra kiterjedő, globalizáló közeget bárhonnan el lehet érni, ha rendelkezésre áll a technikai apparátus és az annak működtetéséhez szükséges pénz. A kibertér

[1] Donna Haraway: A Cyborg Manifesto: Science, Technology and Socialist-Feminism in the Last Twentieth Century. In Donna Haraway: *Simians, Cyborgs and Women: The Reinvention of Nature.* New York, Routledge, 1991. 149–181.

használatával együtt járó társadalmi, politikai és gazdasági előnyök a hagyományos térbeli és társadalmi megoszlások mentén helyezkednek el, hiszen az internetes hozzáférés nagy területi és társadalmi egyenlőtlenségeket okoz.[2] Egy másik megfogalmazás szerint az elektronikus információs rendszerek és infrastruktúrák, valamint az ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét nevezzük kibertérnek.[3] A *Nemzeti Kiberbiztonsági Stratégia* szerint a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.[4] Ebben a fejezetben a *Nemzeti Kiberbiztonsági Stratégia* meghatározása alapján választottuk ki a hírszerzésre alkalmazott kibertámadásokat.

A kibertér fogalmának vizsgálata azért is szükségszerű, mert a 2016 júliusában megrendezett varsói NATO-csúcstalálkozón hivatalosan deklarálták, hogy a kibertér az ötödik hadszíntérnek tekinthető.[5] Ennek oka, hogy a NATO szerint a számítógépes támadások jelentős kihívást jelentenek a szövetség tagjainak biztonságára nézve, és hatásaikat tekintve ugyanolyan károsak lehetnek, mint a korábbi négy fizikai dimenzióban (szárazföldi, légi, tengeri, kozmikus) végrehajtott hagyományos támadások.[6] Erről szintén részletesen szóltunk az 1. fejezetben.

A hírszerzés és a felderítés fogalmának tisztázása elengedhetetlen a kibertérben megvalósuló katonai hírszerzés vizsgálata során, hiszen gyakran egymás szinonimáiként is használják e definíciókat, köszönhetően annak, hogy mindkét kategória hasonló tevékenységet és célt foglal magában, továbbá a nemzetközi szakirodalomban az *intelligence* szó jelenik meg, amely felderítésként és hírszerzésként egyaránt fordítható.[7]

[2] Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 48. (108.) (2001), 7. 769–779.

[3] Mészáros (2001): i. m.

[4] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[5] *State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016.* Press Release 100. North Atlantic Treaty Organization, 2016. július 9.

[6] Kovács László: *Biztonságpolitika: a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

[7] Füzesi Ottó: *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésére.* Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2004.

A *Magyar Hadtudományi Lexikon* szerint a hírszerzés „a titkosszolgálati tevékenység egyik alapvető szolgálati ága, amely külföldi bizalmas politikai, gazdasági, technikai, tudományos, katonai híranyagok, adatok, információk tervszerű gyűjtését, elemzését, értékelését végzi nyílt és titkosszolgálati erőkkel, eszközökkel, módszerekkel".[8]

Egy másik megfogalmazás szerint a hírszerzés az állam egyik funkciójaként értelmezhető, amelynek célja a nemzeti érdekek védelme és érvényre juttatása az erre a feladatra létrehozott, közvetlenül a kormányzati irányítás alatt működtetett szervezetek által végrehajtott titkos és nyílt forrású információk megszerzése által.[9] Fontos kiemelni, hogy jelen meghatározás a hírszerzés bizonyos területét jelöli, hiszen fejlődésének köszönhetően a társadalom számos szegmensében megtalálható (például gazdasági, politikai hírszerzés).[10]

Az állam a hírszerző tevékenység végrehajtására hírszerző szervezeteket (szolgálatokat, hivatalokat) működtet, amelyek célja, hogy megfelelő információkkal támogassák a döntéshozatalt. A hírszerző szolgálatok katonai és polgári hírszerző tevékenységet folytatnak. A hírszerzés tevékenységi rendszere magába foglalja az adat- és információszerzést, az elemzés-értékelést, valamint a hírszerző műveletek végrehajtását. Ezen tevékenységek folyamatos kölcsönhatásban vannak, egymással elválaszthatatlan egységet képezve.[11]

A katonai hírszerzés a katonai felderítő szervek által békeidőben és háborúban folytatott megszakítás nélküli tevékenység, amelynek célja az ellenséges vagy várhatóan ellenséges ország, állam katonapolitikai helyzetére, hadigazdasági potenciáljára, fegyveres erőire, valamint a hadszínterekre vonatkozó adatok megszerzése és elemzése.[12]

A polgári hírszerzés feladata az ország elleni politikai és gazdasági törekvések feltérképezése, valamint a kormányzat külpolitikai és külgazdasági érdekeinek érvényesítése, támogatása.[13] Mindezek megvalósítását bizalmas információk megszerzésével segíti elő, amelyek a politikai és kormányzati döntések meghozatalához elengedhetetlenek.

[8] *Magyar Hadtudományi Lexikon.* Budapest, Magyar Hadtudományi Társaság, 1995. 558.

[9] Izsa Jenő: A hírszerzés céljáról és rendszeréről. *Hadtudomány,* 19. (2009), 1–2. 72.

[10] Dobák Imre: *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2014.

[11] Dobák (2014): i. m.

[12] *Magyar Hadtudományi Lexikon* (1995): i. m.

[13] Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere. (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására.) *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100.

A felderítés a *Hadtudományi Lexikon* értelmezése szerint:

> „az állami apparátus vezető szervei és a különböző szintű parancsnokságok azon intézkedéseinek, rendszabályainak és tevékenységeinek összessége, amelyek egy ország vagy országcsoport érdekeiről, célkitűzéseiről, szándékáról, terveiről, tevékenységéről, erőforrásairól, helyzetéről, fegyveres erőinek felépítéséről, csoportosításáról, haditechnikájáról, kiképzettségi helyzetéről és a hadszíntérré váló terület előkészítéséről szóló adatok megszerzését, gyűjtését, tanulmányozását célozzák."[14]

Ezek alapján a felderítés a katonai műveletek támogatásán belül értelmezhető tevékenység, amely magában foglalja a vezetéshez szükséges ellenségre, terepre és egyéb tényezőkre vonatkozó adatok, információk megszerzését, feldolgozását és elemzését.[15]

A kibertérben megvalósuló hírszerzés során érdemes megemlíteni a számítógép-hálózati műveletek fogalmát, amely a másik fél hálózatos számítógépes rendszerei felderítésére, adatok megszerzésére, működésük korlátozására, akadályozására, befolyásolására irányul a számítógép-hálózati felderítés és támadás módszereivel, továbbá mindemellett a saját hasonló hálózatok működését biztosítja.[16]

A hírszerzés alapjául szolgáló lehetséges kiberműveletek

A következőkben néhány lehetséges kibertérben megvalósuló, a hírszerzés alapjául szolgáló, az elmúlt néhány évtizedben jellemző kiberműveleti technika definícióját mutatjuk be.

A *zero-day exploit,* más néven nulladik napi támadás egy olyan biztonsági rés, sebezhetőség, amelyet még azelőtt képes kihasználni a támadó, mielőtt felfedezték vagy nyilvánosságra hozták volna azt.[17]

A DoS *(denial of service),* más néven *szolgáltatásmegtagadással járó támadás* lényege, hogy olyan sok kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal már nem tud feldolgozni. Ennek következtében nem lesz elérhető a szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver.[18] A támadás irányulhat a célpont

[14] *Magyar Hadtudományi Lexikon* (1995): i. m. 339.
[15] Börcsök–Vida (2014): i. m.
[16] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.
[17] Animesh Kumar: Zero Day Exploit. *SSRN,* 2014. január 14.
[18] Fehér Krisztián: *Kezdő hackerek kézikönyve*. Budapest, BBS-INFO, 2016. 202–204.

hálózati kapcsolatának vagy a célpont rendszerben működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére, amely során a támadó célja a célpont erőforrásainak lefoglalása.[19]

A *hátsóajtó*-alkalmazás *(backdoor)* a felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nemcsak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti.[20]

A *vírus* rosszindulatú program, amely jellemzően saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A rendszerbe a felhasználó engedélye nélkül kerül be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD-kártya, merevlemez, MP3- és videólejátszó, mobiltelefon stb.) vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölhetik vagy módosíthatják, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nemcsak adathordozó eszközök által terjedhetnek, hanem elektronikus levelezés során az üzenetek részeként (például csatolmányként), vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is.[21]

A *trójai programok* látszólag vagy akár valójában is hasznos funkciókat látnak el, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak, könyvtárakat vagy adatállományokat törölnek. Tehát a program a felhasználó tudta nélkül a háttérben nem kívánt műveleteket is végrehajthat, mint például vírustelepítés, titkos információk megszerzése (például banki adatok, jelszavak, PIN-kódok), hátsó ajtó létrehozása vagy akár közvetlen károkozás is.[22]

[19] Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám. 1788–1919.

[20] Deák Veronika: Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14. (2019), 2. 256–271.

[21] Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem, 2012.

[22] Kovács László: Az információs terrorizmus eszköztára. *Hadmérnök,* (2006), különszám.

A *zsaroló program,* más néven *ransomware* célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsaroló programok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló sok esetben kiterjeszti a fizetésre rendelkezésre álló időt, vagy törli az adatokat a felhasználó infokommunikációs eszközéről.[23]

A *social engineering* az ember megtévesztésével, kihasználásával és manipulálásával teszi lehetővé belső és bizalmas információk megszerzését vagy akár egy infokommunikációs eszköz megfertőzését kártékony programmal.

A *whaling* az adathalászat egyik típusa, lefordítva bálnavadászatot jelent; talán azért is, mert a „nagy halakat", vagyis egy szűkebb felhasználói kört, a vállalatok, szervezetek vezetői csoportját célozza. Ennél a technikánál az adathalász üzenetek általában valamely üzleti partnertől vagy állami intézménytől, hatóságtól érkeznek.[24]

Katonai hírszerzés a kibertérben

A katonai hírszerzés már az 1980-as évek kezdetétől jelen van a kibertérben. A technológiai fejlődés következtében pedig ezek a támadások egyre kifinomultabbak a támadás céljait és a végrehajtás módját tekintve.

Szeretnénk időrendi áttekintést nyújtani a leglényegesebb hírszerzési műveletekről és az így azonosítható fejlődési/változási görbéről. Elsősorban megvizsgáljuk a kibertámadások típusainak fejlődését, majd azonosítjuk a támadás létrehozásához és végrehajtásához kapcsolódó erőforrások változását, végül megnézzük, hogy az idő előrehaladtával hogyan változtak meg a hírszerzési műveletek céljai.

[23] Ibrar Yaqoob et al.: The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. *Computer Networks,* 129. (2017). 444–458.

[24] Pavel Y. Leonov et al.: The Main Social Engineering Techniques Aimed at Hacking Information Systems. *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* IEEE, 2021. 0471–0473.

Áttekintés

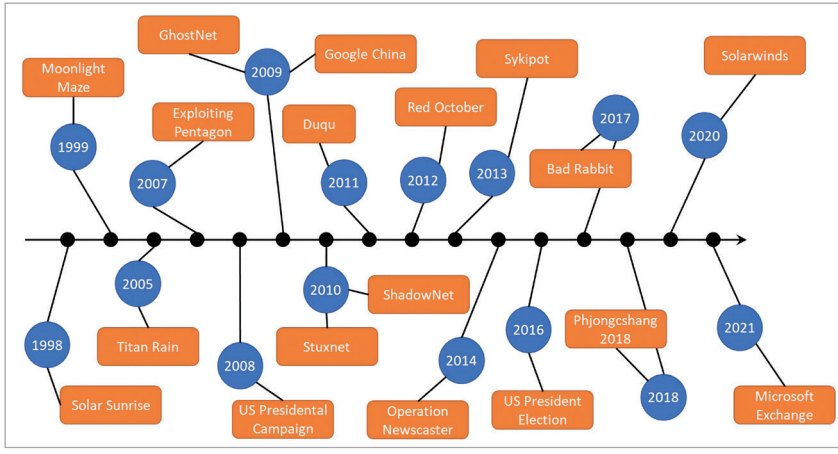
Az első kibertámadások az 1980-as évekre tehetőek, és elsősorban magánszemélyek által készített vírusok voltak, nem kapcsolódtak szorosan a katonai hírszerzéshez. A 80-as évek végén már megjelentek a katonai hírszerzéshez kapcsolódó támadások is, elsősorban az egykori NDK, az Egyesült Államok és a Szovjetunió területén. Az igazi áttörést a 90-es évek vége hozta el, ahol már célzottan történtek hírszerző akciók a kibertérben. Míg a 20. század végén, illetve a 2000-es évek elején még csak évente egy-egy nagyobb horderejű támadást jegyzett fel a történelem, a 2010-es évektől kezdődően havonta rögzítettek újabb és egyedibb támadásokat a világ minden tájáról.

A katonai hírszerzést megvalósító kiberműveletek kapcsán fontos kiemelni az APT- *(Advanced Persistent Threat)* támadásokat is, amelyek folyamatos, tartós kiberbiztonsági fenyegetettséget jelentenek. Ezen támadások végrehajtásáért szervezett kiberbűnözői csoportok felelősek. Az e csoportok által végrehajtott támadások céljai, motivációi és felhasznált eszközei hasonlóak, sok esetben megegyeznek a katonai hírszerző kiberműveletek során alkalmazott módszerekkel, technikákkal. Ilyen csoportok a teljesség igénye nélkül például az alábbiak:

a) *APT1* (Unit 61398 néven is ismert, a kínai hadsereg által felügyelt csoport, amely 2006 óta folytat kiberkémkedési tevékenységet, és erőssége, hogy azonos időben több tucat szervezettől képes volt információkat eltulajdonítani.)
b) *APT4* (Más néven Maverick Panda, Sykipot Group, kínai hátterű, és főként a repülőgépipar, az autóipar, a távközlés, valamint a kereskedelmi szervezetek támadását célozta.)
c) *APT28* (Fancy Bear és Sandworm néven is ismert orosz csoport, körülbelül 2000 óta hajt végre kibertámadásokat elsősorban kormányzati, katonai és biztonsági szervezetek ellen.)
d) *APT29* (Dukes és Cozy Bear néven egyaránt ismert orosz csoport, amely feltételezhetően az orosz Külföldi Hírszerző Szolgálat [SVR] irányítása alatt működik, és számos amerikai, európai és NATO-tagállam kormányzati hálózatait, kutatóintézeteit célzó kibertámadás végrehajtásáért felelős.)
e) *APT35* (Irán által szponzorált csoport, amely 2014 óta elsősorban a Közel-Keleten tevékenykedik, és számos kibertámadás fűződik a nevéhez, amely kormányzati, energia-, közlekedési, technológiai és távközlési szektorokat is érintett.)

f) *APT37* (Észak-koreai, 2012 óta kiberkémkedést végrehajtó csoport, többek között a dél-koreai, vietnámi, japán és közel-keleti közlekedési, egészségügyi, autóipari, repülőgépgyártási szektorokat célozta.)
g) *APT38* (2009 óta aktívan tevékenykedő észak-koreai csoport, amely Lazarus Group néven is ismert; támadásai mögött főként pénzügyi motiváció áll, ennek következtében elsősorban bankokat, pénzügyi intézményeket céloz.)
h) *APT41* (2012 óta aktív, kínai, államilag támogatott kémtevékenységet is végző csoport, amely többek között egészségügyi, távközlési, energia- és technológiai ágazatokat érintő támadásokat hajt végre.)
i) *G0010* (WhiteBear néven is ismert, 2004 óta tevékenykedő orosz csoport, amely már több mint 45 országban fertőzte meg kormányzati, katonai, oktatási, egészségügyi, kutatási szektorok szervezeteit.)[25]

Az *1. ábrán* látható idővonalon a legfontosabb katonai APT- és katonai hírszerzési támadások szerepelnek:



1. ábra: Hírszerzési célú kibertámadások 1998–2021 között
Forrás: a szerző szerkesztése

[25] MITRE ATT&CK: Groups. 2021.

1. táblázat: Az elmúlt évek hírszerzést megvalósító kibertámadásai

1998:	Solar Sunrise	Az eredeti feltevések szerint az amerikai védelmi minisztérium hálózatát támadta meg Irak hírszerzési célból. Később kiderült, hogy egy izraeli mentor irányításával két amerikai tinédzser felelős a támadásért, de emiatt bizonyosodott be, hogy a kritikus infrastruktúrák kibertámadások célpontjai lehetnek. A támadás során számos kormányzati számítógéphez szereztek hozzáférést, közülük 11 az amerikai légierő és haditengerészet bázisain volt megtalálható. A Solar Sunrise arra is figyelmeztetett, hogy a jelentős támadási képességek nem csak szakértők által találhatók meg. Utóbb kiderült, hogy semmilyen titkos anyag nem került ki a minisztérium hálózatából.[26]
1999:	Moonlight Maze	Bár magát az esetet 1999-re datáljuk, mivel a nyomozás ekkor fejeződött be, a kibertámadás már 1996 óta folyamatosan tartott az Egyesült Államok ellen. Érintette többek között a Pentagont, a National Aeronautics and Space Administrationt (NASA), katonai és kormányzati szervezeteket, kutatóintézeteket, egyetemeket, valamint az amerikai Energiaügyi Minisztériumot is. A Moonlight Maze nyílt forráskódú Solaris rendszereket célzó Unix-alapú támadás. A támadás elkövetése Oroszországra, a feltételezések szerint a G0010 vagy más néven Snake csoportra volt visszavezethető, amelynek során több ezer titkos dokumentum vándorolt az egyik nagyhatalomtól a másikhoz.[27]
2005:	Titan Rain	Az előző esethez hasonlóan ebben az esetben is korábban, már 2003 óta zajlott a kibertámadás az Egyesült Államok védelmi hálózatai ellen. A támadások nemzetbiztonsági információk megszerzését tűzték ki célul, a támadóknak számos kormányzati és védett hálózatba sikerült bejutniuk, így például többek között a Pentagon és a NASA rendszereibe is képesek voltak behatolni. A támadásokat Kínáig tudták visszanyomozni, egyes feltételezések szerint az APT1 (Unit 61398) csoport volt az elkövető. Az eset különlegessége, hogy itt már nem egyetlen sérülékenységet használtak ki a támadók, hanem jól megtervezett támadások sorozatát hajtották végre.[28]
2007:	Exploiting Pentagon	Az amerikai védelmi miniszter magán-e-mail-fiókját ismeretlenek törték fel, így képesek voltak a Pentagon hálózataihoz hozzáférni, és titkosított adatokat eltulajdonítani. A feltételezett elkövetők kínai hackerek voltak, azonban a kínai állam ezt hivatalosan tagadta.[29]

[26] Kenneth J. Knapp – William R. Boulton: Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management,* 23. (2006), 2. 76.

[27] Azhar Ushmani: Cyberwarfare History and APT Profiling. Advance Online Publication. *International Journal of Computer Science Trends and Technology (IJCST),* 7. (2019), 4.

[28] Dana Rubenstein: *Nation State Cyber Espionage and its Impacts.* Washington University in St. Louis, 2014. december 1.

[29] Robert N. Charette: DoD Admits to Being Severely Hacked. *IEEE,* 2008.

2008:	Presidential Campaign	A kiberhírszerzés eljutott arra a pontra, ahol már a választások kapcsán is képes volt beleszólni az amerikai politikai játszmákba. 2008-ban mind a demokratikus, mind a republikánus párt kampányához kapcsolódó adatokat tulajdonított el egy kínai hackercsoport.[30]
2009:	GhostNet	A GhostNet összehangolt kibertámadás-sorozat volt, a világ 103 országában működött, és állami, pénzügyi, illetve ipari titkok megszerzését célozta. A GhostNet-rendszer arra irányítja a fertőzött számítógépeket, hogy töltsenek le egy gh0st RAT (remote access tool) néven ismert trójai programot, amely lehetővé teszi a támadók számára, hogy teljes, valós idejű irányítást szerezzenek az eszköz felett. A támadássorozat során kormánytagokat és kormányközeli szervezeteket is megfigyeltek. A megfigyelő kémprogramok mögött Kína állt, és elsősorban a dél-ázsiai országokban ténykedett. Érdekesség, hogy a kémprogramot először a dalai láma számítógépén fedezték fel. A támadássorozat nevét az elkövetőiről, a GhostNet APT-csoportról kapta.[31]
2009:	Google	Kínai hackerek törték fel a Google vállalati szervereit, és hozzáférést kaptak egy olyan adatbázishoz, amely titkos információkat tartalmazott gyanúsítottakról, kémekről, ügynökökről és az amerikai kormány által megfigyelt terroristákról. Ezenkívül a támadók információt szerezhettek az amerikai nemzetbiztonsági és bűnüldöző szervek dokumentumairól, valamint a kapcsolódó titkosszolgálati tevékenység végrehajtásával és ellenőrzésével összefüggő bírósági végzések tartalmáról.[32]
2010:	Shadow-Network	A ShadowNetwork a GhostNet folytatásának tekinthető. Miután a GhostNethez kapcsolódó sérülékenységeket megszüntették, a támadások száma továbbra sem csökkent. Így térképezték fel a ShadowNetworköt, amelynek célja továbbra is elsősorban India vezetőinek megfigyelése, illetve titkos anyagok Kínába továbbítása volt. A kiberhadművelet során a támadók *social media* és felhőszolgáltatásokat biztosító platformokat (Twitter, Google, Yahoo) használtak arra, hogy a vírusokat az áldozatok gépére telepítsék.[33]

[30] Morgan Swartley: Political Marketing: How Social Media Influenced the 2008–2016 US Presidential Elections and Best Practices Associated. *Senior Honors Theses,* 726. 2018. szeptember 4.

[31] Ronald J. Deibert – Rafal Rohozinski: Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor,* 2009. március 29.

[32] Ellen Nakashima: Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say. *The Washington Post,* 2013. május 20.

[33] Steven Adair et al.: *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* A Joint Report of the Information Warfare Monitor and Shadowserver Foundation. Toronto, 2010. április 6.

2010:	Stuxnet	A Stuxnet egy 2010-ben felfedezett féreg volt, amely a hírszerzési tevékenység megvalósítása mellett az iráni nukleáris létesítmények, ipari vezérlők felügyeleti és adatgyűjtési (SCADA) rendszereinek újraprogramozását célozta. A kibertámadáson keresztül konkrét fizikai támadásokat voltak képesek elérni a támadók. A Stuxnet elsődleges célja Irán nukleáris programjának teljes megakadályozása volt. Ennek megvalósítására több nulladik napi sérülékenységet használtak ki a számítógépek megfertőzésére. A fájlok megfertőzésével a féreg hozzá tudott férni a programozható logikai vezérlőkhöz (PLC), amelyeket a számítógépek az ipari eszközök teljesítményének szabályozására használnak. Ezáltal a Stuxnet képes volt az urándúsító centrifugák észrevétlen tönkretételére és a dúsítási folyamat megzavarására. Legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban, és szakértők szerint legalább két évvel vetette vissza az iráni atomprogramot.[34]
2011:	Duqu	A Duqu a korábbi Stuxnet hasonmása, a magyarországi Crysys kutatólaboratórium ismerte fel. Fontos, hogy bár nagyon hasonló kialakítással rendelkezett, mint a Stuxnet, nem volt teljesen ugyanaz. A Duqu egy kifinomult, információszerzésre alkalmas kártékony program. A Duqu Microsoft Windows operációs rendszerek nulladik napi sérülékenységei felhasználásával szerzett meg bizalmas információkat. Újdonságként értelmezhető a Duqu azon jellemzője, hogy a támadások mögött álló szervezetek kapcsolatban állnak egymással, közös belső információs platformmal rendelkezhetnek *zero-day* támadási felületekkel kapcsolatban. A támadás az izraeli Unit 8200 csoporthoz köthető.[35]
2012:	Red October	A Vörös Október nevű vírust az orosz Kaspersky Lab fedezte fel 2012-ben, és állításuk szerint a vírus már 2007 óta gyűjtött információkat Microsoft Excel- és Word-felhasználók gépeiről. A vírus elsősorban nagykövetségeket, diplomáciai szervezeteket, egyetemeket, tudományos kutatást folytató cégeket, ipari és kereskedelmi szervezeteket, repülőgépészeti intézményeket, valamint katonai szervezeteket célzott. A Red October legfőbb célja bizalmas, titkos dokumentumok megszerzése és a megfertőzött hálózatok feltérképezése volt. A vírus előnye, hogy addig ismeretlen metódus alkalmazásával fertőzte meg a számítógépeket, ám a terjedéshez a korábban bevált módszereket, így például adathalász leveleket, fertőzött weboldalakat és Microsoft Office-, PDF-, Java-programok sebezhetőségeit alkalmazta.[36]

[34] Marie Baezner – Patrice Robin: Stuxnet. *ETH Zurich*, 4. (2017).

[35] Bencsáth Boldizsár et al.: Duqu: Analysis, Detection, and Lessons Learned. *ACM European Workshop on System Security (EuroSec),* 2012.

[36] Henry Mwiki et al.: Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. In *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham, 2019.

2013:	Sykipot	A kínai hackerek a Sykipot néven ismert rosszindulatú programmal fertőzték meg az Egyesült Államok kormányzati és védelmi szervezeteit, valamint a piaci szektort is, például banki intézményeket, a távközlést, illetve az energiaszektort. A Symantec szerint a Sykipotot már 2006 óta használták célzott támadásokban. A Sykipot *malware* adathalász e-maileken keresztül terjedt, rosszindulatú csatolmányok vagy linkek útján. A kártékony program lehetővé teszi fájlok feltöltését, letöltését, így bizalmas információk megszerzését vagy további rosszindulatú programok telepítését. A támadás végrehajtásáért az APT4 vagy más néven Sykipot Group volt felelős.[37]
2014:	Operation Newscaster	A támadás során *social engineering* technikák segítségével tudtak támadók eljutni a célszemélyekhez. A bizalom kiépítésére 14 álszemélyt alakítottak ki, akik aktívan részt vettek a *social media* platformokon (Facebook, Twitter, LinkedIn), és folyamatosan publikáltak posztokat saját blogjaikon. Ezáltal valós személyek látszatát keltve kerülhettek fontos emberek közelébe. A támadók a hamis személyek alkotta összetett és összehangolt hálózat támogatására egy konkrét „virtuális rendszert" is felállítottak, és fiktív hírportál (NewsOnAir.org) biztosította az álszemélyek háttértörténeteinek hitelességét. A hálózat létrehozását követően az iráni támadók megkezdték a kapcsolatfelvételt a közigazgatásban, kormányzati szervezetekben dolgozó személyekkel a megfelelő szintű bizalom kiépítése érdekében. A célszemélyekből több mint 2000 fős hálózatot hoztak létre, a megszerzett információk köréről azonban nincs információ.[38]
2016:	President Election Campaign	A támadás célja a 2016-os amerikai választások befolyásolása volt, ahol több e-mail és titkosított dokumentum szivárgott ki. A kiszivárogtatások mögött a választók véleményének befolyásolása volt a feltételezett cél. Az amerikai közvélemény szerint az orosz kormányzat közvetve, információs műveletekkel és az ehhez információt szolgáltató kiberkémkedéssel próbálta befolyásolni az amerikai elnökválasztás eredményét. A támadók e-mail-fiókokat törtek fel, az ott megszerzett információkat nyilvánosságra hozták, továbbá számtalan álhírt jelentettek meg a közösségi médiában. A támadások végrehajtása az orosz APT28 (Cozy Bear) és APT29 (Fancy Bear) csoporthoz köthető.[39]
2017:	WannaCry, NotPetya, BadRabbit	A 2017-es évben kerültek elő először a zsaroló vírusok. Rögtön három híres eset is bekerült a hírekbe: WannaCry, NotPetya és BadRabbit. Céljuk minden esetben a célpontok sérülékenységének vizsgálata, információszerzés és a megtámadott szervezetek működésének korlátozása volt. Feltételezések szerint a WannaCry-támadást az észak-koreai Lazarus csoport, a NotPetya-műveletet pedig az orosz Sandworm csoport hajtotta végre.

[37] Hippolyte Djonon Tsague – Bheki Twala: *Reverse Engineering Smart Card Malware Using Side Channel Analysis With Machine Learning Techniques.* IEEE International Conference on Big Data (Big Data), 2016. 3713–3721.

[38] Gabi Siboni – Sami Kronenfeld: Iranian Cyber Espionage: A Troubling New Escalation. *INSS Insight,* 2014. június 16. 561.

[39] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9.

2018:	False-flag	A Dél-Koreában rendezett téli olimpián használt rendszerekhez, adatbázisokhoz és adatokhoz jutottak hozzá a támadók. A támadás érdekessége azonban leginkább az, hogy mestersségesen Észak-Koreára és Kínára terelték a támadás gyanúját. Az információszerzés mellett a támadóknak sikerült megzavarni az olimpia internetes és televíziós közvetítéseit, valamint leállítani a jegynyomtatási rendszert.[40]
2020:	SolarWinds	A SolarWinds egy amerikai magánvállalat, amelynek szoftverét világszerte rengetegen használták, köztük távközlési vállalatok, katonai és kormányzati szervezetek, így például a Pentagon, a NASA és a National Security Agency (NSA) is. A SolarWinds az Orion nevű szoftverrel támogatja az informatikai hálózatok felügyeletét és kezelését, beleértve az adatok összesítését, elemzését és megjelenítését. A FireEye kezdeti felfedezését követő vizsgálatok azt mutatták, hogy a hackerek már 2019 októberében megfertőzték a SolarWinds Orion szoftverét, lehetővé téve számukra, hogy 2020 márciusában egy szoftverfrissítésen keresztül rosszindulatú szoftvereket telepítsenek a vállalat ügyfeleinek hálózatába. A támadás érdekessége, hogy a támadók képesek voltak hosszú ideig észrevétlenül ügyködni, illetve hogy a cég szoftverét használókon keresztül az Egyesült Államok prominens vezetőiig is képes volt eljutni a kártékony program. A támadás előnye, hogy a biztonsági frissítésben könnyedén elrejthető a kártékony kód. A támadás kifinomultságára és komplexitására utal, hogy több mint 1000 képzett mérnök részvételével hajtották végre.[41] Feltételezések szerint az orosz Cozy Bear csoport felelős a támadás végrehajtásáért.
2021:	Microsoft Exchange	A Microsoft Exchange Server elleni támadásban több mint 30 000 egyesült államokbeli, világszerte pedig több tízezer vállalat rendszerei érintettek. A szakértők szerint kínai állami hackerek találtak egy olyan hibát, amelynek segítségével tetszőleges programot voltak képesek telepíteni a vállalatok szervereire. Így a biztonsági réseken keresztül úgynevezett hátsóajtóprogramokat *(backdoor)* telepítettek a támadók a rendszerekbe.[42]

Megjegyzés: Az évek során sokkal több támadás valósult meg, nem csak a nagyhatalmak között, azonban az itt felsoroltak gyakorolták a legnagyobb hatást a kibertér hadszíntérré válására. Érdemes azt is megjegyezni, hogy a lista csak a katonai hírszerzéshez kapcsolódó kibertámadásokkal foglalkozik, így a fontosabb magánakciók, illetve egyéb információs műveletek (például lélektani hadviselés) vagy szolgáltatások működésének korlátozását célzó támadások nem jelennek meg a felsorolásban.

Forrás: a szerző szerkesztése

[40] Joseph Marks: The Cybersecurity 202: Russia's False Flags in Winter Olympics Cyberattack Herald a More Complicated Future. *The Washington Post,* 2019. október 21.

[41] Marcus Willett: Lessons of the SolarWinds Hack. *Survival,* 63. (2021), 2. 7–26.

[42] Matthieu Faou – Mathieu Tartare – Thomas Dupuy: Exchange Servers Under Siege From at Least 10 Apt Groups. *WeLiveSecurity,* 2021. március 10.

A sikerek okai

A bemutatott támadások korábban nem ismert új technológiára, sebezhetőségre épültek. Ebben a részben azt szeretnénk bemutatni, hogy milyen újdonságok jelentek meg az egyes támadásokban, amelyek miatt azok sikeresek lehettek. Alapvetően három fő időszakot vizsgálunk meg. Először az internet kialakulásának kezdetét elemezzük, majd a 2000-es éveket, végül napjaink kibertámadásait vesszük górcső alá.

A kezdetek

Az internet kialakulását az 1980-as évek végére tehetjük, amikor még jellemző volt, hogy nem igazán számítottak támadásokra. A szoftverek fejlesztése során egyáltalán nem gondoltak a készítők arra, hogy támadások használhatják ki sérülékenységeiket. A támadások így könnyen kivitelezhetőek voltak, akár egyetlen ember is képes volt óriási káoszt teremteni.

Az első ismert kibertámadást 1988-ra lehet datálni, amikor is Robert Tappan Morris frissen végzett diák kíváncsi volt, hogy mekkora is az internet jelenleg. Ezért írt egy egyszerű programot, amely számítógépről számítógépre vándorolt, és mindig küldött egy jelet Morrisnak az újonnan megismert gépről. A program azonban annyira gyorsan reprodukálódott, és küldte az üzeneteket Morrisnak, hogy a hálózat nem bírta kellően gyorsan továbbítani a jeleket Morris gépére, blokkolta a kommunikációhoz kapcsolódó hálózati részt, így kialakítva az első DoS *(denial of system)* támadást. Hivatalosan Morris az első személy, akit ténylegesen el is ítélt a bíróság.[43]

Az egyik legnagyobb hírszerzési akció ebben az időben a Moonlight Maze támadás volt, amely valószínűsíthetően 1996-tól egészen 1999-ig tartott, illetve amelynek során sikerült adatokat továbbítani az Egyesült Államokból Oroszországba. A támadás során csak publikusan elérhető hibákat használtak ki a hackerek. Egész egyszerűen azért, mert abban az időben, ha a rendszergazdák találtak valamilyen hibát a rendszerben, azt megosztották másokkal is, ám a szoftverekhez ezekben az időkben még nem jártak olyan gyorsan frissítések,

[43] Hilarie Orman: The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy,* 1. (2003), 5. 35–43.

mint napjainkban. Volt, hogy fél év vagy akár egy év is kellett, amíg a publikusan is ismert biztonsági réseket sikeresen javították a szoftverekben.[44]

2000-es évek

A 2000-es évek hajnalán az internet mérete és felhasználási köre rendkívüli iramban növekedett. Egyre több és több online szolgáltatás vált elérhetővé, amely akár már magában is nagy károkat tudott okozni. Azonban erre az időre jellemző volt, hogy már nem csak diákcsínyként megvalósított támadásokat hajtottak végre, és a fejlesztők elkezdtek foglalkozni a szoftverek és rendszerek védelmével annak érdekében, hogy a hackerek ne legyenek képesek könnyedén hozzájutni a titkos és védett dokumentumokhoz, információkhoz.

A támadások sikerét a 2000-es évek elejétől az biztosította, hogy a hackerek jelentős csoportokat alkottak, és a támadásokat rendkívül precízen tervezték meg. Nemcsak egyetlen sérülékenységet használtak ki az adott támadás során, hanem több irányból támadtak, és több típusú támadást is bevetettek.

Talán a legismertebb ilyen támadássorozat a GhostNet és annak folytatása, a ShadowNet volt. A támadás során e-maileket küldtek a támadók kormányzati és gazdasági szervezetek tagjainak, amelyek számukra a saját területükön hasznos és érdekes információkat tartalmaztak. A megnyitott üzenet azonban rosszindulatú programot tartalmazott, amelyet ha elindítottak az áldozatok, akkor engedélyezték egy trójai program futtatását. A rosszindulatú kód Microsoft Windows operációs rendszereken működött, és a támadók képesek voltak valós időben teljesen átvenni az irányítást az áldozatok gépe felett, illetve a kamerát bekapcsolni, és videóképet rögzíteni, továbbá a mikrofont bekapcsolva hangot is rögzíteni.[45]

Ebből a támadásból is látszik, hogy nem pusztán dokumentumok ellopása volt a cél, hanem teljes megfigyelés és lehallgatás. A támadók mindezt úgy voltak képesek megtenni, hogy több éven keresztül senkinek sem tűnt fel. Ez a tény arra enged következtetni, hogy rendkívül precízen és szervezetten hajtották végre az akciót.

A másik fontos említendő eset a Stuxnet, amelynek különös jelentősége a hírszerzés mellett, hogy ez volt az első fizikai károkat okozó kibertámadás.

[44] Ushmani (2019): i. m.

[45] Nart Villeneuve – David Sancho: *The "Lurid" Downloader.* Trend Micro Incorporated, 2011.

Elsősorban programozható logikai vezérlőket (PLC) támadott, olyan ipari gépek vezérlő egységeit, amelyekkel például jármű-összeszerelést automatizálnak, vagy rostos üdítők palackozását. A Stuxnet során ezeket a vezérlőket nukleáris anyagok szétválasztására használták, és egész egyszerűen minden este, miután a gyár dolgozói hazamentek, a vírus bekapcsolta a vezérlőket, és maximális teljesítményen üzemeltette őket, aminek hatására másnap már nem működtek tovább.[46] A Stuxnet után a magyar CrySyS laboratórium felfedezte a Duqu vírust is, amelyről feltételezhető, hogy vagy a Stuxnet fejlesztői készítették, vagy a Duqut fejlesztő csapat már korábban látta és ismerte a Stuxnet forráskódját. A Duqu célja azonban nem fizikai károkozás volt, hanem egyértelműen katonai hírszerzés.

A Stuxnet és a Duqu sikeressége, mindamellett, hogy *zero-day* sebezhetőségeket használtak ki, abban rejlett, hogy valós nagyvállalatok elektronikus aláírásaival rendelkeztek. A legtöbb operációs rendszer már a 2000-es években is ismerte az elektronikus aláírás fogalmát, és ha valaki olyan szoftvert szeretett volna telepíteni (tudtával vagy tudta nélkül), amely nem megbízható forrásból származik, vagyis nem rendelkezik hiteles aláírással egy, már ismerten megbízható szolgáltatótól, akkor csak nagy nehézségek árán lehetett feltelepíteni. A Stuxnet és a Duqu is használt megbízható szolgáltatóktól eltulajdonított aláírásokat. Míg a Stuxnet egy RealTek-aláírást használt, addig a Duqu a C-Media aláírását tulajdonította el. Mindkét cég rengeteg audiohardvert gyártott abban az időben személyi számítógépekhez, és a hardverükhöz kapcsolódó *driverszoftverekhez* használták az elektronikus aláírásokat.[47]

Napjaink támadásai

A *social media* platformok (Facebook, Twitter, LinkedIn), a különféle videómegosztó és streamingportálok (YouTube, Twitch, Videa), valamint a blogoldalak (Blogger.com, Wix) lehetőséget adnak, hogy minél több információt osszunk meg magunkról. Ezeket a felületeket pedig külső szemlélőként arra is használhatjuk, hogy eldöntsük valakiről, hogy milyen személyiség, megbízható-e, szeretnénk-e vele együtt dolgozni stb. Tehát ezen platformok alkalmasak arra, hogy bizalmat érezhessünk a *social* platformon megjelenő személy iránt.

[46] Baezner–Robin (2017): i. m.
[47] Bencsáth et al. (2012): i. m.

A bizalomépítésre épülő támadás egyik példája az Operation Newscaster, amelynek célja az volt a támadók részéről, hogy kormányzati tagok, nagyvállalatok vezető pozícióiban lévő személyek számítógépét fertőzzék meg. Ahhoz, hogy ezeknek az embereknek a közelébe kerüljenek, a támadóknak újságírói és kormányzati állásokat kellett szerezniük. Ez természetesen nem egyszerű feladat egy külföldi katonai feladatokat ellátó személynek sem. A támadók mögé tehát álszemélyiségeket építettek fel, akik rendszeresen használták a különböző *social platformokat,* így képesek voltak bizalmat kiépíteni a munkaadókkal, megbízható munkaerővé váltak. Az Operation Newscaster volt 2014-ben az addigi legnagyobb kiberkémkedés, amelyhez *social engineering* technikát alkalmaztak rendkívül magas szinten.[48]

Amellett, hogy a *social engineering* ekkora teret nyert a kibertámadások során, egy másik aspektusa is továbbfejlődött a hírszerzésnek. Méghozzá a nyomok eltüntetése és a hamis nyomok előállítása is fontos célként jelent meg; többször is előfordult, hogy a támadás elkövetésének gyanúja más nemzetre, hackercsoportra terelődött, sok esetben nem is sikerült feltárni az elkövetők pontos körét.

Utóbbi aspektusra kiváló példa a 2018-as téli olimpia során végrehajtott, és később False-flagnek keresztelt támadás, amely során a hackerek észak-koreai IP-címeket használtak a támadások során, hogy tovább fokozzák a már akkor is jelentős feszültséget Dél-Koreával szemben. Egyértelmű bizonyítékot azonban senki sem talált arra, hogy ki volt az elkövető, bár a politikai helyzet miatt elsősorban Oroszországot tekintik a támadó félnek.

A 2020-as évekre a felhőalapú szolgáltatások és az óriási méretű információs rendszerek száma megsokszorozódott. Számos nagyvállalat esetében megfigyelhető, hogy nem éri meg minden rendszert saját kézben tartani, helyette olyan szolgáltatók jöttek létre, amelyek egy cég vezetését segítve biztosítanak eszközöket (szoftvereket, mérnököket), hogy a vállalat rendszereit kezeljék.

Ezért is kavart akkora port a SolarWinds elleni támadás. A támadás célja továbbra is a magas beosztású vállalati személyek és kormánytagok lehallgatása és megfigyelése volt, de ebben az esetben nem konkrétan az adott személyeket keresték meg, vagy a vállalatokhoz/kormányzati szervekhez törtek be a támadók, hanem egy szolgáltató céget, a SolarWindset támadták meg, amely több mint 30 000 vállalat számára üzemeltetett és menedzselt IT-erőforrásokat. A támadás sikere abban rejlett, hogy nem magában a szoftverben helyeztek el vírust, hanem

[48] Siboni–Kronenfeld (2014): i. m.

egy frissítésben. A rendszereket természetesen időnként frissítik, javítják, hogy még jobban működjenek, és ha egy ilyen frissítésbe rosszindulatú kódot helyezünk el, akkor az egy idő után minden vállalathoz, aki a szolgáltatást igénybe veszi, eljut. További érdekessége volt a támadásnak, hogy a rosszindulatú programkód egy idő után törölte önmagát. Emiatt a SolarWinds szoftverét használó vállalatok nagy része soha sem tudja meg, áldozatul esett-e a támadásnak, vagy sem.[49]

A célok változása

Érdemes megfigyelni, hogyan változtak a hírszerzési műveletek céljai az évek előrehaladtával, elsősorban a technikai, technológiai fejlődés következtében. Azonban minél több szenzort és beavatkozó egységet kötnek a hálózatra vagy az internetre, annál bonyolultabb hírszerzési támadások valósulhatnak meg. A 2. ábra összefoglalja, hogy melyek a támadásokból azonosítható főbb célok.

2. ábra: A hírszerzési kibertámadások céljai
Forrás: a szerző szerkesztése

[49] Willett (2021): i. m.

a) *Dokumentumok, statikus adatok megszerzése.* Az internet korai fázisában elsősorban bizalmas dokumentumok gyűjtése volt a cél. A Moonlight Maze vagy a Titan Rain elsősorban titkos információk, dokumentumok megszerzésére irányult. Az így megszerzett dokumentumokat a támadó nemzet saját céljaira használta fel.
b) *Folyamatos megfigyelés.* Amint eljutottunk arra a pontra az internet és az eszközök fejlődése folyamán, hogy kamerákat és mikrofonokat telepítettek a számítógépekbe, a hackerek ezeket a perifériákat kihasználva képesek voltak valós idejű lehallgatásra és megfigyelésre is, mint a GhostNet- és a ShadowNet-támadások esetén.
c) *Befolyásolás.* A dokumentumokat és a lehallgatás eredményeit elsősorban belső célokra használták fel, de számos olyan támadást is végrehajtottak, amelynek célja a másik fél befolyásolása volt. A 2016-os amerikai választásokon például kibertámadások segítségével próbálták befolyásolni a választási eredményeket, illetve a választók döntését. Mindemellett fontos megemlíteni a különféle *social engineering* technikákat is, hiszen sok esetben ezek elsődleges célja és eszköze a befolyásolás (például Operation Newscaster).
d) *Beavatkozás, korlátozás és fizikai károkozás.* A katonai hírszerzéshez kapcsolódó műveletek egyre inkább kiegészülnek olyan eszközökkel, amelyek be akarnak avatkozni a rendszerek működésébe, korlátozni szeretnék a rendszereket, szolgáltatásokat, és fizikai károkat is megpróbálnak okozni. Az első ismert példa a Stuxnet, ahol az eszközök egy, az internettől elzárt hálózaton voltak megtalálhatók. Érdemes megjegyezni, hogy ezért is jelent kiberbiztonsági szempontból hatalmas kockázatot az IoT- (dolgok internete) és CPS-rendszerek (kiberfizikai rendszerek) terjedése napjainkban, ahol egyre több és több szenzort, illetve beavatkozó egységet szeretnénk hálózatba kötni.
e) *Káoszteremtés.* A kibertérben végzett katonai hírszerzés során nem csak konkrét dokumentumok eltulajdonítása vagy személyek lehallgatása jelenhet meg célként. A káoszteremtés is rendkívül fontos információval bír, hiszen segítségével megfigyelhető, hogy mely rendszerek sérülékenyek, milyen gyors az áldozat reakcióideje, illetve milyen fejlett helyreállítási stratégiával rendelkezik. Az Észtország ellen indított 2007-es szolgáltatásmegtagadásos támadás célja az ország kormányzati hálózatának blokkolása volt. De idesorolhatjuk a 2017-ben népszerűnek számító zsaroló vírusok megjelenését, ahol az adatlopások mellett ellehetetlenítették az áldozatok saját eszközeihez való hozzáférést is.

A védekezési mechanizmusok fejlődése

A támadások folyamatos fejlődése következtében természetesen a védekezési mechanizmusok is folyamatosan fejlődtek annak érdekében, hogy a korábbi esetek többször már ne fordulhassanak elő. Jelen fejezetben azt vizsgáljuk, hogy miként fejlődtek a védelmi mechanizmusok az évek/évtizedek során a feltérképezett kibertámadások következtében.

Az első vírusirtó 1987-ben került piacra McAfee néven.[50] A vírusirtók akkoriban elsősorban a kártékony programok lenyomatait egy adatbázisban tárolták. A vírusirtó olyan lenyomatokat keresett a számítógépeken, amelyek egyeztek valamely elemmel az adatbázisban.

Hálózati rendszerek már az internet előtt is léteztek (például: ARPANET), és kialakultak az első tűzfalak is a hálózat védelme érdekében. Érdekes tény, hogy az első tűzfal leírását szintén 1987-ben publikálták. A kezdeti tűzfalak egyszerűen működtek: egy hozzáférési listát tartottak fent azokkal az IP-címekkel, ahonnan a hálózat tagjai fogadhattak üzenetet. A tűzfal működés közben ellenőrzött minden csomagot, amely a hálózathoz érkezett, és megvizsgálta, hogy a listában megtalálható címről érkezett-e az üzenet.[51]

Mindezek csak kezdetleges védekezési mechanizmusok voltak, és, mint ismerjük a történelmet, a támadó csoportok mindig egy lépéssel a fejlesztők előtt jártak.

Az Egyesült Államokban több, nem célzottan katonai hírszerzési célú kibertámadás is történt, az azonban egyértelművé vált, hogy az ország kritikus infrastruktúrái veszélynek vannak kitéve a kibertámadásokkal szemben. Ennek következménye volt az 1997-ben végrehajtott Eligible Receiver projekt, amely, jelenlegi terminológiánk szerint, célzott sérülékenységvizsgálat volt. Etikus hackerek első alkalommal támadták meg szándékosan országuk belső infrastruktúráit, hogy felkészülhessenek a lehetséges kibertámadásokra.[52] Sajnos a felkészülés nem volt tökéletes, hiszen mint utóbb kiderült, a Moonlight Maze támadás már 1996-tól tulajdonított el dokumentumokat az Egyesült Államokból.

[50] Jeffrey S. Kline: *McAfee Associates, Inc. Competitive Strategies for the Computer AntiVirus Industry.* 1998.

[51] Kenneth Ingham – Stephanie Forrest: *A History and Survey of Network Firewalls.* Technical Report. Albuquerque, University of New Mexico, 2002-37.

[52] James Adams: Virtual defense. *Foreign Affairs,* 80. (2001), 3. 98–112.

A kibervédelem felmérésének következő jelentős pontja a 2002-ben kivitelezett Digital Pearl Harbour[53] gyakorlat, sérülékenységi vizsgálat volt, összekötve azonnali védekezési stratégiákkal: kiberháborút szimulálva bizonyíthatóvá vált, hogy kiberterroristák súlyos gazdasági és társadalmi problémákat okozhatnak. Biztonsági szakértők egy csoportja azt a feladatot kapta, hogy tervezzen meg 4 különböző iparág elleni támadást.

2008-ban az Egyesült Államok elszenvedte az addigi legnagyobb katonai hírszerzési támadást, amikor a Közel-Keleten egy amerikai katonai laptopba helyezett adathordozó segítségével rengeteg titkos információt tulajdonítottak el. Az Egyesült Államok ennek hatására riadót fújt a kibertámadás kivédésével kapcsolatban. Az Operation Buckshot Yankee hadművelet fordulópontot jelentett az amerikai kibervédelmi stratégiában. Az akció során többrétegű és robusztus katonai védelmi hálózatot építettek a Pentagon köré. A Pentagon ettől a ponttól kezdve szorosan együttműködik az NSA-vel, hogy együttes erővel védjék és ellenőrizzék a kormányzati hálózatokat és kritikus infrastruktúrákat. A védelmi stratégiát az USA a legközelebbi szövetségeseire is kiterjesztette.

Ez a fajta törekvés 2013-ra eljutott arra a pontra, hogy a NATO védelmi miniszterei megegyeztek abban, hogy az együttműködésben részt vevő tagállamok által üzemeltetett hálózatokhoz kapcsolódó kibervédelmi intézkedések szintén összefogást igényelnek, hiszen ha az egyik tagállam kibertámadást szenved, más tagállamok is könnyű célponttá válhatnak. Hozzátéve azt is, hogy a megegyezés előtti évben, 2012-ben több mint 2500 szignifikáns kibertámadás történt a NATO területén belül, azonban egyik támadás sem járt sikerrel.[54]

Konklúzió és jövőbeli kitekintések

Ebben a fejezetben történeti áttekintést adtunk a kibertérben megvalósuló katonai hírszerzésről az internet és a számítógépek létrejöttekor megismert támadásoktól kezdve egészen napjaink támadásaiig. Megvizsgáltuk, hogy miképpen változtak a hírszerzési technikák az idő előrehaladtával, illetve bemutattuk, hogy milyen

[53] Eric Purchase – Caldwell French: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In *Guarding Your Business.* Boston, Springer, 2004. 47–64.

[54] Liu Yi: The Thoughts On Our Army Security Management of Removable Mass Storage Device. *Information Security and Technology,* (2012), 10.

stratégiák és fontosabb döntések történtek a kibervédelem megvalósítása során, hogy az esetleges támadásokat a nemzetek képesek legyen elhárítani.

A történeti áttekintést az 1998-ban azonosított Solar Sunrise esetével kezdtük, majd tovább vizsgáltuk a kibertérben azonosított támadásokat, így például az első szolgáltatásmegtagadásos támadást, zsaroló vírusokat, teljes megfigyeléssel és lehallgatással kapcsolatos eseteket, egészen a napjainkban történt eseményekig, mint a SolarWindset és a Microsoft Exchange-et érintő hírszerző támadások.

Ezt követően a történeti áttekintés során megvizsgált támadások sikerességét azonosítottuk. Jól látható, hogy a támadások folyamatosan fejlődtek az évek alatt, így minden egyes támadás valamiben új és egyedi megoldást alkalmazott. Továbbá az egyes támadások során más és más aspektusban fejlődtek. Ezek alapján megismerkedtünk többek között az első támadási technikákkal, a videós és audiós megfigyelésekkel, valamint az olyan támadásokkal, amelyek fizikai károkat is képesek voltak okozni.

Bemutattuk, hogyan változtak a támadók céljai a technika fejlődése során. Míg korábban csak titkos anyagok, dokumentumok jelentették a támadások céljait, később jellemzővé váltak a megfigyeléssel kapcsolatos támadások, illetve a káoszteremtésből megszerezhető információgyűjtés is.

Végül azonosítottuk a védekezéssel kapcsolatos lépéseket: az 1997-es Eligible Receiver projekttel kezdtük tanulmányozni, majd a különböző sarkalatos pontok alapján létrejövő események keretében láthattuk, ahogy a NATO tagjai egységesen lépnek fel a kibertérben megvalósuló katonai hírszerzés ellen. 2016-ban a NATO kijelentette, hogy az operatív hadviselés területét kiterjeszti a kibertérre is.

Összességében elmondható, hogy a bemutatott támadások és a hozzájuk kapcsolódó védelmi döntések már részét képezik történelmünknek, és formálták a világot is, hogy eljussunk oda, ahol jelenleg is tartunk.

Jövőbeli kitekintés

Egyértelmű, hogy ez még csak a kezdet; olyan új technológiák születnek napjainkban, mint a dolgok internete (IoT), a kiberfizikai rendszerek (CPS), az okosvárosok *(smart cities),* amelyek középpontjában a különböző információs eszközök közötti kommunikáció áll.

Ezen technológiák esetében különböző szenzorok adatokat (kép, hang, hőmérséklet, koordináta) szolgáltatnak egy központi (elosztott) irányítás számára,

amely képes utasítani a rendszerhez kapcsolt beavatkozókat. Az eszközök minden esetben egyetlen hálózaton találhatóak, ahol maga a hálózat lehet nyitott, vagyis kapcsolódik az internetre, vagy zárt, tehát az internettől elzárt.

3. ábra: Az IoT-rendszerek koncepciója
Forrás: Zigurat: *What Do the Next Five Years Hold for the IoT?* é. n.

A korábban bemutatott támadások között voltak olyanok, amelyek nyitott és zárt hálózatokon keresztül is képesek voltak információkat szerezni, illetve egyéb károkat okozni. Látható, hogy a jövő technológiái is nagy veszélyben vannak, illetve szinte biztosra vehető, hogy ezeket a technológiákat is képesek lesznek a hírszerző támadások a saját irányításuk alá vonni.

Míg napjainkban a különféle platformok leginkább információt gyűjtenek (például: Google, Facebook stb.), és a felhasznált adatokat egy-egy mesterséges intelligencia által kezelt támogató rendszer számára továbbítják (az általunk megadott adatokból a mesterséges intelligencia képes mintákat felfedezni, és következtetéseket levonni arra vonatkozóan, hogy mit szeretünk csinálni, mit fogunk a jövőben tenni stb.), addig a jövőben egyre több beavatkozó egység is a hálózatra lesz kapcsolva, amely ténylegesen képes lesz befolyásolni a környezetét.

A károkozás, valamint a káoszteremtés így sokkal nagyobb méreteket is ölthet (például: önvezető autókat hamis információval manipulálva tetszőleges helyre irányíthatók), illetve azáltal, hogy minél több szenzort kapcsolunk az internetre, saját magunkról szolgáltatunk egyre több és több információt a hírszerzők számára.

A kibervédelem szempontjából a legfőbb cél, hogy ne engedjük meg, hogy harmadik fél képes legyen beleszólni az eszközök közötti kommunikációba.

Összegezve: a jövő egyik legfontosabb kérdése, hogy az eszközök közötti kommunikációs csatornákat a nemzetek mennyire lesznek képesek biztonságossá tenni, illetve ha mégis történik behatolás, milyen gyorsan képesek azokat azonosítani, kezelni, és az okozott károkat helyreállítani.

Irodalomjegyzék

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról

Adair, Steven et al.: *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* A Joint Report of the Information Warfare Monitor and Shadowserver Foundation. Toronto, 2010. április 6.

Adams, James: Virtual defense. *Foreign Affairs,* 80. (2001), 3. 98–112. Online: https://doi.org/10.2307/20050154

Baezner, Marie – Patrice Robin: Stuxnet. *ETH Zurich,* 4. (2017). Online: https://doi.org/10.3929/ethz-b-000200661

Bencsáth Boldizsár – Buttyán Levente – Pék Gábor – Félegyházi Márk: Duqu: Analysis, Detection, and Lessons Learned *ACM European Workshop on System Security (EuroSec)*, 2012. Online: www.hit.bme.hu/~buttyan/publications/BencsathPBF12eurosec.pdf

Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere. (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására.) *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100. Online: http://epa.oszk.hu/02500/02538/00002/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01_063-100.pdf

Charette, Robert N.: DoD Admits to Being Severely Hacked. *IEEE*, 2008. Online: https://spectrum.ieee.org/riskfactor/computing/it/dod_admits_to_being_severely_h

Deák Veronika: Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14. (2019), 2. 256–271. Online: https://doi.org/10.32567/hm.2019.2.21

Deibert, Ronald J. – Rafal Rohozinski: Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor,* 2009. március 29. Online: https://bit.ly/3OfhOnA

Dobák Imre: *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2014.

Faou, Matthieu – Mathieu Tartare – Thomas Dupuy: Exchange Servers Under Siege From at Least 10 Apt Groups. *WeLiveSecurity,* 2021. március 10. Online: www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Fehér Krisztián: *Kezdő hackerek kézikönyve*. Budapest, BBS-INFO, 2016.

Füzesi Ottó: *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésére.* Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2004. Online: https://bit.ly/3n5MTOK

Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám. 1788–1919. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html

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

Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem, 2012.

Haraway, Donna: A Cyborg Manifesto: Science, Technology and Socialist-Feminism in the Last Twentieth Century. In Donna Haraway: *Simians, Cyborgs and Women: The Reinvention of Nature.* New York, Routledge, 1991. 149–181.

Ingham, Kenneth – Stephanie Forrest: *A History and Survey of Network Firewalls.* University of New Mexico, Tech. Rep., 2002.

Izsa Jenő: A hírszerzés céljáról és rendszeréről. *Hadtudomány,* 19. (2009), 1–2. 72–83. Online: www.mhtt.eu/hadtudomany/2009/1_2/072-083.pdf

Knapp, Kenneth J. – William R. Boulton: Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management,* 23. (2006), 2. 76.

Kovács László: Az információs terrorizmus eszköztára. *Hadmérnök,* (2006), különszám. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/2062/kovacs_rw6.pdf?sequence=2

Kovács László: *Biztonságpolitika: a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

Kovács László – Krasznay Csaba: „Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9. Online: https://bit.ly/3Ox1FKi

Kumar, Animesh: Zero Day Exploit. *SSRN,* 2014. január 14. Online: https://doi.org/10.2139/ssrn.2378317

Leonov, Pavel Y. et al.: The Main Social Engineering Techniques Aimed at Hacking Information Systems. *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* IEEE, 2021. 0471–0473.

Magyar Hadtudományi Lexikon. Budapest, Magyar Hadtudományi Társaság, 1995.

Marks, Joseph: The Cybersecurity 202: Russia's False Flags in Winter Olympics Cyberattack Herald a More Complicated Future. *The Washington Post,* 2019. október 21. Online: https://wapo.st/3OwdiRu

Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 48. (108.) (2001), 7. 769–779. Online: http://epa.oszk.hu/00700/00775/00032/769-779.html

MITRE ATT&CK: Groups. 2021. Online: https://attack.mitre.org/groups/G0010/

Morgan Swartley: Political Marketing: How Social Media Influenced the 2008–2016 US Presidential Elections and Best Practices Associated. *Senior Honors Theses,* 726. 2018. szeptember 4. Online: https://digitalcommons.liberty.edu/honors/726/

Mwiki, Henry et al.: Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. In *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham, 2019. Online: https://doi.org/10.1007/978-3-030-00024-0_12

Nakashima, Ellen: Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say. *The Washington Post,* 2013. május 20. Online: https://wapo.st/3xOCmfK

Orman, Hilarie: The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy,* 1. (2003), 5. 35–43.

Purchase, Eric – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Sumit Ghosh – Manu Malek – Edward A. Stohr (szerk.): *Guarding Your Business. A Management Approach to Security.* Boston, Springer. 47–64. Online: https://doi.org/10.1007/0-306-48638-5_4

Rubenstein, Dana: *Nation State Cyber Espionage and its Impacts.* Washington University in St. Louis, 2014. december 1. Online: www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/

Siboni, Gabi – Sami Kronenfeld: Iranian Cyber Espionage: A Troubling New Escalation. *INSS Insight,* 2014. június 16. Online: www.inss.org.il/publication/iranian-cyber-espionage-a-troubling-new-escalation/

Tsague, Hippolyte Djonon – Bheki Twala: *Reverse Engineering Smart Card Malware Using Side Channel Analysis With Machine Learning Techniques.* IEEE International Conference on Big Data (Big Data), 2016. 3713–3721. Online: https://doi.org/10.1109/BigData.2016.7841039

Ushmani, Azhar: Cyberwarfare History and APT Profiling. Advance Online Publication. *International Journal of Computer Science Trends and Technology (IJCST),* 7. (2019), 4. Online: www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P1.pdf

Villeneuve, Nart – David Sancho: *The "lurid" downloader.* Trend Micro Incorporated, 2011.

Willett, Marcus: Lessons of the SolarWinds Hack. *Survival,* 63. (2021), 2. 7–26. Online: www.iiss.org/blogs/survival-blog/2021/04/lessons-of-the-solarwinds-hack

Yaqoob, Ibrar et al.: The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. *Computer Networks,* 129. (2017). 444–458. Online: https://doi.org/10.1016/j.comnet.2017.09.003

Yi, Liu: The Thoughts On Our Army Security Management of Removable Mass Storage Device. *Information Security and Technology,* (2012), 10.

Zigurat: What Do the Next Five Years Hold For the IoT? é. n. Online: www.e-zigurat.com/innovation-school/blog/what-do-the-next-five-years-hold-for-the-iot/