BEVEZETÉS

Az idő előrehaladtával a technológia folyamatos és egyre nagyobb mértékű fellendülését figyelhetjük meg. Napjainkra az infokommunikációs technológiák és információs rendszerek folyamatos fejlődése nagyban hozzájárul a különféle kibertámadások hatékonyságának növeléséhez, az egyre korszerűbb technikáknak köszönhetően. A támadások érinthetik a különféle kritikus infrastruktúrákat, az állami és nem állami szerveket egyaránt, sok esetben pedig bizalmas információk megszerzését célozzák. Azt azonban fontos kiemelni, hogy attól függetlenül, milyen típusú egy adott támadás, illetve milyen céllal hajtják végre azt, minden esetben kulcsfontosságú a különböző infokommunikációs és informatikai rendszerek szervezett, magas szintű védelme és a felhasználók biztonságtudatos szemléletmódjának kialakítása. A bizalmas információk megszerzésére irányuló támadások egyik típusa a social engineering.[1] A social engineering olyan technikák és módszerek összességét jelenti, amely során a támadó a technológia használatával vagy anélkül képes az emberi hiszékenységet, naivitást, sebezhetőséget, és számos további az emberi tényezőre jellemző tulajdonságot kihasználva befolyásolni és irányítani az áldozatát. A social engineer a manipulálás, a kihasználás, a befolyásolás, a megtévesztés, a rábeszélés és a meggyőzés segítségével irányítja áldozatát a céljai elérése érdekében. A támadások céljai igen sokrétűek, irányulhatnak többek között bizalmas információk megszerzésére, módosítására, illetve törlésére, a sérülékenységek és sebezhetőségek feltárására, a célszemély viselkedésének befolyásolására, a belső hálózati hozzáférés, jogosultság megszerzésére, különféle infokommunikációs eszközök rosszindulatú programmal történő megfertőzésére vagy akár egy komplex kibertámadás előkészítésére egyaránt. A social engineering komplex támadási formának tekinthető, számtalan támadási módszert foglal magába, informatikai eszközök nélkül és azok segítségével cselekvő technikákat egyaránt, amelyek megakadályozása kulcsfontosságú feladat. Jelen tanulmány az informatikai eszközök segítségével cselekvő social engineering technikákat, ezen belül is az ezen keresztül terjedő kártékony programok vizsgálatát tűzte ki célul. A kártékony programok és a social engineering kapcsolatának, összefüggéseinek elemzése azért szükséges, mert ez az a terület, amely egyszerre ötvözi a social engineering pszichológiai és műszaki vonatkozásait. Ez a gyakorlatban úgy jelenik meg, hogy nem elég csupán elküldeni egy rosszindulatú kódot tartalmazó fájlt a célszemélynek, valamilyen eszközzel motiválni, manipulálni kell annak aktiválására, hiszen a támadás végrehajtásának sikeressége csak az áldozat által biztosítható. Éppen ezért szükséges a téma mélyebb vizsgálata, hiszen az esetek döntő többségében a felhasználó az, aki lehetővé teszi a kártékony programok terjedését és/vagy működését, így nem elég csupán a kártékony programok műszaki vonatkozásait vizsgálni, mindenképpen szükséges a rosszindulatú programok és az emberi tényező közötti kapcsolat feltárása. A kártékony programok lehetséges terjedésének vizsgálata érdekében szükséges azon social engineering technikák meghatározása és rendszerezése, amelyek lehetővé teszik azok terjedését. Ennek érdekében egy új csoportosítást hoztam létre, hogy segítségével azonosíthatók legyenek a social engineering technikák, az alapján, hogy milyen eszközökön, platformokon keresztül képesek adatot, információt szerezni. Természetesen a kártékony programok social engineering technikák segítségével történő terjesztésére másféle csoportosítás is alkalmazható. A feltételezésem, hogy ezen tulajdonságok alapján a social engineering kategorizálhatók, így jelen tanulmány célja a rosszindulatú programok terjesztésére alkalmas social engineering technikák meghatározása, csoportosítása és mélyebb vizsgálata.

Ahhoz, hogy a témával összefüggő kockázatok és sebezhetőségek minden részletre kiterjedő elemzése megvalósulhasson, nélkülözhetetlen a releváns hazai és nemzetközi szakirodalom mélyebb vizsgálata. A social engineering és a kártékony programok kapcsolatát vizsgáló hazai szakirodalom igencsak hiányos, ezért jelen tanulmányban kísérletet teszek a két terület összefüggéseinek megállapítására. A nemzetközi szakirodalom vizsgálja a social engineering

és a kártékony programok kapcsolódási pontjait, azonban ismereteim szerint összefoglaló csoportosítást még nem publikáltak a témában.

KÁRTÉKONY PROGRAMOK ÉS AZ EMBERI TÉNYEZŐ KAPCSOLATA

Mint minden social engineering technika esetén a kártékony programok kapcsán is ki kell térni az emberi tényező szerepére a támadások előkészítése és kivitelezése során egyaránt. A humán tényező fontossága abban rejlik, hogy a felhasználó az, aki kapcsolatban áll a különféle védendő értékekkel, mint például az adatokkal, információkkal, az infokommunikációs alkalmazásokkal, rendszerekkel és eszközökkel, valamint további felhasználókkal is. [2: 10] Ezen kívül az emberek számos kihasználható tulajdonsággal rendelkeznek, amelyek egy támadás végrehajtása során előnyt biztosítanak a támadó számára. [2] Ilyen tulajdonságok közé tartoznak a teljesség igénye nélkül az alábbiak:

- segítőkészség,
- viszonzási igény,
- befolyásolhatóság,
- naivság,
- nyitottság, érdeklődés
- kíváncsiság,
- hiszékenység,
- figyelmetlenség,
- monotonitás,
- túlterheltség, fáradtság
- hanyagság,
- befolyásolhatóság,
- elégedetlenség,
- bosszúállás,
- szakértelem hiánya
- biztonságtudatosság hiánya.

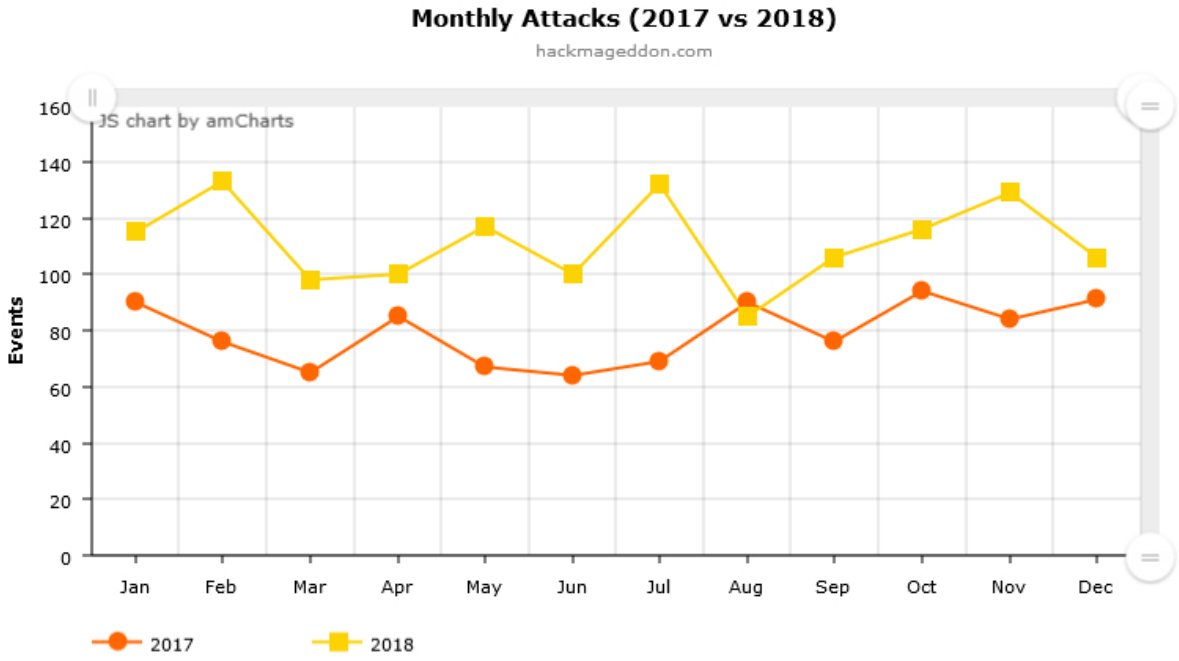
Ezen jellemzők mind felhasználhatók egy támadás végrehajtása során, hiszen a támadó a célszemélyről való előzetes információszerzést követően dönt arról, hogy mely tulajdonságára alapozva kezdi meg a végrehajtáshoz szükséges kapcsolat kiépítését, vagy éppen annak tényleges kivitelezését. Továbbá fontos megemlíteni, hogy a különféle szoftverekkel ellentétben az emberek könnyen befolyásolhatók, manipulálhatók. Ennek számtalan eszköze lehet, attól függően, hogy mi az oka és célja a befolyásolásnak.
Az emberi tényező vizsgálata azért létfontosságú, mert a mai modern világunkban a különböző informatikai eszközök védelme már nagyon fejlett, így a támadó, ha például nem talál sebezhetőséget a felsőbb szinteken, mindig egy szinttel lejjebb fog menni, és addig csinálja ezt, amíg nem talál egy olyan pontot, ami sebezhető. Az esetek döntő többségében pedig pont a felhasználói szint az, ahol a támadó könnyedén találhat sérülékenységet, többek között például a korábban említett kihasználható tulajdonságoknak köszönhetően. Ezen kívül végső soron a felhasználó lesz az, aki aktiválja majd a kártékony kódot, így a rosszindulatú programok aktiválásához elengedhetetlen az emberi tényező vizsgálata, sebezhetőségeinek feltárása.

KÁRTÉKONY PROGRAMOK

A social engineering technikákon keresztül számos kártékony program terjedése valósulhat meg. A kártékony programok csoportjába sorolhatók a rosszindulatú szoftverek, másnéven *malwarek* (Malicious Software). Rosszindulatú szoftvernek tekinthetők azok a szoftverek,

amelyek célja nem az információs rendszer működésének biztosítása és fenntartása, hanem bizonyos információk megszerzése, módosítása, törlése, megsemmisítése, valamint engedély nélküli tevékenységek végzése. Ezen rosszindulatú szoftverek segítségével a támadó könnyedén zavart okozhat a célszemély számára, például túlterhelheti, működésében akadályozhatja, valamint akár működésképtelenné teheti a felhasználó bármely infokommunikációs eszközét. Az esetek jelentős hányadában ezek a programok a felhasználó engedélye és tudta nélkül kerülnek az eszközeire. A malware-ek csoportjába sorolhatók a vírusok, férgek, trójai programok, kémprogramok, zsarolóprogramok, flooderek, dropperek, ál vírusírtók, rootkitek, keyloggerek, backdoor programok és számos további rosszindulatú program. [3]

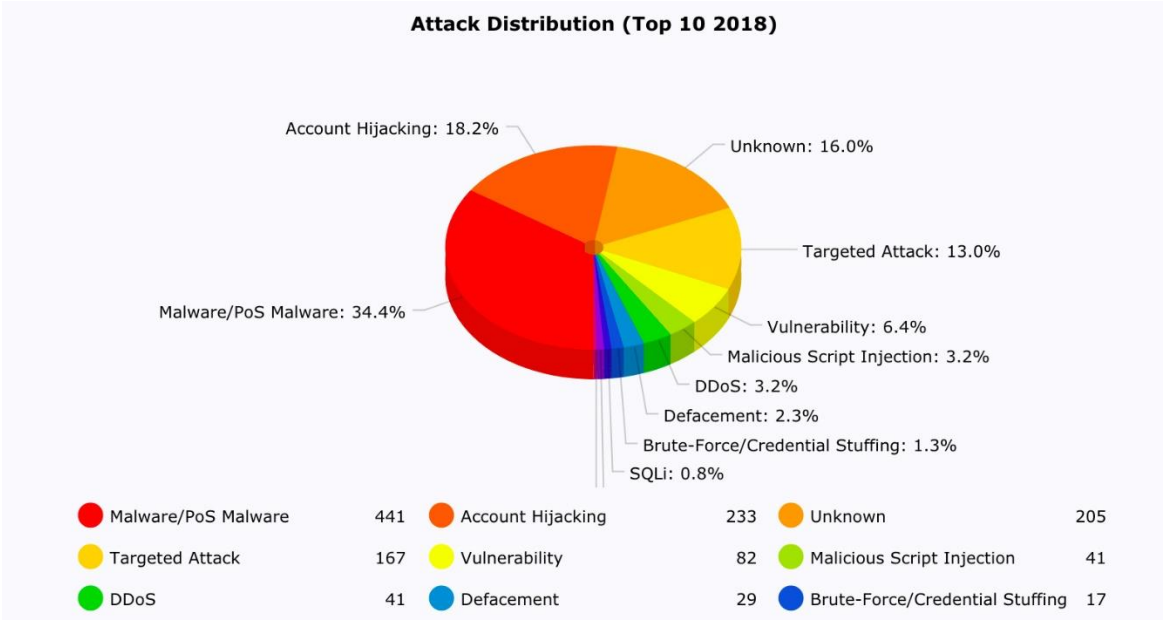
A malwarek évről-évre egyre nagyobb kockázatot jelentenek az általuk megfertőzött infokommunikációs eszközök számának rohamos növekedésének köszönhetően. Az *1*. ábrán látható statisztika tökéletesen szemlélteti, hogy a 2018-ban bekövetkezett kibertámadások száma – egy hónap kivételével – folyamatos emelkedést mutat az azt megelőző 2017-es évhez képest.



1. ábra: Kibertámadások száma (2017 vs. 2018)
Forrás: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/

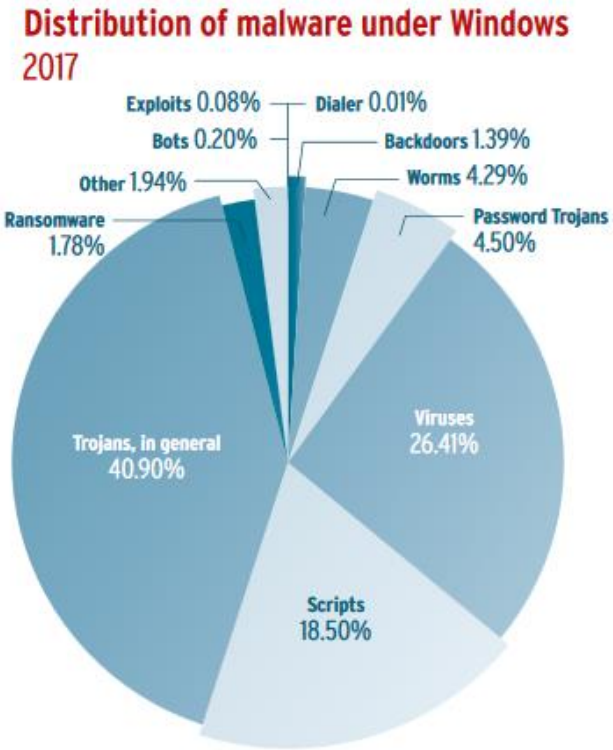
Napjainkban a rosszindulatú programok alkalmazása a támadók egyik leggyakrabban felhasznált módszere annak érdekében, hogy például bizalmas információkat szerezzenek meg, befolyásolják a felhasználót, vagy valamilyen anyagi haszonszerzést valósítsanak meg. Éppen ezért az egyre növekvő felhasználásuk és elterjedésük indokolttá teszik a lehetséges bekövetkezés körülményeinek, például a malwarek terjedésének esetleges módszereinek vizsgálatát.

A 2018-ban bekövetkezett kibertámadások módszerei különbözőek és sokrétűek voltak, amely az alábbi *2*. ábra segítségével ábrázolható. Jól látható, hogy a bekövetkezett események jelentős többségében (34,4%) a malwarek általak a támadások hátterében.



2. ábra: Támadási módszerek megoszlása (2018)
Forrás: https://www.hackmageddon.com/2019/01/15/2018-a-year-of-cyber-attacks/

A kártékony programoknak számtalan típusa ismert, az alábbi *3.* számú ábra összefoglalja, hogy 2017-ben a malwarek mely típusai fertőztek a leggyakrabban Windows operációs rendszerrel rendelkező eszközöket.



3. ábra: Rosszindulatú programok általi fertőzések Windows-os eszközökön
Forrás: https://www.av-test.org/en/news/the-av-test-security-report-20172018-the-latest-analysis-of-the-it-threat-scenario/

A következőkben a rosszindulatú programok néhány típusa kerül ismertetésre.

A *vírus* olyan rosszindulatú program, amely 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 vírusok a rendszerbe a felhasználó engedélye nélkül kerülnek be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD kártya, merevlemez, MP3 és videó lejátszó, 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 törölheti vagy módosíthatja, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nem csak adathordozó eszközök által terjedhet, hanem elektronikus levelezés során az üzenetek csatolmányaként, vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is. [4: 145]

Az *alkalmazáshibát kihasználó vírusok* elsődleges célja egy legfőképp távoli vagy hálózati program elindítása a rendszeren, illetve magasabb szintű hálózati elérés biztosítása a támadó felé úgy, hogy mindeközben ezek a vírusok egy program egy vagy több sebezhető pontjára összpontosítják a támadásukat. Egyes hackerek ezzel a módszerrel tesztelik a különféle rendszerek behatolás elleni védelmét. [5: 29]

A vírusokhoz hasonló jellemzőkkel rendelkeznek a *programférgek*, amelyek a vírusokkal ellentétben nem fájlokat fertőznek, hanem önállóan futó, gazdaprogramot nem igénylő programok, amelyek képesek saját maguk megsokszorosítására. Másolataikat a megtámadott infokommunikációs eszköz háttértárán készítik el, de a hálózat segítségével is eljuttathatják. [4: 145–146]

A *logikai bomba* „olyan program, illetve programrészlet, amely logikailag (funkcionálisan) nem várt hatást fejt ki.” [6: 53] Összességében ezen programok jellemzője a pusztító hatásuk és váratlan megjelenésük, amely egy konkrét esemény, az esetek döntő többségében valamilyen rendszeresemény, mint például egy előre meghatározott időpont bekövetkezése, az eszköz elindulása, leállása vagy akár egy fájl megjelenése, megváltoztatása, illetve törlése következtében valósul meg. [6: 53]

A malware-ek csoportjába sorolhatók a *trójai programok*, amelyek 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 akár adatállományokat törölnek. Tehát a program a felhasználó tudta nélkül a háttérben nemkívánt műveletek is végrehajthat, mint például a vírustelepítés, titkos információk megszerzése (például banki adatok, jelszavak, PIN-kódok), hátsó ajtó létrehozása vagy akár közvetlen károkozás is. [7]

Az előbb említett „*hátsóajtó*”, másnéven *backdoor program* olyan, a felhasználók számára általában nem látható elem, amelyet 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 nem csak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti. A backdoor programok a többi rosszindulatú programhoz hasonlóan települhetnek adathordozók vagy e-mail, illetve egyéb internetes letöltés mellékleteként). [4: 146]

A *dropper* a trójai programok egyik típusaként is értelmezhető. Miután a számítógépbe kerül a kártékony kódot még nem tartalmazó dropper, több olyan kártékony programot, például vírust is képes legyártani és telepíteni, amely az adott operációs rendszeren keresztül futtatható. Ezt követően el is indítja azokat, de a dropperről nem készül másolat, így nem sorolható a klasszikus vírusok csoportjába. [5: 30]

Az *injektorok* a dropperek speciális típusai, amelyek a különféle vírusokat aktív formában töltik be a memóriába, sok esetben a vírus elhelyezésére a lemez megszakításkezelőjében kerül

sor, amely eredményeképpen amikor a felhasználó megpróbálja elérni a lemezt a vírus nem csak aktiválódik, hanem elkezd szaporodni is. Rendszerint használják a szórás módszerét, melynek lényege, hogy egyszerre számos távoli gépre is elhelyezik ugyanazt a vírust, azért, hogy a bekövetkező kitörés ugyanabban az időben több gépen is megvalósuljon, ezáltal pedig egy gyors járvány kialakulásához vezessen. [5: 30]

Az *automatikus jogosultságszerzők* vagy másnéven *autorooter programokat* gyakran alkalmazzák a távoli számítógépek és egyéb infokommunikációs eszközök fertőzéséhez, hiszen ezek általában exploit vírusok segítségével támadják meg a célrendszert és ezzel együtt a támadónak rendszergazdai jogosultságot szereznek a távoli rendszer felett. [5: 31]

A *vírusfejlesztő kitek* olyan vírusok előállítására, fejlesztésére és generálására alkalmas programok, amelyek maga a vírus program megírását és fejlesztését szolgálák. Ezen programok által komolyan programozói tudás nélkül egy alkalmazás segítségével automatikusan is megvalósulhat a vírusok megírása, előállítása és fejlesztése. [4: 146]

Az *elárasztók* vagy másnéven *flooderek* segítségével a támadók olyan mértékben képesek megnövelni a hálózati adatforgalmat, hogy ennek következtében szolgáltatásleállást (Denial of Service- DoS) idéznek elő. Abban az esetben, ha egyszerre, párhuzamosan több egymással kapcsolatban álló gép hajtja végre a DoS támadást, akkor DDoS (Distributed Denial of Service) támadásról beszélünk, amely következtében az adott eszközön az informatikai szolgáltatás részlegesen vagy teljesen elérhetetlenné válik. [5: 32]

A *kémprogramok (spyware)* a rendszerbe jutva a háttérből figyelik a rendszerben lezajló eseményeket, melyekről jelentéseket és adatokat küldenek a támadónak, de céljuk továbbá az infokommunikációs eszközön lévő információk megszerzése a felhasználó tudta nélkül. [4: 146]

A *keyloggerek*, olyan billentyűzet naplózásra alkalmas programok, amelyek a felhasználó által begépelt karaktereket, illetve a képernyő tartalmát naplózzák, majd eltárolják azt. Később ehhez hozzáférhetnek, de akár tovább is küldhetik a támadónak, aki a naplózott karakterekből könnyen bizalmas információkhoz juthat. [8: 52–54]

A spammer programok elsődleges célja kéretlen e-mailek, illetve SMS üzenetek szétküldése a különféle hírlevéllisták és egyéb infokommunikációs eszközök felhasználóinak a fiókjaiba, az azonnali üzenetküldő rendszerek levelezőlistái segítségével. A spam üzenetek jelentős részét arra használják a támadók, hogy adathalász támadást valósíthassanak meg az üzeneteken keresztül és ezáltal jussanak bizalmas és személyes információkhoz. [5: 31]

A hamis vírusírtók vagy másnéven scarewarek, olyan programok, amelyek a felhasználó infokommunikációs eszközén valamilyen vírusírtóként, rendszerkarbantartó vagy egyéb hasonló biztonsági funkciót betöltő programként jelennek meg. Ezen programok számos valójában hamis szolgáltatást kínálnak, mint például a különféle hibák javítása, frissítések telepítése, kártékony programok észlelése, tárhelyfelszabadítás, szükségtelen fájlok eltávolítása, sebezhetőségek feltérképezése. Alapvetően ingyenes programnak tekinthetők, azonban a működésük közben felugró ablakok jelennek meg, amelyek a rendszer fertőzéséről értesítenek. A felugró ablak rendszerint tájékoztat arról, hogy milyen fenyegetéssel állunk szemben, milyen káros következményeket idézhet ez elő (pl. személyes és bizalmas adataink illetéktele kezekbe kerülése), illetve arról is, hogy ez a probléma a program teljes, fizetős verziójával kijavítható, amely megvásárlásával a felhasználó egy újabb hamis szolgáltatásért fizet, valamint további kártékony programok településére is sor kerülhet. [9]

A *zsaroló program*, másnéven *ransomware*, amelynek célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsarolóprogramok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó egy 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 kiterjeszti a fizetésre rendelkezésre álló időt vagy törli az adatokat a felhasználó infokommunikációs eszközéről. [10]

Ilyen zsarolóvírus volt a WannaCry is, amely 2017. május 13-án, egy pénteki napon kezdett el terjedni a világ különböző tájain található Windows operációs rendszerrel rendelkező számítógépeire. A sérülékenységeket kihasználó kód (ETERNALBLUE kódnéven) a ShadowBrokers néven ismertté vált hacker csoport által került ki az internetre 2017. április 14-én. Az Europol állítása szerint több mint 150 országban, mintegy 200 000 számítógép esett a zsarolóvírus áldozatául. A WannaCry egy a Microsoft Windows sérülékenységét használta kis, amelyet az NSA (U.S. National Security Agency) már korábban felfedezett, de ahelyett, hogy jelezte volna ezt a Windows fejlesztőinek, saját célú titkos megfigyelésre használta. A zsarolóvírus 300 $-t kért a titkosított fájlok visszaállításáért. [11] A vírus számos kereskedelmi, egészségügyi és kormányzati intézmény infokommunikációs eszközeinek működését bénította meg. A WannaCry segítségével egy nulladik napi támadás valósult meg, melynek pont az a lényege, hogy egy még korábban nem felfedezett sérülékenységet, biztonsági rést használ ki. AWannaCry esetében, mikor a Windows értesült a rendszer gyenge pontjáról, javította a sérülékenységet és kiadta az operációs rendszer legújabb frissítéseit. Éppen ezért nagyon fontos, hogy folyamatosan frissítsük az operációs rendszerünket és alkalmazásainkat, hogy az esetleges biztonsági rések minél hamarabb javításra kerülhessenek. A WannaCry terjedésének még nem minden aspektusa került nyilvánosságra, de a kiszivárgott információk alapján a Nemzeti Kibervédelmi Intézet egy összefoglalót tett közzé. Ebben részletezi a zsarolóprogram működésének technikai részleteit és a megelőzésére, illetve a megfertőződés esetére ajánlásokat fogalmaz meg. A Wannacry program tulajdonságai leginkább egy spear-phishing kampányra utalnak, amelyben JavaScript és PowerShell kódot alkalmazó makrókkal ellátott MS Office dokumentumot terjesztenek csatolmányként. A zsarolóvírus egy hosszú névvel rendelkező domain-t (iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea[.]com) próbál megszólítani és a kapcsolódás sikere esetén kilép. Ha akár egyetlen számítógép is fertőződik egy lokális hálózaton, a program képes automatikusan tovább terjedni az SMB protokoll használatával. Fontos megjegyezni, hogy ennek következtében a nem frissített, SMB protokoll használatát elérhetővé tevő számítógépek az Interneten közvetlenül fertőződhetnek, külön célba juttatási mechanizmus nélkül. A támadásokban használt malware titkosítja a fájlokat és egy visszafejtéshez használható eszközt (decryptor tool) is letölt. Ezt követően körülbelül 300 dollárt követel Bitcoin-ban a visszafejtéshez használható kódért cserébe. A használói felülete több nyelvet támogat. [12] Az alábbi ***4***. számú ábrán látható, milyen kép jelent meg a WannaCry zsarolóvírussal fertőződött eszközök képernyőjén.

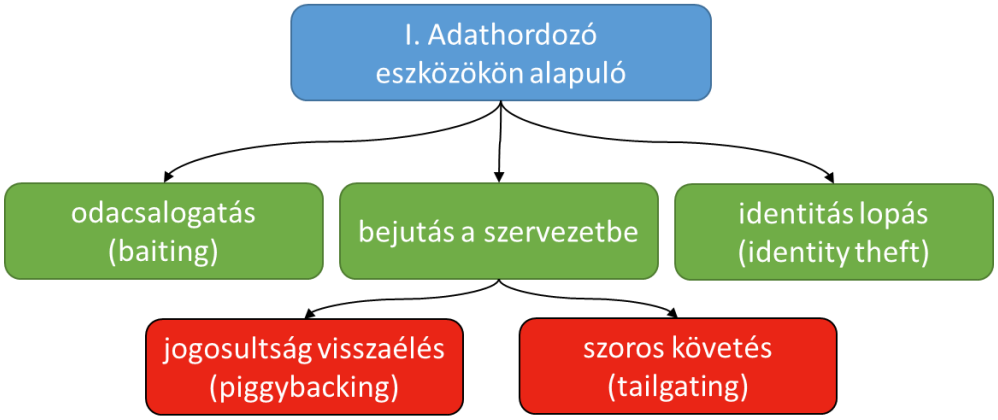
4. ábra: WannaCry zsarolóvírussal fertőzött eszközök kezdőképernyője [11]

A támadó célja a rosszindulatú programmal lehet például információszerzés, azokkal való visszaélés, a felhasználó infokommunikációs eszközének zavarása és működésképtelenné tétele, az eszköz feletti irányítás átvétele, a kártékony program terjesztése, egyéb programok telepítése, pénzszerzés és számos további a támadó egyéni céljának megfelelő tevékenység.

SOCIAL ENGINEERING TECHNIKÁK ROSSZINDULATÚ PROGRAMOK TERJESZTÉSÉRE

A kártékony programok sok esetben social engineering támadások részeként terjednek, illetve aktiválódnak, hiszen rendszerint a felhasználók felelősek a rosszindulatú programok terjedéséért és aktiválásáért. A következőkben bemutatom azokat a social engineering technikákat, melyek hozzájárulnak a különféle kártékony programok terjedéséhez és működéséhez. Célszerű a social engineering módszerek és a rosszindulatú programok kapcsolatát egy új csoportosítás szemszögéből vizsgálni aszerint, hogy milyen módon és milyen social engineering technika által kerül a célszemély infokommunikációs eszközére a rosszindulatú program. A következőkben egy általam kidolgozott csoportosítás bemutatására kerül sor.

Az ***5. ábra*** szemlélteti az *első csoportot, mely* azon social engineering technikákat tartalmazza, amelyek adathordozó eszközök által teszik lehetővé a kártékony programok terjedését.



5. ábra: Az adathordozó eszközökön alapuló kártékony program terjesztés (Saját szerkesztés)

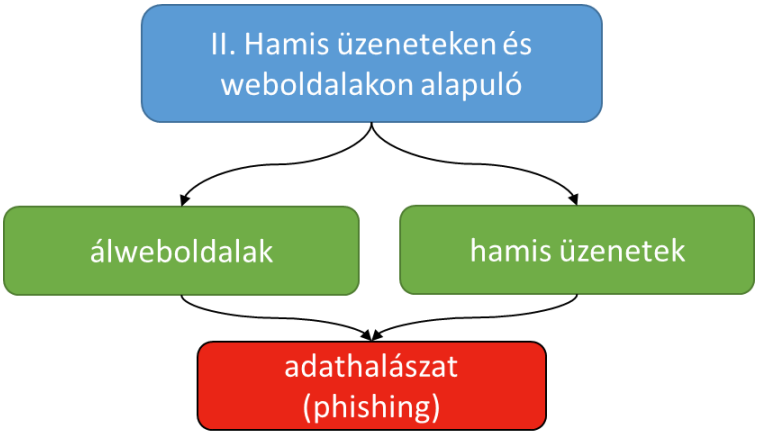
Az első ilyen módszer a „*baiting*”, mely elsősorban a felhasználók kíváncsiságát hivatott kihasználni. A baiting szó, magyarul odacsalogatást jelent, a technika lényege, hogy a támadó valamilyen adathordozó eszközt (CD, DVD, pendrive, SD kártya stb.) elhagy, azt remélve, hogy a célszemély, aki megtalálja az eszközt csatlakoztatni fogja számítógépéhez a kíváncsiság jegyében, hogy kiderítse kié lehet, majd a csatlakoztatást követően az adathordozón lévő fájl megnyitásával már települ is a rosszindulatú program az áldozat számítógépére. Előfordul, hogy a támadó valamilyen figyelemfelkeltő felirattal látja el az adott adathordozót (pl. egy DC-t, DVD-t), annak érdekében, hogy a célszemély mindenképpen csatlakoztassa azt az eszközéhez. Sok esetben a támadók szoftverfrissítésként vagy egy általános szoftverként, programként álcázzák a rosszindulatú programot, hogy a felhasználó gyanakvás nélkül megnyissa az adathordozón található fájlt. [13]

A következő technika a „*bejutás a szervezet épületébe*”, mely során a támadó, valamilyen egyéb módszer segítségével, a biztonsági ellenőrzéseket kijátszva jogosulatlanul, fizikailag bejut a szervezet létesítményeibe. A bejutás történhet a „*tailgating*” vagy a „*piggybacking*” módszerek segítségével. A tailgating, vagyis másnéven „szoros követés” módszer során a támadó a szervezetbe történő belépéskor egy csoporthoz kapcsolódik szorosan, és úgy tesz, mintha annak tagja lenne. [14] Ehhez a technikához némi előkészület szükséges, meg kell érdeklődni, hogy mikor jön az adott társaság, és hogy maga a csoport milyen típusú, hiszen nem mindegy, hogy a támadónak milyen közösséghez kell alkalmazkodnia, mind a ruházat, a felszerelés, az eszközök és a viselkedés tekintetében. A csoport lehet például egy takarítóbrigád, építőipari munkások, karbantartók, vagy akár egy másik szervezet alkalmazottaiból álló társaság is. A piggybacking módszerben a támadónak nincs belépési jogosultsága az adott helyre, ezért kiadja magát egy másik személynek, akinek van, és jogosultságát felhasználva jut be a szervezet épületébe. [15: 206–208] Például a támadó eljátssza, hogy otthon hagyta a kulcsát vagy a belépőkártyáját, és megkéri a biztonsági őrt, hogy engedjék be vagy megkér a szervezetben dolgozó alkalmazottat, hogy a saját kártyájával engedje be a támadót, mert ő elfelejtette magával hozni. Az is előfordulhat, hogy a támadó hamis belépőkártyával jut be az adott épületbe, amely esetében előzetesen meg kell vizsgálni, hogy van-e valamilyen beléptető rendszer az intézményben, ugyanis, ha igen, akkor csak speciális technika segítségével másolható le a szervezet belépőkártyája. [14]

A bejutás a szervezet épületébe technikái szorosan kapcsolódnak az „*identitás lopás*” [16: 49] vagy másnéven „*identity theft*” módszerhez, hiszen az esetek döntő többségében amikor a támadó belép a célszervezet épületébe, nem a saját személyazonosságát használja, hanem valaki mást személyesít meg. Tökéletes példa erre a futárnak való álcázás esete, amikor a támadó a kézbesítő szerepetét veszi fel, ennek megfelelően választja ki ruházatát és valamilyen csomagot hozva szeretne bejutni a létesítménybe. Eljátssza, hogy egy nehéz csomagot cipel és megkér

valakit, hogy nyissa ki az ajtót neki, az esetek jelentős részében az alkalmazottak készségesen beengedik a futárt, ennek következtében pedig mindenféle személyazonosítás nélkül képes bejutni a támadó az épületbe. De ezen kívül a támadónak szános lehetősége nyílik a megszemélyesítésre, így például takarító, karbantartó, építőipari munkás, rendszergazda/IT szakember, új munkatárs, elbocsájtott, felmondott munkatárs, másik osztály, részleg munkatársa, vezetője, de akár egy másik partnerintézmény képviselőjének a bőrébe is bújhat.[8] A szervezet épületébe történő bejutás módszereit azért szükséges részletesen bemutatni, mert ezt követően a támadó már könnyedén mozoghat a létesítményben, így bármilyen rosszindulatú programot telepíthet valamely alkalmazott infokommunikációs eszközére. Éppen ezért a hatékony védelem kialakításáért már a bejutás megakadályozására nagy hangsúlyt kell fektetni.

A ***6. ábra*** szemlélteti, hogy a *második csoportba* sorolhatók azon social engineering módszerek, amely a hamis üzenetek és weboldalak általi megtévesztést alkalmazzák a kártékony program terjesztésére és működésbe hozatalára.



6. ábra: Hamis üzeneteken és weboldalakon alapuló kártékony program terjesztés

A *hamis üzenetek* segítségével történő megtévesztésnek két típusa van, egyrészt, ha az elektronikus üzenetet vagy valamely közösségi platformon továbbított üzenetet egy számunkra ismeretlen személytől kapjuk, másrészt, ha egy ismerőstől, baráttól, munkatárstól. Az ismeretlen személyektől érkező levelek egyik alapja lehet a *phishing* technika, amely a technológiai sajátosságok és az emberi tényező hiszékenységének, illetve naivitásának együttes kihasználásán alapszik. [17] A módszer lényege abban rejlik, hogy az adathalászok a felhasználókat, valamilyen elektronikus csatornán keresztül, egy látszólag teljesen eredeti, valójában pedig egy hamis weboldalra irányítják, ahol arra kérik, hogy adja meg bizalmas adatait, például felhasználóneveket, jelszavakat, bankkártya adatokat, telefonszámokat, címeket, valamint egyéb személyes adatokat. [16]

Azonban ez a támadás nem csak személyes és bizalmas adatok megszerzésére szolgálhat, hanem egy fertőzött adathalász oldal megnyitásával saját eszközünket is tovább fertőzhetjük. A technika előnye, hogy ezen weboldalak megfertőzésével a támadó sokkal egyszerűbben és gyorsabban el tudja érni a felhasználókat, mint az áldozatok infokommunikációs eszközeinek egyesével történő megfertőzése esetén. A fertőzött weboldalakon keresztül pedig számos rosszindulatú program terjed, amely segítségével a támadó képes átvenni az irányítást a böngészők felett, programkódokat futtathat a megfertőzött gépen, valamint további vírusokat is telepíthet.

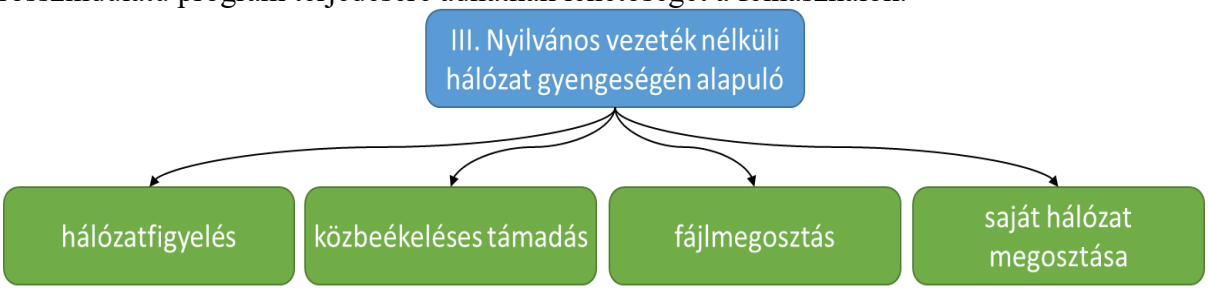
Sok esetben a felhasználó kap egy e-mailt, melyben egy valójában még nem létező technikai problémára, hibára vagy esetleg egy új frissítési, javítási lehetőségre hívja fel a figyelmet a támadó, – akár például egy szoftvereket fejlesztő cég nevében – a felmerült probléma orvoslása

érdekében rosszindulatú kódokat vagy távoli hozzáférést biztosító weboldalakra irányítják a felhasználót, amely által könnyedén irányítás alá vonható, illetve megfertőzhető a célszemély infokommunikációs eszköze. [18]

Előfordulhat, hogy egy ismeretlen személytől érkező üzenet, amely valamilyen ünnepi jókívánságot (pl. karácsonyi, születésnapi, névnapi képeslap) tartalmaz, akkor azt is automatikusan megnyitjuk a kíváncsiság jegyében, hogy vajon ki kedveskedhetett nekünk és mivel.

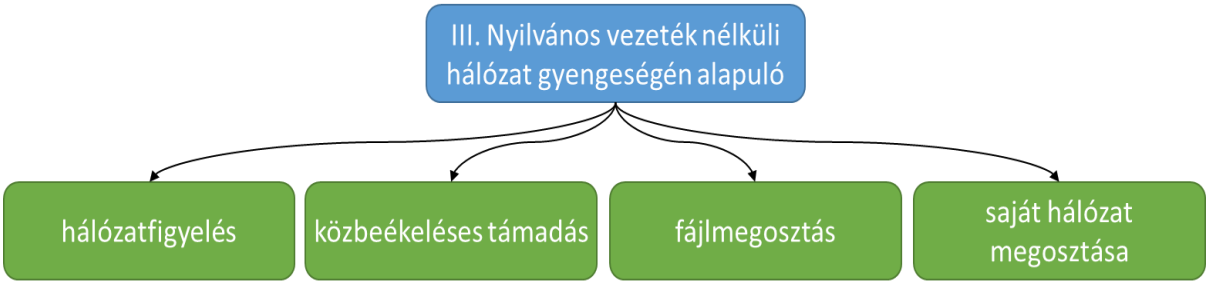
Az üzenetek másik nagy típusát a számunkra ismerős személyektől érkező üzenetek alkotják. Ebben az esetben a támadó valamelyik ismerősünket, barátunkat, rokonunkat vagy akár valamelyik munkatársunkat személyesíti meg, például csinál egy az eredeti személy e-mail címével majdnem teljesen megegyező címet és erről küld a célszemélynek üzenetet. Ez lehet sürgős segítségkérés, egy fontos tény közlése, egy kedveskedő üzenet, munkahelyi feladat kiadása, munkahelyi eseményről történő értesítés, ünnepi jókívánság, de számtalan további figyelemfelkeltő tartalommal ellátható az adott üzenet. Azért nagyon veszélyes ez a technika, mert eszünkbe se jut, hogy ez egy veszélyforrás, hiszen egy megbízható személytől kaptuk az üzenetet. Ahhoz pedig, hogy a támadó hiteles legyen, elég csak megnézni az alkalmazott közösségi oldalát, és rögtön talál számtalan barátot, munkatársat, rokont, akiket alapul véve elküldheti a rosszindulatú kódot tartalmazó fájlt vagy linket. [1: 96–98] A technika alapja, hogy a támadó valamilyen figyelemfelkeltő indokkal arra kéri a felhasználót, hogy nyissa meg a csatolmányt, mert az valamilyen fontos dokumentumot, képet, linket, vagy egyéb fájlt tartalmaz, amit mindenféleképpen látnia kell, és azzal, hogy a felhasználó megnyitja azt, a kártékony program már aktiválódik is.

A *hamis weboldalak* kapcsán érdemes megemlíteni az oldalakon elhelyezett különféle érdekes, izgalmas tartalmat ígérő reklámokat, amelyek megnyitásával szintén számos rosszindulatú program terjedésére adhatnak lehetőséget a felhasználók.



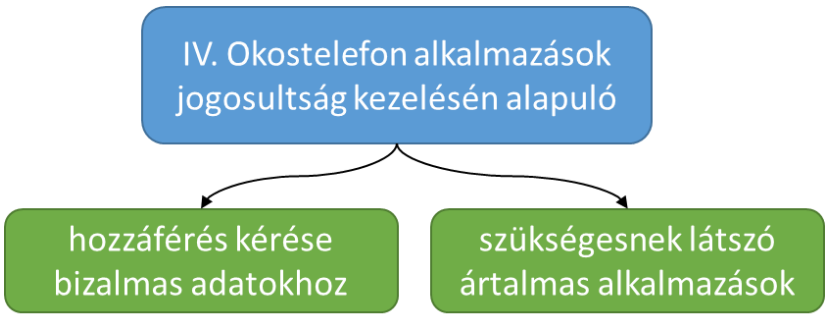
7. ábra: Nyilvános vezeték nélküli hálózat gyengeségén alapuló kártékony program terjesztés (Saját szerkesztés)

A



7. ábra alapján a *harmadik csoportot* a *nyilvános vezeték nélküli hálózat* gyengeséget kihasználó social engineering technika alkotja, amely során a támadó vagy megtámad egy gyenge védelemmel rendelkező nyílt WiFi-hálózatot és annak segítségével fertőzi meg áldozatai eszközeit, vagy azzal téveszti meg a célszemélyt, hogy egy az eredetivel (a hálózat nevével is) szinte teljesen megegyező, nagy jelerősségű csatlakozási pontot hoz létre, ezáltal a felhasználó nem biztos, hogy meg tudja különböztetni a két hálózat közötti különbséget, így automatikusan a nagyobb jelerősségű hotspothoz fog kapcsolódni. [19] A nyílt hozzáférésű WiFi-hálózatok

veszélyei közé sorolhatók a hálózatfigyelés, közbeékeléses támadás (amikor a két fél valójában nem egymással, hanem csak a támadóval kommunikál és ilyenkor minden információ a támadón keresztül továbbítódik a felek között), illetve a fájlmegosztás és rosszindulatú programok. Ez utóbbi módszert a támadók gyakran alkalmazzák kártékony programok terjesztésére vagy fájlok ellopására, hiszen, ha a felhasználó a csatlakozás során nem tiltja le a fájlmegosztás, abban az esetben mások számára elérhetővé válik a hálózaton. Ezáltal a támadó nem csak lemásolhatja az eszközön lévő fájlokat, de fel is tölthet fertőzött fájlokat vagy kártékony programokat az eszközre, illetve hozzáfér minden információhoz, amit a felhasználó elküld az interneten, így nevezetesen az e-mailekhez, bankkártya adatokhoz, azonosítókhoz, felhasználónevekhez vagy jelszavakhoz. [20]



8. ábra: Okostelefon alkalmazások jogosultság kezelésén alapuló kártékony program terjesztés (Saját szerkesztés)

A *negyedik csoportba* sorolhatók az *okostelefon alkalmazások jogosultságait kihasználó* social engineering támadások, amelyet a ***8***. ábra***8. ábra*** szemléltet. A különböző letölthető alkalmazások, - sokszor olyanok is, amelyek alapértelmezett alkalmazások, tehát alapból telepítve vannak a telefonjainkra – a használatukért cserébe számtalan olyan adathoz fér hozzá, amely bizalmas számunkra (pl. tartózkodási hely, névjegyek, üzenetek, hívásadatok, képek, videók, kamera, SD kártya, telefon tartalma stb.). E módszer segítségével a kártékony programokkal fertőzött alkalmazás letöltését és telepítését követően rosszindulatú program által a támadó képes felhasználói jogokat szerezni, ezáltal pedig alkalmazásokat, programokat telepíteni a telefonra, módosíthatja a telefon és az SD kártya tartalmát, de akár hozzáférhet az e-mailekhez, illetve banki adatokhoz is. [21]

Fontos, hogy a social engineering technikákon kívül további módszereken keresztül is megfertőződhet a felhasználó infokommunikációs eszköze. Ez történhet úgy például, ha a felhasználó a felhőszolgáltatás segítségével szeretné vezérelni az eszközét, és az ahhoz szükséges utasításkészlet segítségével azonban biztonsági réseket hoznak létre, amelyeket a támadók ki tudnak használni és ezáltal ellenőrzést szerezhetnek az eszköz felett. [22] Azonban jelen tanulmánynak nem célja az ehhez hasonló támadási módszerek összegyűjtése, így ezen technikák bemutatására nem kerül sor.

A fentebb említett támadási módszerek és egyéb bizalmas információk megszerzésére irányuló támadások esetében egyaránt biztosítani kell az adatok sértetlenségét, bizalmasságát és rendelkezésre állását a megfelelő védelem érdekében. A bizalmasság alapján az információt csak az arra jogosultak és csak a jogosultságuk szintje szerint használhatják fel, illetve rendelkezhetnek a felhasználásról. A sértetlenség az információk és a feldolgozási módszerek teljességének és pontosságának megőrzését és az illetéktelen módosítások kizárását foglalja magában. A rendelkezésre állás szerint az információknak kellő időben, illetve helyen, a jogosultak számára elérhetőnek és felhasználhatónak kell lennie, valamint elvesztésük, megsemmisülésük valószínűségét minimalizálni kell. [23] Kizárólag ezen feltételek együttes

teljesülése esetén beszélhetünk az információ megfelelő és hatékony védelmi mechanizmusáról.

KÖVETKEZTETÉSEK

Összességében megállapítható, hogy a social engineering támadás fajtájától függetlenül annak sikeres végrehajtása két tényezőn múlik, egyrészt az informatikai eszközök és rendszerek sebezhetőségén, valamint a felhasználók biztonságtudatossági ismeretein és azok megfelelő alkalmazásán. Éppen ezért a megelőző proaktív védelem kialakítása minden kétséget kizáróan nélkülözhetetlen egy szervezet életében, hiszen a hatékony és eredményes védelem megvalósításának köszönhetően egy esetleg támadás bekövetkezése esetén sokkal kevesebb erőforrást kell a károk helyreállítására áldozni. Egy ilyen támadás lezajlását követően a különféle adatok, információk, alkalmazások, illetve az informatikai rendszer javítása és helyreállítása jelentős erőforrás ráfordítást igényel a szervezet részéről, amely megmutatkozik például a rááldozott költségekben, időben, illetve emberi erőforrásban is, éppen ezért kiemelt jelentőségű a megelőző védelem kialakítása. A megelőző védelem szerves részét képezi a felhasználók védelmi képességének kialakítása. E képesség hatékony és eredményes kialakítása több elemből áll. A védelmi képesség kialakításának nélkülözhetetlen összetevője a szervezet életét érintő és a mindennapok során megjelenő sebezhetőségek és kockázatok feltárása hiszen a hatékony és eredményes védekezés nem valósulhat meg a hiányosságokra történő rámutatás, majd orvoslás nélkül. [24] A sebezhetőségvizsgálatok során meg kell határozni azokat a területeket, amelyek bármiféle fenyegetést, veszélyt vagy kockázatot jelenthet a szervezet számára, és külön kiemelendő, hogy a szervezet által alkalmazott infokommunikációs eszközök, rendszerek, alkalmazások, a különféle adatok, információk, illetve a felhasználók által okozott sebezhetőségek vizsgálata elengedhetetlen ezen problémák orvoslásához. [25] A sebezhetőségek és kockázatok meghatározását követi a szükséges információbiztonsági szabályok, előírások megállapítása esetleges módosítása a hiányosságok alapján, illetve ezek betartatása. A biztonsági előírásoknak tartalmaznia kell mind az infokommunikációs eszközök és rendszerek biztonsági szabályozását, mind pedig a felhasználókat érintő irányelveket, hiszen csak ezek együttes alkalmazása teszi lehetővé a hatékony védelem kialakítását és megvalósítását. Fontos, hogy a valóságban ne csak a szabályzók elkészítése valósuljon meg, hanem a szervezet ügyeljen ezek mindennapos betartására is. A védelem kialakításának további elengedhetetlen eleme az alkalmazottak megfelelő biztonságtudatosságának kialakítása, hiszen, ha a felhasználók ismerik a lehetséges támadási és védekezési alternatívákat, akkor a különféle bizalmas információk megszerzésére irányuló támadások bekövetkezésének valószínűsége csökkenthető. A biztonságtudatosság növelésére alkalmas lehet a biztonságtudatossági képzés, amely magában foglalja az alkalmazottakra vonatkozó, a szervezet és egyéb szabályozók által előírt szabályokat, biztonsági előírásokat, a lehetséges kockázatokat, veszélyeket, támadási alternatívákat. Ezen kívül a képzésnek tartalmaznia kell az esetleges következményeket. Mindemellett a biztonságtudatosság növelését szolgálják még többek között a különféle biztonságtudatossági, információbiztonsági kampányok, programok és számítógépes, online tréningek.

A korábbiakban említett különböző támadási alternatívák megismerése és megismertetése nélkülözhetetlen a mindennapos infokommunikációs eszközök használata esetén, hiszen ezáltal jelentősen tudjuk növelni a ránk bízott információk kiszivárgását és illetéktelen felhasználását, egyúttal az állami szervek működésének stabilitását, a társadalom és a gazdaság részvevőinek biztonságát. Ezért jelen tanulmány a social engineering technikákon keresztül terjedő kártékony programok vizsgálatát tűzte ki célul. A különféle módszerek és a rosszindulatú programok kapcsolatának, összefüggéseinek elemzése elengedhetetlen a hatékony védelem kialakításához, ezért egy olyan csoportosítást hoztam létre, amely rendszerezi azon technikákat, amelyek alkalmasak a kártékony programok terjesztésére.

[17] MOHAMMAD, M. R., THABTAH, F., McCLUSKEY, L.: Tutorial and critical analysis of phishing websites methods. Computer Science Review, 17 (2015), 1–24. https://doi.org/10.1016/j.cosrev.2015.04.001 (A letöltés ideje: 2017. 10. 06.)

[18] CRIDDLE, L.: What is social engineering? webroot.com, s.d. www.webroot.com/ie/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering (A letöltés ideje: 2017. 11. 02.)

@ WATTS, S.: Secure authentication is the only solution for vulnerable public wifi. Computer Fraud & Security, 1 (2016), 18–20. https://doi.org/10.1016/ S1361-3723(16)30009-4 (A letöltés ideje: 2017. 11. 02.)

[20] KOVÁCS M.: A nyílt Wi-Fi hálózatok veszélyei. 2016. https://blog.crosssec.com/a-nyilvanos-wi-fi-halozatok-veszelyei (A letöltés ideje: 2017. 11. 02.)

[21] DUNHAM, K. (Ed.): Mobile malware attacks and defense. Burlington: Syngress, 2009.

[22] KIS E.: Fertőzésveszély a felhőben. computerworld.hu, 2014. https://computerworld.hu/uzlet/fertozesveszely-a-felhoben-151708.html (A letöltés ideje: 2017. 11. 03.)

@ 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról.

[24] SHAMELI-SENDI, A., AGHABABAEI-BARZEGAR, R., CHERIET, M.: Taxonomy of information security risk assessment (ISRA). Computers & Security 57 (2016), 14–30. https://doi.org/10.1016/j.cose.2015.11.001 (A letöltés ideje: 2017. 11. 04.)

[25] MUHA L., SZÁDECZKY T.: Irányítási rendszerek. Budapest: Nemzeti Közszolgálati Egyetem, 2014. http://vtki.uni-nke.hu/uploads/media_items/iranyitasi-rendszerek.original.pdf (2017. 09.05)