Mérnöki Szimpózium a Bánkiban
(ESB 2019)
http://bgk.uni-obuda.hu/esb/2019

A pszichológiai manipuláció jelenléte a politikában

The presence of social engineering in politics

[1]Kun Tamás

[1]*Óbudai Egyetem, Budapest, Magyarország, kun.tamas@phd.uni-obuda.hu*

Összefoglalás

Az internetes hirdetések meghatározó részei napjainkban a politikai kampányoknak, de nem csak a tájékoztatásra, befolyásolásra alkalmas eszközök vannak jelen, zsarolóvírusok terjesztése is lehet célja a kibertérben tevékenykedő szereplőknek. Változatos módszerekkel, többnyire pénzügyi haszonszerzés motivációjával a támadók széles tömegeket képesek elérni, egyre gyakrabban ismert politikai szereplőkre utaló multimédiás eszközök felhasználásával is. A technikai adottságok (adatpiacok) birtokában lévő nagyvállalatok, valamint az azokhoz való törvénytelen hozzáférési potenciállal bíró csoportok (kiberbűnözők) közötti verseny szemtanúi lehetünk a közélet informális alakítása során.

Kulcsszavak: pszichológiai manipuláció, kiberbiztonság, szociális média, befolyásolás

Abstract

Internet advertising is a reasonable element in political campaigns, as well as providing information, influence and exploration of potential opportunities, but either the distribution of ransomware could be at the aim for cyberspace actors. Through a variety of methods, which is often motivated by financial gain, the attackers can reach relevant masses, recently with the use of well-known politicians' multimedia appearance. There is rivalry between large companies with significant technical capabilities (data markets) and groups with the illegal accessing potential (cybercriminals) for these, and we are spectators of the informal shaping of politics.

Keywords: social engineering, cybersecurity, social media, influence

1 Bevezetés

Mára már meghatározó a politika jelenléte az online média felületein, elég, ha az internetes újságokra gondolunk, amelyek később a közösségi oldalakkal (pl. Facebook, Twitter) egészültek ki, a politika évek óta jelen van már az online térben is. Ez viszont lehetőséget kínál arra, hogy az egyébként legitim szándék mellett olyan szereplők is csatlakozzanak, akiknek „illegitim" csalási vagy megtévesztési céllal lépnek fel. Rosszindulatú kódok és a közvélemény befolyásolása, jellemzően ezek a kiindulópontok a kiberbűnözők számára. A másik oldalán a vizsgált témának a politikai hirdetések és az online kommunikáció állnak, középpontban az aktuálisan alkalmazott eszközök bemutatása.

2 A pszichológiai manipuláció (Social Engineering)

Centralizált tervezés útján a társadalom fejlődésébe, a jövőt illető szabályozás alakításába, valamint a társadalom reagálásának befolyásolásának a kísérlete. A megtévesztés különböző eszközeit alkalmazva személyek irányítása, mely során bizalmas vagy személyes információ birtokába való jutást követően csalási szándékkal alkalmazható. Az online és/vagy kibertérben ez a technika jellemzően adathalászati céllal jelenik meg.

Néhány támadási típus definícióit az alábbiakban ismertetem:

Adathalászat (Phishing): Hamis identitással érzékeny vagy személyes adatok kicsalása a célba vett áldozatoktól

Zsarolóvírus (Ransomware): Olyan kártékony szoftver vagy kód, amelynek célja a kiszemelt felhasználók informatikai eszközein tárolt adatok zárolása, amelyet a váltságdíj megfizetése esetén újra hozzáférhetővé tesz

Trójai programok (Trojan): Olyan kártékony szoftver vagy kód, amely hasznos programnak álcázza magát, jellemzően hozzáférési pontok feltérképezéséhez alkalmazzák

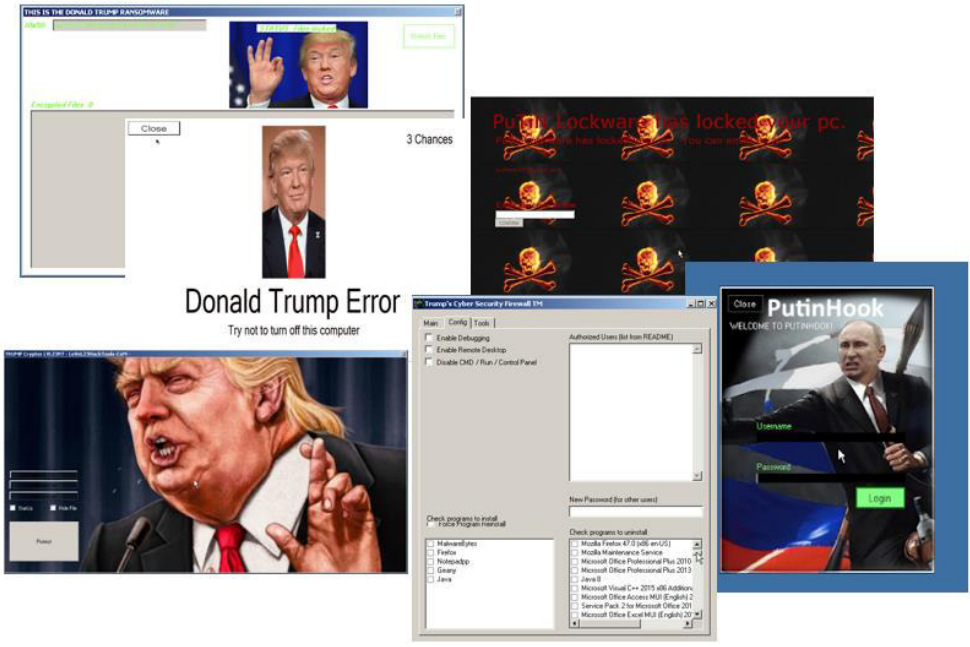
Hátsó bejárat (Backdoor): Jogosulatlan hozzáférés egy számítógéphez, rendszerhez, szolgáltatáshoz vagy adathoz, jellemzően úgy vannak elkészítve ezek a programok, hogy a felhasználók és a rendszergazdák számára észrevétlenek legyenek

(The Cyberwire, 2019)

Ezeknek a támadásoknak potenciális áldozatai többnyire olyan szervezetek és cégek, amelyek üzleti tevékenységet folytatnak, vagy működésük során értékes adatokkal dolgoznak. Tehát annak a valószínűsége, hogy egy olyan magánszemély, aki nem rendelkezik egy szervezetben meghatározó pozícióval támadás áldozatává váljon meglehetősen alacsony, viszont nem kizárható. Ezeknek a személyeknek csoportja többnyire automatizált eszközökkel van célba véve és a „nagy számok törvényére" alapoz. A támadások egy másik oldalról megközelített bontásában beszélhetünk **adatlopásról (information theft)** ebben az esetben a támadó értékes üzleti titkok, ügyféladatok, szellemi tulajdon stb. megszerzésére törekszik, beszélhetünk **megfigyelésről (monitoring)**, amely során az áldozat tevékenységének nyomon követésével jut információhoz, és **szabotálásról (sabotage)**, amikor a támadó célja az áldozat lejáratása, vagy adott esetben egy személy vagy szervezet javaiban való károkozás. A támadók jellemzően **pénzügyi haszonszerzés** céljával indítanak támadásokat, azonban nem szabad elfelejteni a kibertérben zajló műveletek katonai jellegét sem. A kritikus infrastruktúrák, amelyek nemzetbiztonsági kockázatot jelentenek (energiaszektor, pénzügyi szektor, egészségügy, légi és földi forgalom stb.) ellen intézett támadások esetében már nem beszélhetünk kizárólag kereseti lehetőségekről, komoly politikai indíttatások vannak jelen a háttérben.

2.1 A Talos Group felmérése

Az Egyesült Államokban a Cisco Talos nemrégiben detektált néhány malware terjesztéssel kapcsolatos esetet, ahol a támadók szervezetten politikai szereplőkkel hirdettek, különösképpen az amerikai elnökkel, Donald Trumppal. A vírusok szerzői többek között ransomware és trójai típusok is megjelentek, mely előbbi díjfizetésre kényszeríti az áldozatot és zárolja, valamint titkosítja az adatokat, a trójai esetében pedig rejtett hozzáféréssel hátsó bejáratot biztosít egy szervezeten belüli hálózathoz. Az alábbi képen (1. ábra) néhány zsarolóvírus (Trump Crypter, PutinHook stb) és egy trójai program (Trump Cyber Security Firewall) látható, amely igyekszik az áldozattal elhitetni, hogy az említett politikai szereplők felelősek a számítógép zárolásáért vagy működésének kompromitálásáért. (Biasini & Brumaghin, 2019)



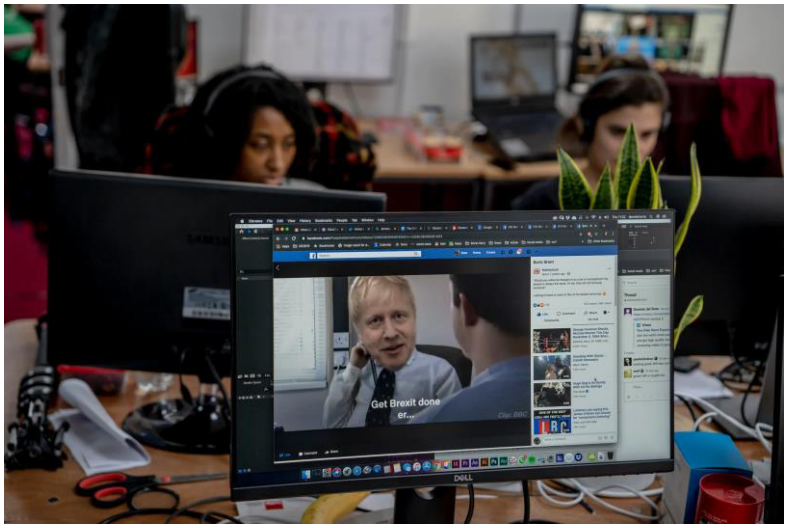
1. ábra - Malware/Ransomware 2020 (Biasini & Brumaghin, 2019)

Már előre szólnak a találgatások, hogy a 2020-ban megrendezésre kerülő amerikai elnökválasztáson lesz-e olyan körülmény, mint amilyen 2016-ban volt, ami kétségbe vonná a választás lezajlásának tisztaságát. A félrevezetés ebben az esetben is véleményem szerint az, hogy a cél manapság nem az eredmények meghamisítása, hanem a folyamatokba való beavatkozás és a közvélemény hozzáállásának és reagálásának a formálása. Ugyanis ha abból indulunk ki, hogy egy választás eredménye hamis, azaz nem tükrözi a választópolgárok kinyilvánított akaratát, akkor szükségszerűen meg kellene jelennie egy reakciónak (releváns utcai zavargások, magas létszámú tüntetések, sztrájk stb.) ami igazolná, hogy csalás történt. Ha eleve a közhangulat kerül befolyásolásra, akkor a törvényi keretek között a legitim játékszabályok feltételezett betartása (amennyiben észrevétlenül maradnak a háttérben az adatközpontok felépítései, monitorizálások, szavazólisták készítése jogosulatlan adatszerzés mellett stb.) valósíthatók meg a kívánt kimenetek. Ebben az esetben már nem beszélhetünk az eredmények tükrében csalásról, viszont hogy ezt az eredményt milyen eszközök alkalmazása révén érjük el, meglehetősen vitatható.

3 A pszichológiai manipuláció alkalmazása a politikában

Egy esetleges külföldi beavatkozás híresztelése az online megtévesztés egyik leghatékonyabb forrása volt régebben sorsdöntő választások előtt. Most azoban néhány jelölt maga is ilyen manipulációs taktikához fordult a brit választási kampányban. Hamis Twitter-fiókok, manipulált videók, trükkös weboldalak és természetesen a választásokba beavatkozó külföldi érdekeltségek kérdése is az asztalon volt. A választópolgárok egy „szelíd ízelítőt" kaptak az online kampányolás által nyújtott lehetőségek tárházából egy olyan fontos választás előtt, amely egy generáció sorsát döntheti el. (Satariano & Tsang, 2019)

A lejáratás (blackmailing) egyik tipikus eszköze a szabotálásnak (sabotage). Jelen esetben a technika alkalmazásán van a hangsúly a politikában, legális forrásokon keresztül. Ismert politikai szereplő, ismert filmrészlet vagy jelenet (könnyebb azonosítás, amely segít a terjesztésben) és az időzítés, amely jellemzően a leginteraktívabb időszakban, a választási hajrában az utolsó héten jelenik meg.



2. ábra - A brit Munkáspárt dezinformációs kampányvideójának pillanatképe (Satariano & Tsang, 2019)

A Momentum (a brit Munkáspárt lobbiszervezete) által megszerkesztett videóban (2. ábra) a brit konzervatívok jelöltjét egy divatmagazin szerkesztőjének szerepébe öltöztették, melyhez tartozó hanganyagot Boris Johnson saját kampányvideója szolgáltatott, annyi különbséggel, hogy úgy szerkesztették meg a videót, hogy a végén Jeremy Corbynt javasolja a következő miniszterelnöknek.

Az internet adta lehetőségek között ott szerepel az is, hogy ezeknek a dolgoknak nem csupán a terjesztése adott, hanem utána is tudunk járni viszonylag gyorsan és egyszerűen a hírek valódiságának. Nem árt, hogy ha több forrásból tájékozódunk, összevetjük egymással őket, majd ezek után formálunk véleményt. Ez nem jelenti azt, hogy minden, amit elénk tesznek az csak és kizárólag megtévesztő jellegű, viszont tudni kell olvasni a sorok között. A példának bemutatott videón még jól fellelhető, hogy manipulált dologról van szó, azonban rendelkezésre állnak olyan szerkesztési metodikák is, amelyeknél a szerkesztés ténye messze nem ennyire szembetűnő.

3.1 A közösségi médiában a politikai hirdetések létjogosultságának kérdése

A brit Guardianban jelent meg egy cikk a politikai hirdetések szereplésével kapcsolatban az online térben, mely cikkben a szerzők azt részletezik, hogy a politikai pártoknak el kellene számolniuk a közvélemény felé a finanszírozott hirdetések helyéről, tárgyáról és azok árával kapcsolatban a tiszta verseny érdekében. Számos szabályozási rés van azonban, amelyet a közösségi média felületek birtoklói és az adatbrókerek jó üzleti lehetőségnek tekintenek. A digitális poilitikai hirdetések piaca különbözik a hagyományos nyomtatott vagy televízióban sugárzott eszközöktől, mert az új generációs hirdetések adat alapúak, amelyek személyre szabottan fogyasztói magatartás függvényében jól szegmentálhatók a lakosságon belül. Nem lehetünk biztosak abban, hogy a környezetünk ugyanazokat a tartalmakat kapják, mint mi magunk, így fennáll a veszélye konfliktusok generálódásának számára, mert az egyes hirdetések más-más hallgatóságnak vannak címezve (politikai táborok). Az adat alapú hirdetések és a tartalom marketing multimilliárd dolláros iparággá nőtte ki magát az utóbbi években és a politikai pártok, valamint a hozzájuk kapcsolódó csoportok komolys összegeket fektetnek ebbe. (Neudert & Howard, 2019)

3. ábra - A brit Konzervatív Párt dezinformációs kampányvideójának pillanatképe (Neudert & Howard, 2019)

Ebben a videóban (3. ábra) a brit Konzervatív Párt azt állította a brit Munkáspárt képviselőről, hogy a pártnak nincs valós forgatókönyve a Brexit tárgyalások rendezéséről, az eredeti interjúban a riporter kérdésére adott választ egy néma hallgatásra és pisolgásra cserélve, benne a konzervatívok politikai üzenetével.

Fontos itt megjegyezni, hogy ebben az esetben látszólag minden szereplő egymásra mutat, viszont a szálak összeérnek. A brit kampányban a két jelentősebb párt, a Konzervatív Párt és a Munkáspárt egyaránt alkalmazta a rendelkezésre álló eszközöket a siker érdekében. Ami viszont lényegében változtatja meg a dolgokat az pedig az, hogy a nagy adathalmazok birtokában lévő szervezetek a technológiai szektorban jelentős befolyással bírnak a közhangulat alakításában, hiszen ezeken a felületeken jelennek meg a hirdetések, ők moderálják a tartalmat, valamint a választópolgárok adófizetői pénzét teszik el a szolgáltatásuk nyújtása során, az fizeti a számlát, akit befolyásolni szeretnének a valótlan tartalmakkal. Így a felvetés jogos lenne a választók részéről, hogy mégis mennyibe kerül ez nekik.

4 Konklúzió

A tudatos internethasználat és a körültekintő (kritikus megközelítésű) szemléletmód fontos

szerepet játszanak abban, hogy döntésképesek tudjunk lenni. Ez alatt azt értjük, hogy bár a szükséges információ teljes mértékben nem áll rendelkezésünkre (tehát nem vagyunk szakemberek), viszont elegendő mennyiségű tudás birtokában vagyunk azonban ahhoz, hogy egy esetleges csalást felismerjünk. Az óvatosság tárgya ebben az esetben nem az attól való rettegés, hogy csalás áldozatává válunk, hanem azt kell jelentenie, hogy tisztában vagyunk ennek a lehetőségével („benne van a pakliban"), ezért szükségszerűen kellő körültekintéssel járunk el bármely olyan eszköz használata során, amikor olyan adatok megadásáról, megosztásáról vagy adott esetben kezeléséről van szó, mely illetéktelen kezekben jelentős károkat okozhat magunk vagy mások számára. Itt kiemelném a munkahelyeken kezelt adatok körét, ahol véleményem szerint nem a végtelenségig szigorított szabályozás fogja meghozni a kívánt eredményt, hanem a kialakított bizalom, valamint az, hogy a munkavállaló legalább két három lépéssel képes legyen tovább gondolni egy adatszivárgás következményeit és saját felelősségét, és adott esetben reagálni tudjon egy elkövetett hibájára. A magánéletünkben is rendkívül fontos, hogy olyan területeken, mint a pénzügyeink (online banki tranzakciók, lekérdezések, ügyintézés stb.) értenünk kell a folyamatok alapvető működését, ez által védekezni is képesek vagyunk csalási szándékú megkeresések ellen.

A kommunikációs trendek fejlődésében újszerű dolog, hogy az élő közvetítés (egy választási műsor eredményvárója) mellett ma már kommentfolyam (hozzászólási felület) is szerepel a weben, ahol a választópolgárok valós időben szólhatnak hozzá a közvetítéshez, ez pedig lehetőséget teremt arra is, hogy a létező felhasználók mellett mesterséges intelligencia által vezérelt chatbotok (csevegő számítógépek) véleménye is bekerüljön a diskurzusba. Ez utóbbi azért lehet lényeges, mert még a legutolsó pillanatban is generálható kommunikációs zaj a döntési folyamatban, de alkalmas arra is, hogy a passzív rétegből (azok a választópolgárok, akik rendszerint nem vesznek részt a választásokon) mozgásra késztesse őket.

Mindig az ember lesz a szűk keresztmetszet a biztonsági kérdésekben, hiszen az érdekérvényesítési szándék nem gépi természetű. Nap, mint nap egyre több adat generálódik a világban és az összefüggési pontokat csak „megfelelő szűrők" segítségével lehet kimutatni. Ma is és a jövőben is az egyik legfontosabb pillére lesz az életünknek, hogy különbséget tudjunk tenni a valós és a fiktív hírek, hirdetések vagy puszta vélemények tekintetében, a manipulatív technikák és a technológia fejlődésével a kreált valóságok egyre élethűbbé válnak, amíg végleg el nem tűnik a határ a realitás és a virtualitás között.

5 Hivatkozások

[1] Biasini, N., & Brumaghin, E. (2019. 11 05). *How adversaries use politics for compromise*. Forrás: https://blog.talosintelligence.com/2019/11/political-malware.html

[2] Neudert, L.-M., & Howard, P. (2019. 11 11). *Online politics needs to be cleaned up – but not just by Facebook and Twitter*. Forrás: https://www.theguardian.com/commentisfree/2019/nov/11/online-politics-facebook-twitter-social-media-political-parties

[3] Satariano, A., & Tsang, A. (2019. 12 10). *Who's Spreading Disinformation in U.K. Election? You Might Be Surprised*. Forrás: https://www.nytimes.com/2019/12/10/world/europe/elections-disinformation-social-media.html

[4] The Cyberwire. (2019. 12 11). *Glossary*. Forrás: https://thecyberwire.com/glossary.html