CTI Jelentés

Mobile Security Threats

(Mobilfenyegetettségek)

NEMZETBIZTONSÁGI SZAKSZOLGÁLAT

NEMZETI KIBERVÉDELMI INTÉZET

Bevezetés

Bár az okostelefon feltalálása az IBM-hez köthető, amikor 1992-ben megalkották az első ilyen készüléket (Simon Personal Communicator), a hétköznapi használatban ez jóval később, a 2000-es évek közepén terjedt el. Az összes gyártót számba véve 2006-ban körülbelül 100 millió eszközt adtak el. Ez évről évre rendkívüli mértékben nőtt egészen 2016-ig, amikor elérte és azóta is megközelítőleg tartja az évi 1,5 milliárd eladott eszközt. Jelenleg a Föld lakosságának több mint 70%-a, 5 milliárd ember birtokol legalább egy ilyen telefont. Míg kezdetben leginkább a fiatalok használtak okostelefont, ez mostanra teljesen megváltozott és minden korosztály számára egy általános és hétköznapi eszközzé vált. Az egyre bővülő felhasználói közösség velejárója sajnos az is hogy ezek a felhasználók nem minden esetben kezelik megfelelő tudatossággal az eszközeiket, amelyet a kiberbűnözők igyekeznek is kihasználni, hogy anyagi és más javakat szerezzenek mások naivitásából és figyelmetlenségéből fakadóan.

Jelen dokumentum célja, hogy ismertesse az olvasóval a mindennapos telefonhasználat veszélyeit és a különféle kockázatokat, amelyek a nem tudatos felhasználói magatartásból eredhetnek. Mivel a mai okostelefonok már miniszámítógépeknek minősülnek és hasonló folyamatokat tudunk velük elvégezni (bankolás, emailezés, közösségi tevékenységek stb.) mint egy számítógépen (PC, laptop stb.), ezért sok hasonlóság van a két fajta eszköz között a ránk leselkedő biztonsági fenyegetéseket tekintve. Természetesen egy az egyben nem feleltethető meg az egyik eszköz a másiknak, de olyan információkkal gazdagodhat az olvasó, amelyeket számítógéphasználat közben is kamatoztathat.

Tartalomjegyzék

Veszélyforrások

A mobilbiztonsági fenyegetésekre általában az emberek egyetlen, mindent átfogó fenyegetésként gondolnak, de valójában ezeket négy különböző kategóriába lehet sorolni:

- **A mobilalkalmazások biztonsági fenyegetései:** Az alkalmazásalapú fenyegetések akkor fordulnak elő, amikor az emberek olyan alkalmazásokat töltenek le, amelyek legitimnek tűnnek, de valójában adatokat szivárogtatnak a háttérben a készülékükről a csalók számára. Ilyenek például a kémprogramok és a rosszindulatú programok, amelyek segítségével személyes és üzleti információkat lopnak el az emberek észrevétele nélkül.
- **Webalapú mobilbiztonsági fenyegetések:** A csalók saját weblapokat hoznak létre és a céljuk, hogy valamilyen formában ide irányítsák az áldozataikat. Miután ez megvalósult, valamilyen felhasználói interakció során a háttérben rosszindulatú fájlok töltődhetnek le az eszközre vagy a csalók számára értékes, hozzánk tartozó érzékeny adatokat küldhetünk észrevétlenül. Az adathalász technikák közül a legtöbb ide sorolható.
- **Hálózati biztonsági fenyegetések:** A hálózati alapú fenyegetések különösen gyakoriak és kockázatosak, mivel a kiberbűnözők kódolatlan adatokat lophatnak el. A legtöbb esetben ezt nyilvános WiFi hálózatokon keresztül hajtják végre, de a rosszul beállított otthoni hálózat is célpont és eszköz lehet a felhasználó ellen.

- **Mobileszköz biztonsági fenyegetések:** Nem túl gyakori, de semmiképpen sem elhanyagolható a fizikai fenyegetettség: ha az eszköz elvesztésére vagy ellopására kerül és egy hacker kezébe kerül, közvetlenül hozzáférhet a hardverhez, ahol a személyes adatokat, jelszókat, banki adatokat és egyéb érzékeny információkat tárolja a felhasználó.

Pszichológiai manipuláció (Social engineering)

A pszichológiai manipuláció a támadások egy olyan típusa, amikor elsősorban **nem technikai oldalról** valósul meg a behatolás, hanem az **emberi hiszékenységet és/vagy segítőkészséget kihasználva** történik meg a rendszer kompromittálása. A támadó igyekszik elnyerni az áldozata bizalmát, aki egy sikeres támadás esetén olyan dolgokat tesz meg amit a csaló eredetileg akart. A pszichológiai manipulációs támadások leggyakoribb csatornái: telefonhívás, SMS, Facebook, Twitter és különféle chat alkalmazások.

A legmegfelelőbb **védekezési módszer a józan ész használata**. Érdemes kételkedve fogadni minden olyan megkeresést, amikor a másik felet nem ismerjük. Ezek a bűnözők minden esetben arra építenek és a beszélgetés elején már határozottan lépnek fel annak érdekében, hogy az áldozat ne kérdőjelezze meg a megkereső hitelességét. Leginkább az emberi félelmet, segítőkészséget, kíváncsiságot vagy türelmetlenséget célozzák.

Gyakran olyan szakzsargont, kifejezéseket használnak, amivel azonnal azt az érzést keltik az emberben, hogy tényleg az általa említett cég nevében (telekommunikációs cég, közműszolgáltató stb.) történt a megkeresés és segíteni szeretne a további problémák elkerülése érdekében. Érdemes átgondolni, hogy valóban kapcsolatban állunk-e az említett céggel. Ha igen, a legjobb módszer, ha megkeressük a szolgáltató központi ügyfélszolgálatának a telefonszámát és mi hívjuk vissza az említett problémával. Természetesen előfordulhat az is hogy ténylegesen az adott cégtől történt a megkeresés, de ha elkövetünk mindent annak érdekében, hogy megbizonyosodjunk a probléma valódiságáról, senkinek sem ártunk, csak magunkat kíméljük meg egy sor további kellemetlenségtől. Kezeljük higgadtsággal az ilyen megkereséseket és ne hagyjuk magunkat becsapni!

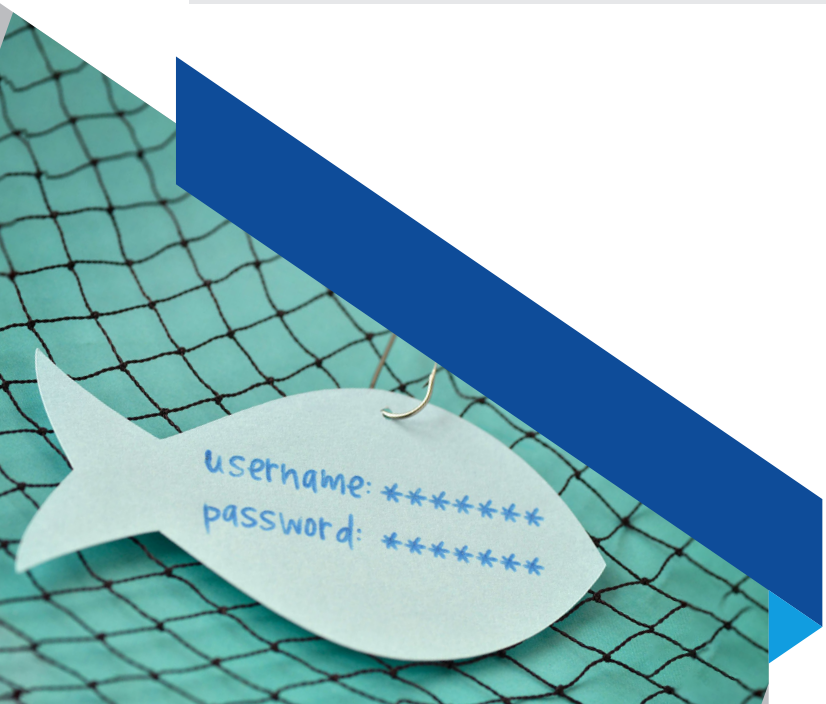
Adathalászat (Phishing)

Napjaink komoly informatikai fenyegetései közé tartozik az adathalász tevékenység. A phishing szó a „password" és a „fishing" szavakból tevődik össze, ami annyit jelent, hogy jelszavakra halászni. Az adathalászathoz a támadók változatos módszereket használnak, így egyre gyakrabban hamisítanak e-maileket vagy weboldalakat, ezzel próbálva a felhasználókat rávenni bizalmas adatok (jelszavak, hozzáférési adatok, bankkártyaszámok, speciális céges adatok stb.) kiszivárogtatására, amelyet a későbbiekben a támadó felhasznál. A megkeresés történhet telefonon, SMS-ben vagy e-mail-en.

Három fő kategóriája van:

- Az első amikor **tömeges, nem célzott** a támadás. Ilyenkor rengeteg embernek küldik ki ugyanazt a levelet vagy SMS-t. Ha 1000 kiküldött példányból csak egy felhasználó "akad horogra", az már sikeres támadásnak mondható. A hatékonysága a felhasználó tudatosságán és éberségén felül, legfőképpen a levél szerkezetén és a megfogalmazás módján múlik.

*2021. márciusában SMS-ben terjedni kezdett Magyarországon a **FluBot nevű kártevő**, amely káros hivatkozást tartalmazott és látszólag egy csomagküldő szolgáltatótól származott. A hivatkozásra kattintva egy olyan weboldal jelenítődött meg, amely rendkívül jól utánozta valamely nemzetközileg ismert futárszolgálat arculati elemeit. Az oldal egy **alkalmazás letöltésére akarta rávenni a felhasználót** arra hivatkozva, hogy a csomagját nyomon tudja vele követni. Amennyiben a felhasználó letöltötte az alkalmazást, egy **adatlopó** képességekkel ellátott vírus, az úgy nevezetett FluBot települt az eszközre. A csalók a vírus települése után hozzáfértek a legtöbb szolgáltatáshoz: SMS és MMS küldés, Bluetooth, NFC, telefonkönyv stb. Az alkalmazás saját magát telepítette fel és akár a netbank applikációkban tárolt adatokhoz is hozzáférhetett.*

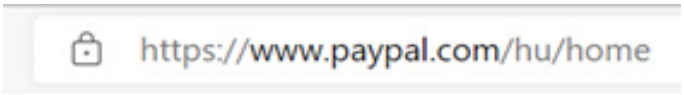


- Egy másik módszer a **lándzsás adathalászat** (ún. „spearphishing”), amikor egy **konkrét személyt vagy céget céloznak** meg a csalók. Előzetes információgyűjtés történhet az áldozatról a támadás hatékonyságának növelése érdekében. Legtöbbször az említett csatornákon történik egy megkeresés amikor valamilyen problémára hivatkozva próbálnak kikényszeríteni egy interakciót a felhasználóból. Ilyen lehet egy olyan tartalmú e-mail, amiben a banki adataink megadására vagy megváltoztatására buzdítanak például egy lejáró jelszó kapcsán. Ezt direkt módon is megtehetik a kiberbűnözők, amikor a részünkre küldött emailben feltett kérdésekre válaszként várják a számlaszámot, azonosítót és jelszót, de a legelterjedtebb módszer amikor egy hivatkozást kapunk SMS-ben vagy e-mailen, ami egy weboldalra mutat. Rendszerint megszólalásig lemásolják a bank eredeti oldalát, így ha a figyelmünk egy kicsit is lankad, belefuthatunk a csapdájukba.

Egy hamis, Paypalhoz hasonló adathalász oldal

Egy laikus felhasználó számára semmilyen különleges dolog nem lelhető fel az oldalon, de érdemes egy pillantást vetni a címsorra:

Ezzel szemben a hivatalos PayPal oldalának címsora:



Látható a különbség, a kicsit rutinosabbak azonnal észrevehetik, hogy valószínűleg egy adathalász oldalon vannak. Érdemes ilyenkor azonnal elhagyni az oldalt.

A Threat Group-4127 ilyen adathalász technikát alkalmazott, hogy Hillary Clinton 2016-os amerikai elnökválasztási kampányához kapcsolódó e-mail fiókokat célozzon meg. Közel 2000 Google fiókot támadtak meg, és az accounts-google.com domainen keresztül történt meg ezen felhasználók megtévesztése.

- A harmadik módszer a bálnavadászat (ún. whaling), amikor kimondottan felsővezetőket céloznak meg. Az ő nevük és elérhetőségük viszonylag egyszerűen kideríthető, így folyamatosan ki vannak téve ennek a veszélynek. Ha őket sikeres támadás éri, komoly anyagi vagy egyéb kár érheti a vállalatot.

2020 novemberében az ausztrál Levitas Capital nevű fedezeti alap társalapítója egy hamis Zoom hivatkozást nyitott meg amellyel egy rosszindulatú programot telepítettek a céges hálózatára. A támadók 8,7 millió dollárt próbáltak ellopni, végül "mindössze" 800.000 dollárt sikerült zsákmányolniuk.A reputációs kár azonban ennél jóval nagyobb volt, mivel a Levitas elveszítette a legnagyobb ügyfelét, és rövid időn belül az alap bezárásra kényszerült.

Egy másik eset történt 2016-ban Ausztriában, amikor a FACC nevű repülőgépipari vállalattól 58 millió dollárt sikerült kicsalnia a támadóknak bálnavádaszattal. A cég felelőssé tette és menesztette az akkori vezérigazgatóját.

További információkért, olvassa el hosszabb tájékoztatónkat az NBSZ NKI oldalán az adathalászatról és hallgassa meg az erről készült podcastünket is!

Nem biztonságos, nyilvános Wi-Fi

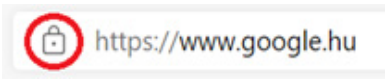
Egyre több helyen kínálnak a vendégek számára ingyenesen elérhető WiFi-t, például kávézókban, pubokban, éttermekben, hotelekben és még a tömegközlekedési eszközökön is; mert felismerték a vállalkozók és tulajdonosok, hogy az ember előszeretettel részesít előnyben egy olyan helyet egy másikkal szemben, ahol ingyenesen tud internetezni. Ezt az emberi tulajdonságot a hackerek is igyekeznek kihasználni. Viszonylag egyszerű lehallgatni a hálózati kommunikációt, így a **nyilvános WiFi hálózatok mindig kockázatot jelentenek** a felhasználó számára, ugyanis nem lehet tudni, hogy ki hozta létre, titkosítva van-e és ki figyelheti azt.

Önmagunk védelme érdekében ezért érdemes néhány szabály betartására törekedni:

- Ha nem muszáj, ne használjunk nyilvános WiFi-t, egy mobilinternet sokkal biztonságosabb választás lehet!
- Ha nem tudjuk elkerülni a publikus WiFi használatát, alkalmazzunk egy nem ingyenes VPN megoldást (Virtual Private Network)! Ez az eszköz segít titkosítani a hálózati forgalmunkat és nagy mértékben megnehezíti a hackerek számára, hogy értékes információkat nyerjenek ki a kommunikációnkból. Érdemes magánjellegű és céges elintéznivalóinkat is VPN-en keresztül lebonyolítani.

Hálózati kommunikáció VPN-en keresztül

Az olyan weboldalak, amelyek címe előtt egy lakat található, HTTPS protokollt használnak, vagyis titkosítják a kliens és a szerver közötti kommunikációt.



Bár nem biztosít teljes védelmet a kódolt kommunikáció, nagyban megnehezíti a támadók dolgát, ha csak ilyen weboldalakat látogatunk. Érdemes azonban arra figyelni, hiteles-e az adott oldal, ugyanis a csalók is létrehozhatnak ilyen weblapokat, így nem elég, ha csak arra figyelünk, hogy HTTPS protokollal legyen ellátva.

Végponttól végpontig terjedő titkosítási hiányosságok

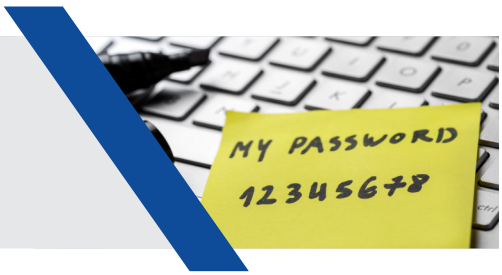
Nem csak a WiFi hálózatok, hanem a titkosítatlan alkalmazások igénybevétele is biztonsági kockázatokat rejtenek. Úgy kell tekinteni például a nem biztonságos csevegő szoftverekre, mintha úgy beszélgetne két ember (akik azt hiszik egyedül vannak), hogy a közelben valaki hallgatózik és fel tud jegyezni minden olyan információt, amely elhangzik kettőjük között. A titkosítás arra szolgál, hogyha még egy hacker le is tudja hallgatni a kommunikációt, az olyan módon legyen rejtjelezve, hogy irreálisan sok idő és erőforrás legyen szükséges annak feltöréséhez. Ilyen biztonságot nyújtó chat alkalmazások például a Telegram, Signal, Threema, Wire, Viber, WhatsApp és a Silence.

Kémprogramok (Spyware)

A kémprogramok olyan **rosszindulatú szoftverek**, amelyek a **végfelhasználó tudta nélkül** települnek egy számítástechnikai eszközre. Képes ellopni az érzékeny információkat és internethasználati adatokat, majd azokat továbbítani a támadóknak, hirdetőknek vagy adatszolgáltató cégeknek. Bármilyen szoftver besorolható kémprogramnak, ha a felhasználó engedélye nélkül települ az eszközre és **valamilyen adatot továbbít** egy másik félnek. A telepítést követően figyeli az internetes tevékenységet, nyomon követi a bejelentkezési adatokat és kémkedik az érzékeny információk után. Bár a kémprogramok elsődleges célja általában a hitelkártyaszámok, banki információk és jelszavak megszerzése, gyakran előfordul olyan eset is, hogy féltékeny házastársak vagy aggódó szülők telepítik a családtagjaik telefonjára. Ezekkel a szoftverekkel képesek az eszköz tulajdonosát fizikai helyzete alapján követni, e-mailjeit és SMS-eit elolvasni, telefonhívásait lehallgatni és rögzíteni, valamint a fájljaihoz, képeihez és videóihoz hozzáférni.

A kémprogramokat nehéz lehet felismerni, főleg a laikusok számára. Az első jel lehet a telefonokon, hogy meglehetősen megnő az adathasználat és csökken az akkumulátor élettartama. Az ún. **antispyware programokkal megelőzhető a feltelepítésük**, ha pedig már előzőleg települt, akkor ezek segítségével felfedezhetők és eltávolíthatók. Ilyen programok például a Bitdefender, McAfee, Panda, TotalAV és Norton.

Gyenge jelszavak



Az informatikai rendszerekbe (netbankok, közösségi médiás felületek, e-mail szolgáltatások, videómegosztók, alkalmazás áruházak, streaming szolgáltatók stb.) a **felhasználónevünk és jelszavunk segítségével tudunk belépni**. Amikor az adott rendszerhez hozzáférést nyerünk, a naplózó rendszer a felhasználónévhez rendelve rögzíti a tevékenységünket. Ha valaki megszerzi a felhasználónevünket és a hozzá tartozó jelszót, minden olyan adathoz hozzáférhet, amelyhez mi is, illetve használhatja ezt a hozzáférést ugródeszkaként más rendszerek eléréséhez. A rendszer szemszögéből ez olyan, mintha mi hajtanánk végre az adott műveleteket, így amit a támadó tesz, a mi nevünkben kerül rögzítésre a rendszer naplóállományaiban.

A **jelszavainkat gondosan kell megválasztanunk** és körültekintően kell kezelnünk, ugyanis a támadók célja, hogy a felhasználónévvel vagy e-mail címmel együtt a jelszót megszerezve hozzáférjenek fiókjainkhoz. Kétféle módszer létezik a jelszavak feltörésére:

- **brute force** (nyers erő) támadással: a lehetséges karakterek kombinációiból próbálják a jelszót összeállítani, ez rövid, egyszerű jelszavak esetén mindig célravezető, azonban egy megfelelően hosszú, vegyes karakterekből álló karaktersorozatot lényegesen nehezebb megfejteni a módszerrel.

- „Szótár alapú" támadással: értelmes szavakat, gyakran használt jelszavakat (pl.: név + születési dátum) próbálnak ki.

> *A Google egy 2019-es tanulmánya szerint a megkérdezettek 59%-a használt nevet vagy születésnapot a jelszavában, és 24%-uk elismerte, hogy az alábbiakban felsoroltakhoz hasonló jelszót használt: 1234, 12345, 123456, 12345678, baseball, football, password, qwerty. Az ilyen típusú jelszavak választása rendkívül nagy mértékben növeli a kockázatát annak, hogy egy esetleges támadás során a hacker sikeresen kompromittálni tudja rendszereinket, fiókjainkat.*

További információkért a helyes jelszóhasználatról olvassa el a dokumentum végén szereplő javaslatainkat vagy hallgassa meg az erről készült podcast adásunkat .

Elveszett vagy ellopott eszközök

Az okostelefonok megjelenése előtt az elvesztett vagy eltulajdonított telefonok nem jelentettek hatalmas biztonsági kockázatot, főleg abban az esetben, ha feltöltőkártyás csomagja volt az illetőnek. Természetesen ebben az esetben is kikerülhettek érzékeny információk a tulajdonosról, de nem hasonlítható össze a jelenlegi helyzettel. Minél több mindenre használjuk az okostelefonunkat, annál nagyobb biztonsági kockázatot jelent, ha hozzáférést szerez egy illetéktelen személy. A mobileszközökön tárolt információk biztonságban tartásához az is szükséges, hogy az eszközt fizikai biztonságban tartsuk. Van néhány egyszerű módja annak, hogy megnehezítsük az adatok ellopását, ha azok rossz kezekbe kerülnének:

1. Soha ne hagyja felügyelet nélkül a mobilkészülékét!
2. Legyen feltűnésmentes a készülékével!
3. Matricázza fel az eszközét az elérhetőségével arra az esetre, ha a készülék elveszne!
4. Állítsa be a képernyő időkorlátját rövid időre!
5. Használjon jelszavakat a készülék vagy bármilyen fontos dokumentum feloldásához!
6. Ne használja az "automatikus kitöltés" funkciót a jelszavakhoz!
7. Töröljön minden olyan dokumentumot, amelyre már nincs szüksége!
8. Készítsen biztonsági másolatot a fontos fájlokról!
9. Fontolja meg egy nyomkövető alkalmazás telepítését!
10. Engedélyezze a távoli eszköztörlést/helyreállítást!

Elavult operációs rendszerek és alkalmazások

A **mobilbiztonság folyamatos munkát** igényel a **sebezhetőségek felkutatása** és foltozása érdekében. Az Apple és a Google sok ilyen sebezhetőséget az operációs rendszerfrissítésekkel kezel. Az Apple például 2016-ban felismerte, hogy három nulladik napi sebezhetősége van, amelyeket kihasználva a támadók kémprogramokat telepíthetnek az eszközökre. Az ilyen és hasonló esetekben a kiadott javítás csak abban az esetben érvényesül, ha a felhasználók **naprakészen tartják mobiltelefonjaikat,** és ha van elérhető frissítés, telepítik azokat. Mivel ezeket a programokat is emberek írják, mindig előfordulhat egy-egy váratlan hiba, amelyet a hackerek igyekeznek megtalálni és saját előnyükre fordítani. Az elmúlt évtizedben az Apple és a Google összesen több mint 4000 sebezhetőséget foltozott be operációs rendszereikben. Az általános vélekedés az, hogy az Android sokkal kevésbé biztonságos, de a sebezhetőségek száma mindössze 60/40 arányban oszlik meg az Android és az iOS között. Ezen sebezhetőségek egy részét csak azután javították ki, hogy a kiberbűnözők már kihasználták azokat. Nemcsak a techóriások szoftverjeiben lehetnek hibák, hanem azokban az alkalmazások százaiban is, amelyet a hétköznapok során az emberek használnak, így ezeknek a naprakészen tartása is éppoly fontos, mint az Android vagy iOS rendszereké.

Android hibák

Strandhogg (2019)

A legújabb jelentős Android hiba 2019 novemberében hackerek ezt a sebezhetőséget arra használták, hogy banki alkalmazásokat kompromittáljanak azáltal, hogy rosszindulatú szoftvereket helyeztek el a Google Play különböző alkalmazásain. A sebezhetőséget azután fedezték fel, hogy a kiberbűnözők több cseh ügyfél bankszámláját lecsapolták. A kutatók megerősítették, hogy az Android minden verziója veszélyben volt.

StageFright (2015)

A StageFright, bár nem exploit, mégis katasztrofális Android sebezhetőség volt. A javítás kiadása előtt a jelentések szerint az androidos készülékek öt teljes éven át támadhatók voltak. A kutatók az androidos médiatárban találták meg a hibát.

iOS hibák

Trident (2016)

A Trident néven közösen ismert három iOS sebezhetőséget egy olyan hackerakcióban használták ki, amelynek célpontjai polgárjogi aktivisták voltak számos régióban. A sebezhetőség lehetővé tette a hackerek számára, hogy a hírhedt Pegasus kémprogramot (amelyet az NSO izraeli kiberkémkedési vállalat fejlesztett ki) a felhasználók tudta nélkül telepítsék a mobileszközökre. A hackerek egy ártalmatlannak tűnő linket tartalmazó SMS-t küldtek, amelyre kattintva a telefon újraindult, és a végfelhasználó minden látható figyelmeztetés nélkül telepítette a kémprogramot. A kémprogram ezután hozzáférhetett a telefon minden eleméhez, beleértve az e-maileket, jelszavakat és olyan alkalmazásokat, mint a Facebook, a WhatsApp és a Viber.

Ujgurok (2019)

Az év elején a Google biztonsági kutatói nyilvánosságra hozták, hogy azonosítottak egy régóta tartó hackerakciót, amely az ujgurokat, a kínai Hszincsiang tartományban élő muszlim kisebbségi közösséget célozta meg. A támadás az iPhone biztonsági réseit használta ki, ami lehetővé tette, hogy kémszoftvereket távolról telepítsenek a felhasználók okostelefonjaira. A telepítést követően a kémprogram segítségével nyomon követhették a felhasználók tartózkodási helyét, és hozzáférhettek olyan érzékeny információkhoz, mint például a jelszavak. A felhasználókat rávették, hogy kattintsanak egy linkre egy sor rosszindulatú weboldalon, amelyek aztán kémprogramot telepítettek a telefonjukra.

Alkalmazás hibák

Pegasus/WhatsApp (2019)

A kiberbűnözők az év elején a WhatsAppot vették célba. A hackereknek sikerült kihasználniuk az üzenetküldő szolgáltatás hanghívás funkciójának sebezhetőségét. A felhasználóknak még csak válaszolniuk sem kellett a hívásra ahhoz, hogy a kémprogram megfertőzze a mobilkészüléket. A WhatsApp gyorsan reagált, és kiadott egy frissítést, amely letiltotta a kémprogramot. A Facebook jelenleg perli az NSO izraeli kiberkémkedéssel foglalkozó céget, amely szerintük felelős a támadásért.

XcodeGhost (2015)

Az XcodeGhost 2015-ben került az Apple címlapjára, amikor az App Store-ban számos alkalmazásról kiderült, hogy rosszindulatú szoftvereket tartalmaz. Az Xcode az a programozási keretrendszer, amelyet az Apple az iOS-alkalmazások, a MacOS és a Safari-bővítmények létrehozásához használ. Kínában egy nem biztonságos verziót terjesztettek, amely körülbelül 3000-4000 eszközt érintett. Az alkalmazásfejlesztők által bevételszerzésre és analitikára használt harmadik féltől származó könyvtárakat a bűnözők többször használták arra, hogy különféle alkalmazásokat rosszindulatú szoftverekkel fertőzzék meg.

Hardveres hibák

BlueBorne (2017)

Ez a Bluetooth sebezhetőség lehetővé tette a hackerek számára, hogy a rosszindulatú szoftvereket csatlakoztatható Bluetooth eszközöknek álcázzák. Miután ezek a kódok rákerültek az okoseszközökre, a hívásokat lehallgathatták, az üzeneteket elolvashatták, zsarolóprogramokat helyezhettek el az eszközökön vagy további rosszindulatú szoftvereket terjesztésére használhatták fel. Az áldozatoknak még csatlakozniuk sem kellett az ismeretlen eszközhöz, hogy a hackerek hozzáférjenek a személyes adataikhoz. A jelentések szerint az egész támadás mindössze tíz másodpercet vett igénybe a telefonba való behatoláshoz.

Krack (2017)

A Krack egy rendkívül komoly Wi-Fi sebezhetőség volt. A hackerek bármilyen, a Wi-Fi hálózaton átmenő információt ellophattak, például jelszavakat vagy hitelkártyaadatokat. A szakértők azt tanácsolták a felhasználóknak, hogy óvakodjanak a nyilvános Wi-Fi hotspotokhoz való csatlakozástól, és csak HTTPS titkosítással rendelkező weboldalakat böngésszenek.

Spectre és Meltdown (2018)

A Spectre és a Meltdown chipszintű sebezhetőségek voltak, amelyek lehetővé tették a kiberbűnözők számára, hogy feltörjék az eszköz hardverét. Hozzáférhettek a telefon memóriájához, amely érzékeny információkat, például jelszavakat tartalmazott. A bűnözők rosszindulatú alkalmazásokon vagy internetes böngészőn keresztül tudtak behatolni a készülékekbe.

Összefoglalás

A fentebb felvázolt sérülékenységek és technikák azt a képet festhetik le számunkra, hogy bármelyik pillanatban érthet bennünket egy olyan támadás, amellyel a kiberbűnözők személyes adatokat és érzékeny információkat, akár pénzt is lophatnak tőlünk. Ez a valóságban sajnos így van, azonban megfelelő körültekintéssel, tudatos eszközhasználattal és felelősségteljes gondolkozással közel nullára csökkenthető annak az esélye, hogy valaha is áldozatai legyünk egy ilyen támadásnak. Természetesen vannak rajtunk kívül álló tényezők, amelyekre nincs ráhatásunk, de ha elvégezzük azokat a folyamatokat, amelyeket megtehetünk, több mint valószínű, hogy nem fogunk belefutni ilyen esetekbe.

Érdemes a tudásunkat naprakészen tartani és mindig informálódni az aktuális fenyegetettségekről, hogy a lehető leggyorsabban tudjunk reagálni az ilyen eshetőségekre.

Rengeteg IT biztonsághoz kötődő információt olvashat a honlapunkon , illetve további érdekességekkel jelentkezünk Kibertámadás című podcast műsorunkban is.

Az NBSZ-NKI javaslatai a felhasználók számára

- Az alkalmazásokat mindig csak elismert, hivatalos áruházból érdemes beszerezni (Google Play, App Store, Amazon). Ez nagyban csökkenti a fertőzött fájlok letöltésének kockázatát.

- Ha ezektől eltérő oldalról szerzi be alkalmazását, győződjön meg arról, hogy az adott weboldal biztonságos és naprakész!

- Érdemes egy biztonsági alkalmazás telepítését megfontolni. Ilyen például a Norton Mobile Security, az Avast! Mobile Security, az AVG AntiVirus, Panda vagy a Bitdefender.

- Kerülje a nyilvános WiFi hálózatok használatát!

- Ellenőrizze az alkalmazások által kért hozzáférési engedélyeket és gondolja át, hogy valóban szükség lehet-e az adott jogosultság megadására az alkalmazás számára!

- Mindig használjon jelszavas védelmet az eszközök zárolásához! A jelszavak legyenek minél hosszabbak és alfanumerikusak, vagyis tartalmazzanak kis- és nagybetűket, számokat és írásjeleket! Ezeknek a kombinációja, esetleg mondatként vagy kifejezésként való használata már megfelelő védelmet nyújthat a felhasználónak.

- Vannak olyan hitelkártya-társaságok, amelyek lehetővé teszik a kártyabirtokosok számára egy olyan alkalmazás használatát, amely egy ideiglenes, egyszeri hitelkártyaszámot generál.

- **Fogadjon kétséggel minden ismeretlentől származó megkeresést!** Csak azután forduljon felé bizalommal, ha meggyőződött az illető hitelességéről és szándékairól!

A jelszavak választásánál érdemes az alábbi szempontokat figyelembe venni:

- *Ne legyen ránk jellemző, mert kevés információ birtokában is könnyen kitalálható (pl.: családtag neve + születési dátum egy rövid kereséssel a közösségi oldalakon kideríthető).*
- *Nem szerencsés, ha a jelszó csak egy szóból áll (például az „almafa" szó biztosan szerepel egy támadó által kipróbálandó jelszavak listájában).*
- *Jó, ha a jelszó hosszú és többféle karaktert (kisbetű, nagybetű, szám, írásjel) tartalmaz, mert ezzel megnehezíti a brute force technikával való feltörést.*
- *A legjobb, ha néhány szóból álló jelmondatot választunk, amelyben van kisbetű, nagybetű, szám és írásjel is. Ezt könnyű megjegyezni, azonban nehéz kitalálni, brute force technikával feltörni pedig szinte lehetetlen.*

A jelszavak kezelése történjen az alábbiak szerint:

- *Fontos, hogy soha senkinek ne adjuk „kölcsön" a jelszavunkat, hiszen nem tudhatjuk, hogy az adott személy körültekintően fogja-e kezelni!*
- *Ne írjuk fel a jelszavunkat, mert ez könnyen illetéktelen kezekbe kerülhet!*
- *Ne használjuk mindenhol ugyanazt a jelszót, mert ha a támadók egyet feltörnek, minden más rendszerünkhöz hozzáférhetnek!*
- *Rendszeresen változtassuk meg a jelszavainkat, a támadónak minél több ideje van próbálkozni, annál nagyobb valószínűséggel tudja megszerezni a hozzáférésünket!*
- *Használjunk valamilyen jelszókezelő rendszert! Ezek olyan szoftverek, amelyek titkosított formában tárolják jelszavainkat. A megoldás előnye, hogy ehhez csupán egyetlen, ún. mesterjelszót kell fejben tartanunk, azt, amellyel hozzáférhetünk magához a jelszószéfhez. A mesterjelszóból kerül leképezésre az a titkosító kulcs, amivel a hitelesítő adatokat (felhasználónév, jelszó) tároló adatbázis – esetlegesen további kriptográfiai komponensek bevonásával – titkosításra kerül. Ilyen például a 1Password, KeePass, Dashlane, RoboForm, LastPass, Password Safe, Bitwarden, Keeper, Kaspersky Password Manager, LogMeOnce stb.*

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022