ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

NEUMANN JÁNOS
INFORMATIKAI KAR

SZAKDOLGOZAT

OE-NIK	Hallgató neve:	**Kerese Laura**
2021	Hallgató törzskönyvi száma:	**T/004093/FI12904/N**

Óbudai Egyetem
Neumann János Informatikai Kar
Kiberfizikai Rendszerek Intézet

SZAKDOLGOZAT FELADATLAP

Hallgató neve: **Kerese Laura**
Törzskönyvi száma: T/004093/FI12904/N
Neptun kódja: [redacted]

A dolgozat címe:

Adathalász technikák bemutatása saját esettanulmányon keresztül
Phishing techniques presented in an own case-study

Intézményi konzulens: Sziklai Zsolt
Külső konzulens: Peltz Gergő Bendegúz

Beadási határidő: 2021. december 15.

A záróvizsga tárgyai: Számítógép architektúrák
IoT, beágyazott rendszerek és robotika specializáció

A feladat

Manapság az adathalász e-mailek küldése egy elterjedt módja különböző személyes adatok eltulajdonításának. Az áldozat megtévesztésével kicsalt nevek, kódok, jelszavak illetéktelen kezekbe kerülve kárt okozhatnak a magánszemélynek vagy egy munkahely esetén a vállalatnak is.

A dolgozat mutassa be az adathalász támadások célját, menetét, térjen ki a történelmi vonatkozásokra, és példák bemutatásával tekintse át, hogy milyen technikák alkalmazhatóak az ilyen támadásoknál. Részletezze, hogy milyen szokásokkal kerülhetjük el az ehhez hasonló incidenseket, illetve vállalati környezetben milyen elhárító intézkedések hozhatók az alkalmazottak irányában.

A hallgató tervezzen és valósítson meg egy adathalász támadást multinacionális környezetben és elemezze ki a célszemélyek reakcióját. Az eredmények alapján tegyen javaslatot a védelmi szabályozás átdolgozására, hogy azok betartása nagyobb védelmet nyújthasson.

A dolgozatnak tartalmaznia kell:

- a feladat leírását,
- az adathalász technikák bemutatását,
- védelmi intézkedéseket,
- a támadás megtervezését,
- a támadás megvalósítását nagyvállalati környezetben,
- az eredmények kiértékelését,
- javaslat védelmi szabályozás esetleges módosítására.

ÓBUDAI EGYETEM Neumann János Informatikai Kar 1. Budapest

.....
Dr. Fleiner Rita
intézetigazgató

A szakdolgozat elévülésének határideje: **2023. december 15.**
(OE TVSz 55.§ szerint)

A dolgozatot beadásra alkalmasnak tartom:

.....
külső konzulens

.....
intézményi konzulens

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

HALLGATÓI NYILATKOZAT

Alulírott hallgató kijelentem, hogy a szakdolgozat / diplomamunka saját munkám eredménye, a felhasznált szakirodalmat és eszközöket azonosíthatóan közöltem. Az elkészült szakdolgozatomban / diplomamunkámban található eredményeket az egyetem és a feladatot kiíró intézmény saját céljára térítés nélkül felhasználhatja.

Budapest, 2021.12.06.

.....
hallgató aláírása

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: Neptun kód: Tagozat:

Kerese Laura [redacted] Nappali

Telefon: Levelezési cím (pl: lakcím):

[redacted] [redacted]

Szakdolgozat / Diplomamunka[1] címe magyarul:

Adathalász technikák bemutatása saját esettanulmányon keresztül .....

Szakdolgozat / Diplomamunka[2] címe angolul:

Phishing techniques presented in an own case-study.....

Intézményi konzulens: Külső konzulens:

Sziklai Zsolt..... Peltz Gergő Bendegúz.....

Kérjük, hogy az adatokat nyomtatott nagybetűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2021.02.24.	Téma átbeszélése	
2.	2021.03.04.	Feladat lap átbeszélése	
3.	2021.03.31.	Irodalomkutatás átbeszélése	
4.	2021.05.14.	Formai követelmények átnézése	

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Szakdolgozat I. / Szakdolgozat II. (BSc) vagy Diplomamunka 1 / Diplo-mamunka 2 / Diplomamunka 3 / Diplomamunka 4[3] tantárgy követelményét teljesítette, beszámolóra / védésre[4] bocsátható.

Budapest, 2021.05.15.....

.....
intézményi konzulens

[1] Megfelelő aláhúzandó!
[2] Megfelelő aláhúzandó!
[3] Megfelelő aláhúzandó!
[4] Megfelelő aláhúzandó!

ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

Neumann János Informatikai Kar

KONZULTÁCIÓS NAPLÓ

Hallgató neve: **Kerese Laura** Neptun kód: [redacted] Tagozat: Nappali

Telefon: [redacted] Levelezési cím (pl: lakcím): [redacted]

Szakdolgozat / Diplomamunka[1] címe magyarul:

Adathalász technikák bemutatása saját esettanulmányon keresztül

Szakdolgozat / Diplomamunka[2] címe angolul:

Phishing techniques presented in an own case-study

Intézményi konzulens: Sziklai Zsolt

Külső konzulens: Peltz Gergő Bendegúz

Kérjük, hogy az adatokat nyomtatott nagybetűkkel írja!

Alk.	Dátum	Tartalom	Aláírás
1.	2021.09.04.	Feladat átbeszélése	
2.	2021.10.01.	Engedélykérés a projekt megvalósításához	
3.	2021.12.04	Rendszerterv átbeszélése	
4.	2021.12.08.	Formai követelmények átnézése	

A Konzultációs naplót összesen 4 alkalommal, az egyes konzultációk alkalmával kell láttamoztatni bármelyik konzulenssel.

A hallgató a Szakdolgozat I. / Szakdolgozat II. (BSc) vagy Diplomamunka 1 / Diplo-mamunka 2 / Diplomamunka 3 / Diplomamunka 4[3] tantárgy követelményét teljesítette, beszámolóra / védésre[4] bocsátható.

Budapest, 2021.12.13. .....

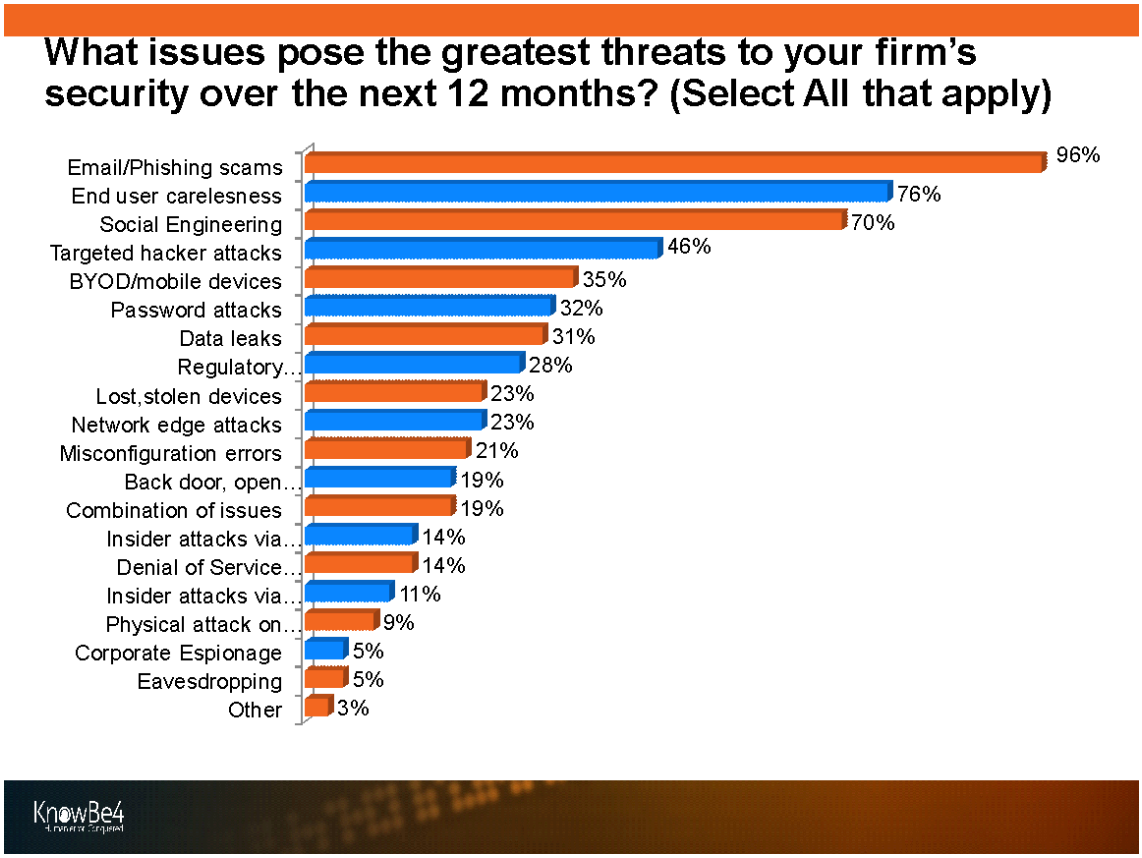
intézményi konzulens

[1] Megfelelő aláhúzandó!
[2] Megfelelő aláhúzandó!
[3] Megfelelő aláhúzandó!
[4] Megfelelő aláhúzandó!

Tartalomjegyzék

1. Bevezetés

Az adathalászat manapság egy aktuális veszélyforrás az interneten, mely kis- és nagyvállalatokat, de akár átlag felhasználókat is érinthet. A dolgozatban ezen technikák és az ellenük való védekezési módok bemutatására kerül sor. Ez egy globális probléma, melyben a csalók sokféle technikát alkalmazva érik el a személyes adatok megszerzését, mely nagy pénzösszegekhez juttathatja őket. Ezt láthatjuk az 1.1. ábrán, mely egy 2019-es felmérés eredménye, amelyben 600 nemzetközi céget kérdeztek meg arról, hogy milyen támadásra számítanak az elkövetkezendő tizenkét hónapban.



1.1. ábra - A cégek milyen támadásokra számítanak [32]

1.1 Mi az adathalászat?

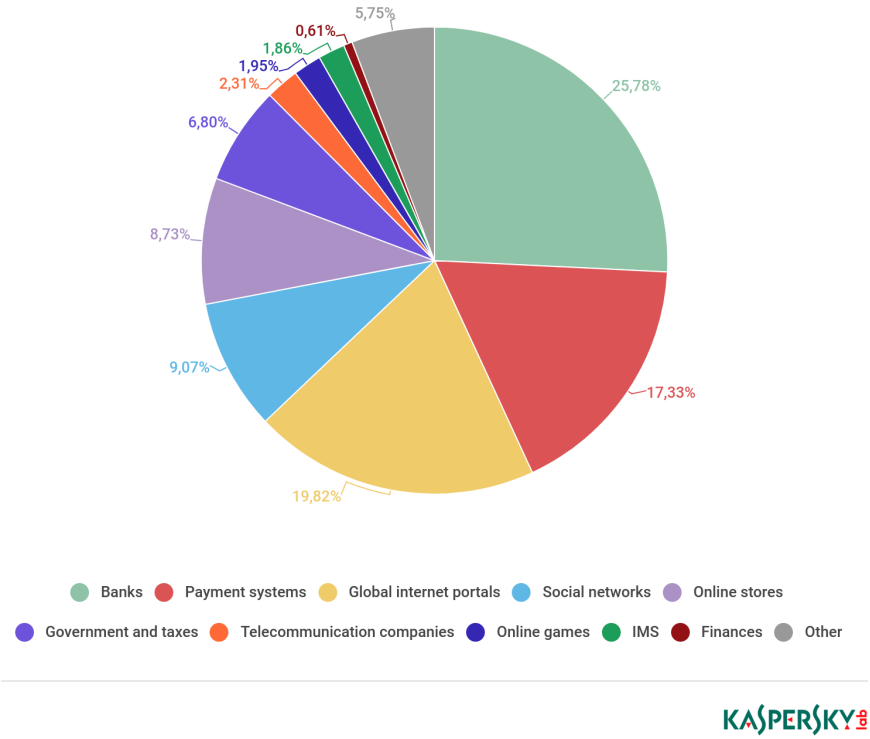
Az adathalászat egy olyan pszichológiai befolyásolási („social engineering”) technika, mely különféle módszerek segítségével a támadás célpontját próbálja befolyásolni személyes adatok, például e-mailcím, felhasználónév, jelszó vagy pénzügyi információk feltárására. Ezeket az információkat a támadó az áldozat kárára fordíthatja. Az adathalász („phishing”) kifejezés a horgászat szó angol megfelelőjéből („fishing”) származik. Az analógia azért is helytálló, hiszen a támadó „csalival” becserkészi az áldozatot, majd „elhalássza” a megszerezni kívánt személyes adatokat vagy értékes információt. A támadó fő célja a személyes adatok eltulajdonítása például egy csaló weboldal

használatával, mely általában szinte teljesen megegyezik egy ismert cég hivatalos oldalával. A támadó a dolgozat későbbi részében ismertetett különböző módszerekkel eljuttatott üzenetet küld az áldozatnak, melynek szövegében biztatja egy link megnyitására, mely egy belépési felületre vezet. Az áldozat megpróbál bejelentkezni az oldalra. Ez természetesen nem fog működni, viszont a belépés gomb megnyomásával az adatok a támadóhoz jutnak. Ezáltal ő fel tudja használni ezeket az eredeti oldalra való belépéshez.

A leendő áldozatnak eljuttatott link vezethet olyan oldalra is, ahonnan kártékony szoftver letöltése történik. Ennek során a felhasználó az adatait is elvesztheti. Sokszor a csaló nagy összegek befizetésére biztatja az áldozatot, így a becsapott visszakaphatja az elvesztett fájlokat. Ez persze nem garantált.

1.2 Támadás célja

A támadás fő célja a pénzszerzés a megszerzett információk kereskedésével, felhasználásával. Ezt az is bizonyítja, hogy az adathalász támadások nagy része elsősorban bankok és fizetési rendszerek ellen irányul. A képen a Kaspersky Lab 2019 első negyedévre vonatkozó statisztikája megerősíti ezt. [1.2.ábra] Az ellopott bejelentkezési adatokkal az adathalász megszemélyesítheti a célpontot, beléphet a megszerzett e-mail, banki fiók, vagy egyéb platformra is, ezzel nagy károkat okozva a felhasználónak.



1.2. ábra - A leginkább támadott szektorok [33]

1.3 Miért működik ez a módszer?

A módszer alapja általában a pszichológia ráhatás. A küldött üzenetben a támadó meggyőzi az egyént a kártékony lépés elvégzésének fontosságáról/sürgősségéről. Ehhez különböző, pszichológiából többé vagy kevésbé ismert befolyásolási technikákat alkalmaz. A figyelemfelkeltő üzenet gyors cselekvésre készteti a felhasználót, sietteti a levélben levő hivatkozás megnyitására, bejelentkezésre. Példaként egy vállalatnál a felső vezetéstől érkezettnek tűnő levél esetén a dolgozó jellemzően eleget tesz a kéréseknek, mivel nem akar konfliktusba kerülni a főnökeivel. A másik hatásos módszer, melynél a felhasználót valamilyen nagy nyereménnyel kecsegtetik. A sürgető levélben szerepelhet, hogy például csak az első 100 ember nyerhet, valamint rövid időkorlátot adnak a válaszra. Ezzel gyakran elérik, hogy a célszemély meggondolatlanul megnyitja a kapott honlapot, megadja adatait.

2. Történelem

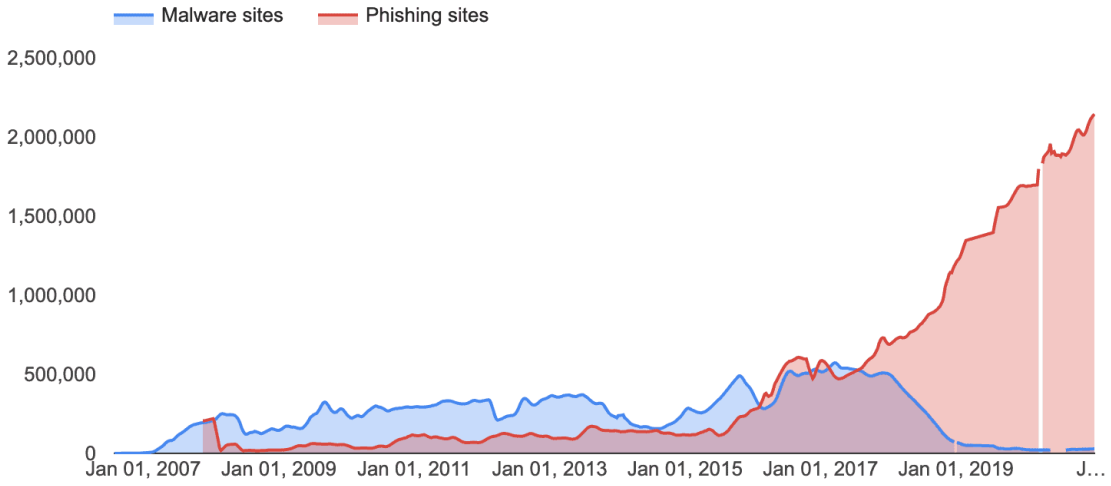
Az 1990-es évek elején az egyetlen lehetőség az otthoni internetezésre a telefonos hozzáférés volt. Ez sokak számára megfizethetetlen költséget jelentett, így alternatív megoldást használtak. Az AOL egy harminc napos díjtalan próbaverziót kínált, amelynél azonban néhányan megtalálták a módját, hogy a próbaidő lejárta után is legyen ingyenes internet hozzáférésük. Megváltoztatva a képernyőnevüket úgy tűnt, mintha AOL rendszergazdák lennének, így korlátlan hozzáférést kaptak az internethez. Az internethasználat szélesebb elterjedésével a csalók ezt a taktikát arra használták, hogy internetszolgáltató rendszergazdának álcázták magukat, és az ő nevükben küldtek e-maileket a felhasználóknak, hogy megszerezzék a bejelentkezési adataikat. Ezután a csaló hozzáférhetett az adott felhasználó fiókjához, és innen küldhetett további e-maileket, spameket.

Az első adathalász e-mail 1995 körül keletkezett. A fogalom a köztudatba csak pár évvel később került be a „Love Bug" nevezetű támadáskor.

Az egyik nagy mérföldkő az adathalászat történetében a „Love Bug" támadás volt 2000. május 4-én. A támadó világszerte küldött ki e-maileket „ILOVEYOU" vagyis „szeretlek" címmel, egy levélhez csatolt rosszindulatú szövegfájlal. Akik megnyitották az ártalmatlannak tűnő csatolmányt, megfertőzték a számítógépüket. A kiszabaduló féreg felülírta a gépen lévő képfájlokat, és ha az adatvesztés nem lenne elég, a képek egy példányát elküldte a felhasználó összes Outlook-ban található címzettjének. Ez a támadás megmutatta, hogy lehetőség van arra, hogy egy e-mail felhasználói interakcióval továbbküldjön adatokat más címzetteknek az emberi pszichológia és a technikai hibák kihasználásával. 45 millió számítógép esett áldozatul ennek a támadásnak. Akkoriban ez az összes internethozzáféréssel rendelkezők 12,5 %-a volt. [1]

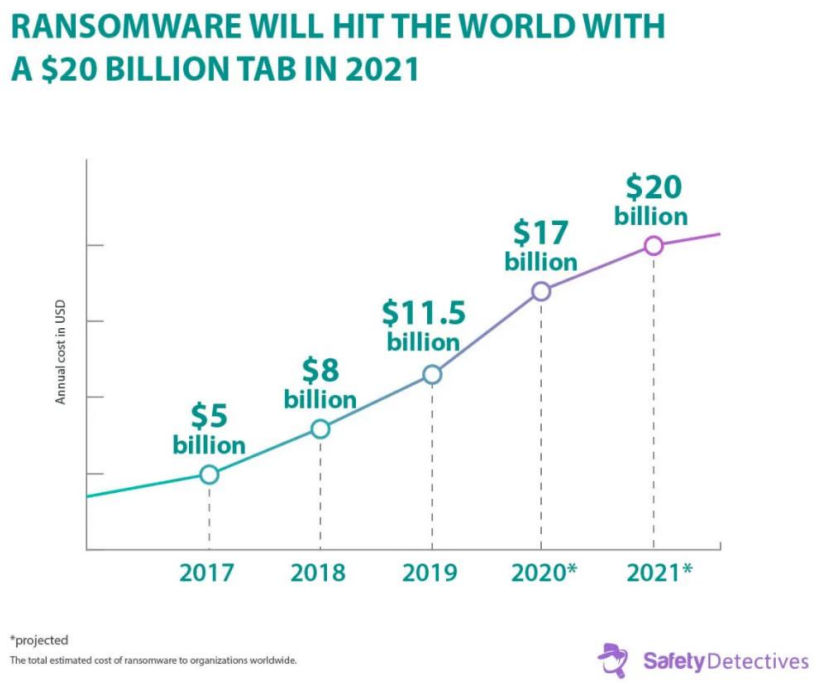
2.1. ábra - Internethozzáféréssel rendelkezők száma 2000-ben [34]

A technika fejlődésével a spamszűrőknek köszönhetően kevesebb kéretlen levelet kapunk, viszont az emberek két évtized után se tanulták meg, hogy nem adhatnak meg bárhova bejelentkezési adatokat és nem nyithatnak meg gyanúsnak tűnő linkeket. A mai napig rengeteg adathalász támadás történik a világban, amelyek a világgazdaságnak is nagy károkat okoznak. Az FBI adatai szerint 2020-ban csak az USA-ban 2,9 milliárd USD veszteség érte a gazdaságot. [6]



2.2. ábra - Az adathalász oldalak növekedése [35]

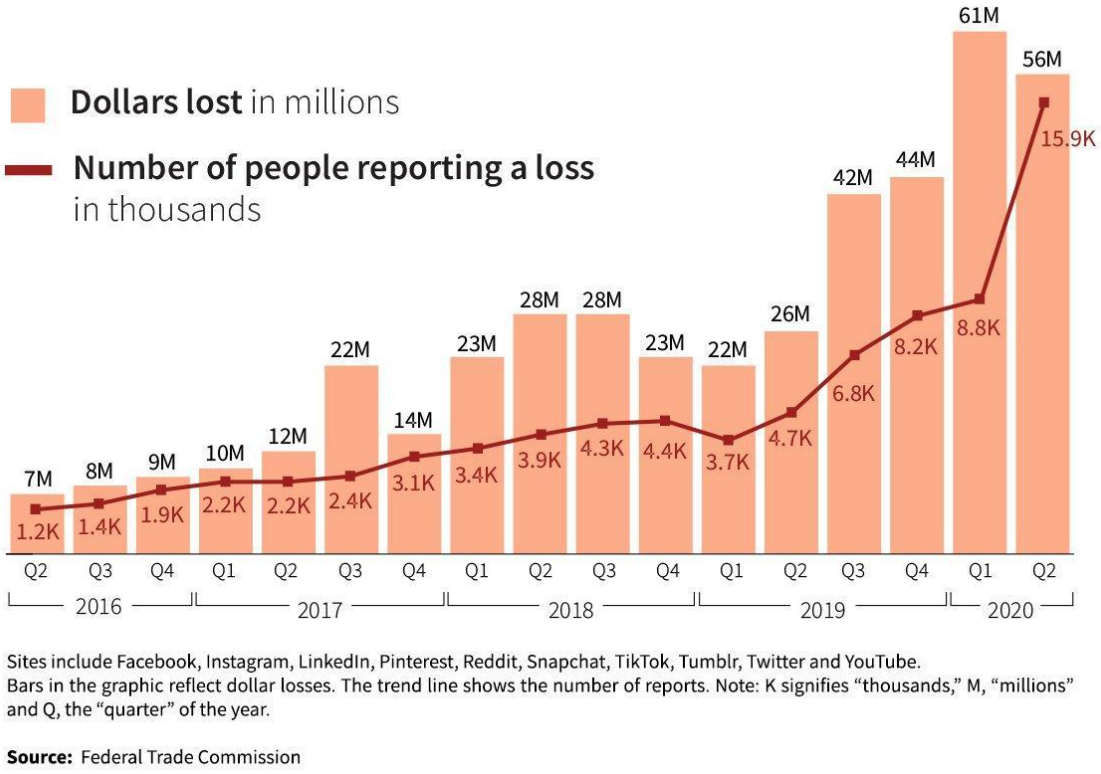
A sikeres adathalász e-mailek segítségével telepített kártékony programok telepítése további lehetőségeket nyújt az információlopáshoz. Manapság az egyik legelterjedtebb támadás a „ransomware" vagyis a zsarolóvírusok terjesztése, melyek az áldozat adatait titkosítva követelnek nagy összegek befizetését. 2013-ban történt az első nagy zsarolóvírus támadás, a „Cryptolocker", majd 2017-ben a „WannaCry" rengeteg gépet fertőzött meg világszerte, és hatalmas károkat okozott sok vállalatnak. A „MIT" szerint a zsarolóvírusok okozta kár csak az USA-ban 7,5 milliárd dollár volt 2019-ben. Ebben az évben az egész világon ez az összeg körülbelül 11.5 milliárd dollár volt. [2] [4] [5]



2.3. ábra - Zsarolóvírusok által okozott károk [7]

Az adathalász támadások főleg e-mail és rosszindulatú linkek formájában terjedtek el. A spam szűrők egyre kifinomultabbak lettek. A Microsoft közleménye szerint 2019-ben több mint 13 milliárd gyanús e-mailt blokkolt, melyből 1 milliárd adathalász támadást tartalmazott. Egy 2020-as jelentés szerint a káros linkekre való kattintási arány már sokkal alacsonyabb volt, 2019-hez képest 6,6%-kal csökkent. Viszont a felhasználói tudatlanság és az egyre kifinomultabb és egyre nehezebben felismerhető támadási technikák miatt a mai napig rengetegen esnek áldozatul az adathalász támadásoknak. [3] [7]

Jelenleg a közösségi hálózatok mindennapjainkban betöltött növekedő szerepe miatt a támadók is inkább ezen platformok felé mozdulnak, ahogy ezt a lenti ábrából is kiolvashatjuk. 2020 második negyedévére az előző év azonos időszakához képest megháromszorozódtak a felhasználói bejelentések. [8]



Sites include Facebook, Instagram, LinkedIn, Pinterest, Reddit, Snapchat, TikTok, Tumblr, Twitter and YouTube.
Bars in the graphic reflect dollar losses. The trend line shows the number of reports. Note: K signifies "thousands," M, "millions" and Q, the "quarter" of the year.

Source: Federal Trade Commission

2.4. ábra - Közösségi oldalakon jelentett adathalász veszteségek [8]

3. Az adathalász támadás szakaszai

1. Tervezés
   A támadás a tervezéssel kezdődik. Először a támadó azonosítja a célpontokat, információt gyűjt róluk, valamint a támadásban alkalmazott eszközök és technikák használatát dönti el.
   Meghatározza a törvényes webhelyet, létrehozza az eredetihez nagyon hasonló hamis weboldalt, megfogalmazza a hozzá tartozó szöveges üzenetet.
2. Adathalász üzenet
   Ebben a szakaszban megkezdődik a tényleges adathalászat, a tervezésnél eldöntött módszerek alkalmazása (például e-mail vagy SMS kiküldése).
3. Támadás
   Az áldozat nem képes megkülönböztetni az eredeti és az adathalász e-mailek közötti különbséget, így megnyitja a csatolmányt. Ezután a hivatkozás a hamis webhelyre irányítja őket. Az áldozat beírja bejelentkezési adatait, nem tudván arról, hogy rosszindulatú weboldalról van szó.
4. Adatgyűjtés és hasznosítás
   Az adathalász kivonja a begyűjtött információt és felhasználja céljai eléréséhez. A támadó az áldozatot megszemélyesítve megpróbál hozzájutni pénzügyi fiókjaihoz vagy a megszerzett adatokkal kereskedhet az online feketepiacon is.
5. Nyomok eltüntetése
   A támadó megpróbálja eltüntetni nyomait, törli a hamis weboldalt. [9]

4. Támadási technikák fajtái

Az adathalászatot az alkalmazott módszertől és a végcéljától függően különféle módon csoportosíthatjuk. Példának említeném a Hausken által javasolt modellt, mely jól szemlélteti a támadási fajták eltérő céljait. Hausken öt kategóriába osztotta az adathalász típusokat [11]:

- Egyéni célpont elleni támadás
- Több célpont elleni támadás
- Egymást követő támadások
- Véletlenszerű támadás
- Szándékos és nem szándékos hatások kombinációja

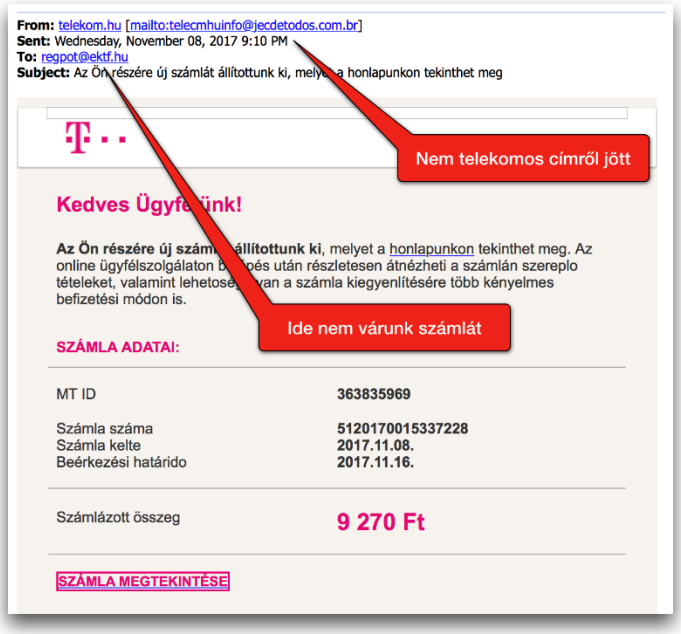
5. Az adathalászat támadási felületek

Az adathalász támadásokat az alkalmazott média felület szerint három fő csoportra bonthatjuk: hang, SMS, vagy interneten keresztüli. Egy tágabb csoportosításban, mely szemlélteti a támadók alkalmazkodását a technológiai változásokra az adathalászat forrásai lehetnek E-mail, telefonon keresztül, azonnali üzenetküldéssel, közösségi médiában, weboldalakon, SMS-ben, vagy Wifin keresztül. Ezek kerülnek részletezésre a továbbiakban. [10]

5.1. ábra - Adathalász támadási felületek csoportosítása – saját ábra

5.1 E-mailes átverések

Az e-mailes átverés az egyik legtöbbször használt adathalász típus. Az internet széles körű elterjedésével ez a technika könnyen alkalmazható, mivel nagyszámú címzett érhető el rajta, valamint lehetővé teszi, hogy a feladó földrajzi helye ismeretlen maradjon. A támadók speciálisan kialakított e-maileket küldenek a célpontok számára, melyben adatmegadásra, pénz befizetésére vagy egy kártékony program telepítésére biztatják őket. A lenti ábra szemlélteti, hogyan nézhet ki egy ilyen üzenet. [10]



5.2. ábra - Adathalász e-mail [36]

5.2 Telefon és VoIP

Nem minden adathalász támadás zajlik az internet felhasználásával. A hang, vagyis a beszéd az egyik legrégebbi és leghatásosabb módszer, amellyel az emberek információt közvetítenek. Az emberek bizalmasabbak egymással mikor telefonon keresztül kommunikálnak, szemben a szöveges üzenetekkel. A célpont nincs tudatában, hogy az átverő képes olyan technikákat alkalmazni, mint a hívó-azonosító hamisítása. Ez a technika a VoIP (voice over IP – IP protokollra alapuló hangátvitel) technológiával lett igazán elterjedt, melyeknél a belföldi és a nemzetközi hívások költségei is elhanyagolhatóak. A módszer a szám hamisításának a képességét használja, majd az áldozatot manipulálják, hogy személyes információkat adjon ki. A telefonos ügyintéző automatizálási módszerek használata tovább javítja a telefonos adathalász támadások esélyeit. Évekkel ezelőtt a gyerekek, mikor játékból ismeretleneket hívogattak, ha a tréfát jelentették, a hívó száma könnyen kideríthető volt. Viszont a közelmúltban lévő fejlődéseknek köszönhetően fennáll annak a lehetősége, hogy a telefonhívás indítható számítógépről a világ bármely pontjáról. [12]

A fő pontok, ami miatt ez a módszer igazán sikeres:

- Bizalom – A telefonos kommunikációnál nagyobb bizalmat szavaznak az emberek.
- Automatizálás – Az automatizált telefonrendszerek megszokása, melyek szintén alkalmazhatóak adathalászatra.
- Hívóközpontok – A telefonközpontok széles körű használatával az emberek megszokták, hogy ismeretlenektől kapnak hívásokat, akik személyes adatokat kérnek tőlük.

- Idősödő korosztály – A világszerte idősödő népesség nagy része csak telefonon keresztül érhető el, az internet sokuk számára ismeretlen. [10]

5.3 Azonnali üzenetküldés

Az azonnali, személyes üzenetküldő alkalmazásokon keresztül is lehetőség van adathalász támadásra. Régebben az MSN, ma például a Facebook Messenger, WhatsApp, Telegram, valamint az online játékokat is kihasználhatják a támadók. Ez ideális környezet az adathalászok számára, melyben a valós idejű csevegés közben bevonják az áldozatot, és arra ösztönzik őket, hogy tárják fel személyes adataikat. Az egyik népszerű módszer, mikor a támadó az üzenetben elhiteti a célponttal, hogy fiókját feltörték, és kéri, hogy adja meg az adatait bejelentkezés útján. [10]

5.4 Közösségi média

A közösségi oldalak széles körű elterjedése lehetővé teszi az emberek számára az egyszerű kapcsolatba lépést, kommunikációt. Ilyen például a Facebook, LinkedIn, Twitter, melyeken a legtöbben megadják személyes adataikat. Ez kiváló forrás az adathalászok számára, mivel a születési dátum, telefonszám és munkahely mellett a célpont érdeklődési körére is fény derül. Ha a támadó tudja, hogy a célpont milyen zenét, filmet, sportokat szeret, vagy akár mely helyeket látogatta meg az elmúlt években, ezek segítségével célzott üzenetet is küldhet neki, így könnyebben horogra akaszthatja áldozatát. Ha egy hozzánk közel álló témában kapunk üzenetet, sokkal nagyobb az esély az ehhez kapcsolódó link megnyitására. Például, ha a kedvenc hazai zenekarunktól kapunk egy üzenetet, előbb rákattintunk az abban szereplő hivatkozásokra, mint egy ismeretlen témájú levélnél. [13]

5.5 Weboldalak

Az adathalász weboldalak valamilyen oldalak másolatai, amelyek szinte teljesen megegyeznek az eredetivel, de az áldozatok személyes adatainak gyűjtésére szolgálnak, mikor ők megpróbálnak bejelentkezni. Ezek az oldalak jogszerűnek tűnnek a hasonló színek, képek, logó miatt, így jellemzően nehezen ismerhető fel a csalás. Rana Alabdan tanulmánya szerint az átlagos felhasználók hajlamosabbak azt hinni, hogy az adathalász támadások főleg e-mailek útján történnek, így sokkal inkább kiszolgáltatottak az ilyen jellegű csalásokkal szemben. [10] [14]

5.6 SMS-es kísérlet („SMSiShing”)

Sokan megadják nyilvánosan a telefonszámukat a közösségi oldalakon. Ez a rövid üzenetküldő szolgáltatás lehetővé teszi az adathalászok számára, hogy az SMS-ben például egy megbízható banknak, telefonszolgáltatónak vagy csomagküldési szolgálatnak adják ki magukat. Az okostelefonok elterjedésével lehetőségük van webes linkek küldésére és fogadására az üzenetekben. A figyelemfelkeltő vagy létfontosságúnak tűnő üzenet biztatja a célpontot a weboldal meglátogatására, mely egy bejelentkező felületen kéri a felhasználó személyes adatait. A sikeres támadás után az adathalász a saját

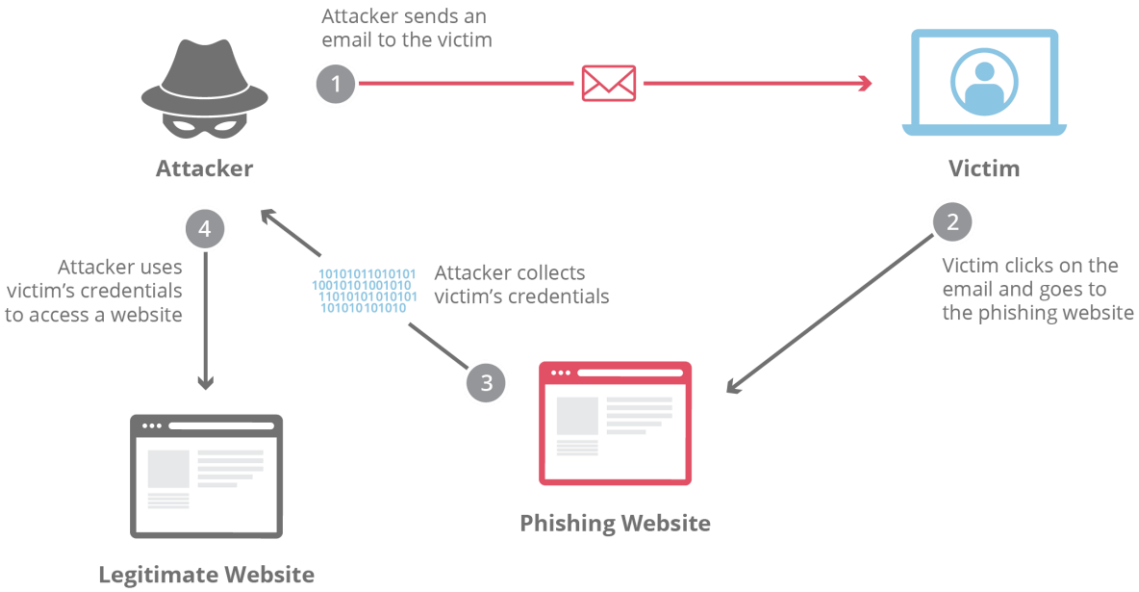
céljára felhasználhatja a megadott adatokat. Egy másik módszer, mikor az SMS link egy rosszindulatú programot tartalmazó webhelyre mutat, mely telepítése után a támadó folytathatja a támadását, az áldozat névjegyei, üzenetei ellopásával, valamint az internetes bejelentkezési adatok megszerzésével. Ezzel a módszerrel a támadó gyakorlatilag teljes hozzáférést szerezhet az eszközökhöz, melyet egyéb, már nem adathalászathoz köthető támadási formák kivitelezéséhez is felhasználhat. [10] [13]

5.7 Wifi hamisítás

Az adathalászat nem célzott formája nyilvános hotspotokon is történhet. Egy valós Wifi hálózat lemásolásával az áldozat azt hiheti, hogy a hivatalos hálózatra csatlakozott, miközben az adatai már továbbítódtak a csalónak. Saját tapasztalatom szerint manapság ez a módszer talán már nem olyan elterjedt mint 10 éve, mivel a mobilszolgáltatóknál lehetőség van saját internet előfizetésre, így nincs szükség a nyilvános hálózathoz való csatlakozáshoz. Viszont vannak helyek, ahol a saját internet nem működik (például repülőn), itt releváns lehet ez a támadási forma. [15]

6. Adathalász technikák

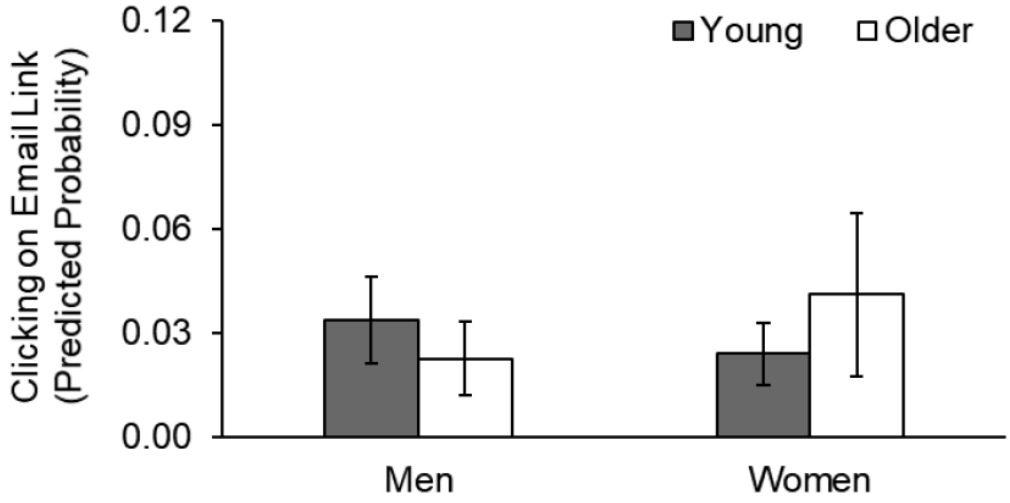
Az adathalászok különböző technikák felhasználásával tulajdoníthatják el a felhasználók adatait, és használhatják fel őket saját céljaikra. Az alábbi ábra bemutatja egy adathalász támadás jellemző lépéseit a kivitelezés során.



6.1. ábra - Adathalász támadás jellemző lépései [37]

6.1 Lándzsás adathalászat („Spear Phishing")

A konkrét egyénekre vagy cégekre irányuló adathalász támadást lándzsás halászatnak hívjuk. Ennél a technikánál a támadók speciálisan kidolgozott anyagokat használnak. Ilyen például, ha ismert emberek nevében küldenek el egy e-mailt, így a célpont még nem is gyanítja az adathalász támadást. A levél témája sokszor kapcsolódik olyan dologhoz, amit a célpont kedvel. A csaló e-mail tartalmazhat személyes információkat, vagy akár az áldozat nevét is, így még kevésbé kelt gyanút a támadás. A közösségi oldalakon, mint például a Facebookon vagy a LinkedInen megosztott publikus információk segítik az adathalászokat, mivel itt tudnak kutatást végezni, majd személyre szabottabb e-mailt küldeni a célpont szakmája, érdeklődési köre és egyéb személyes adatainak ismeretében. A támadás sikeressége az emberi pszichológia szempontjain alapszik. Egy másik példa, mikor az adathalász egy hatóság nevében követel lépéseket, amelyeknek az áldozat kérés nélkül eleget tesz. Ezek a trükkök felhasználhatóak másfajta támadásoknál is, viszont a lándzsás adathalászattal ezek a manipuláló kísérletek pontosabban alkalmazhatók. Több tanulmány kimutatta, hogy az idős nők leginkább fogékonyak az adathalász támadásokra. [10] [16] [17] [18]



6.2. ábra - E-mail hivatkozásokra való kattintás [18]

6.2 Bálnavadászat („Whaling")

A bálnavadászat hasonlóan a lándzsás adathalászathoz főleg egy embert céloz, a különbség abban nyilvánul meg, hogy itt az áldozat egy vezető vagy magas beosztású személy, akinek privilegizált hozzáférése van a vállalat egyes adataihoz. Itt, mint a többi célzott támadásnál sok időt vesz el az előkészület, a felderítési folyamat a célszemélyről, hogy az átverés a lehető legjobban hasonlítson egy hivatalos levélhez. Ez a technika általában e-mail küldésen keresztül zajlik, célja jellemzően az, hogy rosszindulatú programot telepítsen a célrendszerre, így a támadó hozzáférhet a megszerezni kívánt titkos adatokhoz, vagy akár figyelheti a billentyűk leütését a számítógépen. [9]

6.3 „Business Email Compromise (BEC)"

A „BEC" a lándzsás adathalászat egyik fajtája, ami az üzleti levelezéshez való hozzáférés a támadók számára, ezzel komoly károkat okozva a vállalatnak, mely éves szinten megközelítheti a 10 millió dollárt. Az adathalászok billentyűzet figyeléssel hitelesítő adatokat lopva hozzáférést szereznek a szervezet levelezéséhez. Egy másik esetben a pénzügyi részlegen dolgozóknak küldenek e-mailt, melyben nagyobb összeg utalására utasítják őket. Úgy tűnik, mintha a levelet egy felső vezető írta volna, így a dolgozó eleget tesz a kérésnek. Gyakran az adathalászok heteket vagy hónapokat töltenek egy vállalat hálózatán belül egy magas beosztású alkalmazott elemzésével, hogy az ő nevében küldött e-mail még hitelesebb legyen, valamint a vállalat által regisztrált domain nevek használatával tökéletesíthessék a támadást. Ezt a módszertant először 2013-ban fedezték fel. 2018-ban az FBI-nak jelentett támadásoknál az összesített veszteség körülbelül 1,2 milliárd dollár volt. Az adathalászat ezen módszerét azért nagyon nehéz felismerni, mert jellemzően üzleti kapcsolatból eredő bizalomra épít, és közelmúltbeli vagy aktuális eseményeket tematizál. [10] [19]

6.4 „Cross-Site Scripting” (XSS)

Az XSS egy weboldali sebezhetőség, melyet az adathalászok ki tudnak használni a saját céljaik elérésére. Ez a sérülékenység a HTML kimenetet célozza meg. A weboldal általában Java, PHP, vagy .NET-ben íródik. A támadó egy rosszindulatú scriptet helyez a kód forrásába, melyet a felhasználó is láthat. A link megnyitásával megnyílik az eredeti oldal, miközben a felhasználó mit sem sejt a támadásról. A kártékony kód beadható egy weboldalon belüli adatmezőbe, vagy a webhely URL-jébe. A script a weboldal megnyitásakor megpróbálja elérni a böngészőben tárolt adatokat, például a cookie-kat, majd továbbítja őket a támadónak. Így az adathalász hozzáférhet az áldozat böngészőben tárolt fiókjaihoz, és felhasználhatja őket. A módszer megkerüli az SOP („Same-origin policy”) irányelvet, ami biztosítaná, hogy az egyik tartományból betöltött scriptek ne férjenek hozzá a többi tartományhoz tartozó adatokhoz. Például egy blognál az áldozat betölti az oldalt, melyre a támadó korábban írt bejegyzést, mely egy scriptet tartalmazott. Ha az oldalt bármelyik későbbi felhasználó betölti, a script lefut, és amíg az adott személy elolvassa a megjegyzést, személyes adatait rögzítik a támadó szerverén. Ez a folyamat a script eltávolításáig tart. [10]

6.5 „Cross-Site Malicious CAPTCHA Attack”

Ez a rosszindulatú támadás lehetővé teszi, hogy becsapja a felhasználókat, akik öntudatlanul nyilvánosságra hozzák a személyes információikat. A hamis weboldal obfuszkálva jeleníti meg a felhasználó számára a privát információkat, mintha CAPTCHA kihívás lenne, melyet megold a gyanútlan felhasználó, ez után nyilvánosságra hozva az adatokat. Ez a módszer megkerüli az SOP („Same-origin policy”) irányelvet, mely lehetővé tenné, hogy ne férjenek hozzá a támadók a privát információkhoz. A legtöbb oldal megjeleníti a felhasználó számára a személyes adataikat. Ez a technika ezt használja fel, nyilvánosságra hozva az oldalon tárolt adatokat például nevet, telefonszámot, e-mail és lakcímet, keresési előzményeket, részleges hitelkártyaszámokat is. Nethanel Gelernter és Amir Herzberg tíz népszerű weboldalnál tesztelte ezt a technikát 2016-ban, melyek közül kilencnél működött ez a támadás. [29]

	Name	Additional information
Google & Youtube	√	Email address, followed users, liked items, Google+ circles
Facebook	√	Followed users, liked items
Yahoo	√	Anti-CSRF token
Baidu	√	Personal information: calendar, age, education, job, interests etc.
Wikipedia	√	
Amazon	√	Number of items in the cart, customer ID
Twitter		
Taobao	√	Physical address, phone number, birthday
QQ	√	Subject and details of recently received emails
Live & Bing & Outlook	√	Search history, Skype client ID

6.3. ábra - Weboldalak sérülékenységének tesztelése [29]

6.6 „Qrishing”

A QR-kód egy fekete-fehér pixeleket tartalmazó mátrix, mely tömörített információ tárolására alkalmas. A kétdimenziós QR-kódok gyorsan felváltották az elavult egydimenziós vonalkódokat, mivel sokkal olvashatóbbak, több információt tartalmaznak, valamint már minden okostelefon képes a beolvasásukra. A kódban tárolt információhoz való hozzáféréshez egy optikai leolvasóra van szükség, mely sok esetben a telefon kamerája. Miután a QR-kód olvasó dekódolja az információt, megnyílik a kódban tárolt weboldal. Ezek a kódok gyakran láthatóak terméken, újságokban és óriásplakátokon. A QR-kódok készítésének és terjesztésének egyszerűsége miatt ez ideális módszer egy adathalász támadáshoz. Ezt fokozza az, hogy az emberek nem képesek megérteni a kód tartalmát beolvasás előtt. Sok QR-kód olvasó megnyitja a dekódolt tartalmat anélkül, hogy a felhasználó jóváhagyását kérné. Az adathalász kódokat tehet egy olyan területre is, melyen egy törvényes termék vagy vállalat hirdetésének tetteti magát. A beolvasott QR-kód egy rosszindulatú URL-re irányítja a felhasználó készülékét, ahol egy letöltés történik, így megfertőzi az áldozat eszközét, mielőtt átirányítaná őket a törvényes webhelyre. A link egy bejelentkező felületre is mutathat, melyen a felhasználó az adatai megadását követően ezeket a csalók könnyen ellophatják. [20] [21]

6.7 Pszichológiai befolyásolás („Social Engineering”)

A „social engineering” az egyik legrégebbi technika, amit az adathalászok használnak, melyben egy személy vagy személyek manipulálása a cél, az áldozat érzelmével, hiszékenységével, bizalmával vagy jótékonyságával visszaélve. Egy korai példa a görög trójai faló mítosza. Ez a technika nem igényel specifikus közeget és nincs egyedi védekezési stratégiája. Az áldozat érzelmeit felhasználva megakadályozza a racionális cselekvést, ez által személyes adatokat ad át a támadónak. Mosin Hasan az alábbi kategóriákra osztotta a „social engineeringet”:

- **Személyzet megszemélyesítése**: például egy informatikai alkalmazottnak hiteti el magát a támadó, majd így kéri a felhasználó jelszavát.
- **Kívülről jött munkavállalónak álcázás**: például telefon- vagy internetszolgáltatótól érkező személyek, akik segítséget kérve a munkavállalóktól információkat szereznek meg.
- **Megfélemlítés**: például egy magas szintű vezetőnek tetteti magát a csaló, az áldozattal kiabál, kirúgással fenyegeti, sürgeti az információk átadására.
- **Hazugság**: a cél meggyőzni az áldozatot egy valótlan dologról, így a nem kívánt eseménytől való félelem miatt hirtelen döntésekre kényszerítve őt.
- **Zavarkeltés**: például a tűzjelző bekapcsolása a terület kiürítéséhez. Az emberek sietve, zárolatlanul hagyják számítógépüket, így a csaló a bejelentkezve maradt gépekről szerezhet információkat.
- **Szeméttároló búvárkodás („dumpster diving”)**: egy cégnél eldobott papírszemét, ha személyes adatokat tartalmaz, ezen iratok nem megfelelő megsemmisítése hiányában az adathalászok hozzá juthatnak a szeméttárolóból. Ennél a technikánál a

csalók megszerezhetik akár a vállalat szervezeti ábráját, hogy ki kinek a főnöke, így ezeket az információkat felhasználhatják megszemélyesített támadásnál.

- **Fordított social engineering**: a támadó valamilyen hatalmi vagy hatósági helyzetben van. Az áldozatok megkeresik őt, kérdéseket tehetnek fel, majd szívesen megadják adataikat. [10] [22]

6.8 Hirdetésekben tárolt rosszindulatú kód („Malvertizing")

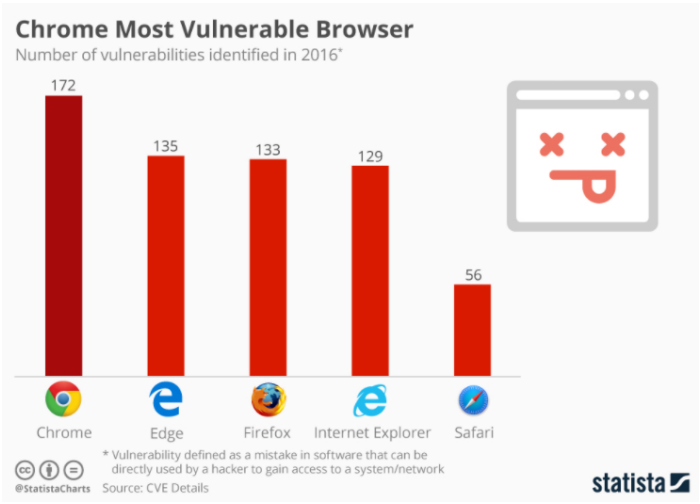
Ennél a módszernél az adathalász egy reklámszolgáltatást használ egy rosszindulatú program tárolására, mely akkor aktiválódik, mikor az áldozat rákattint az adott hirdetésre, így megfertőzve számítógépét, lehetővé téve az adatlopást az eszközről. Ezt a tevékenységet nehéz felismerni és megakadályozni, mert a programot egy törvényes webhelyen tárolják. Ezek a szolgáltatók nem követelik meg az ügyfelektől, hogy adjanak meg konkrét részleteket a hirdetésről vagy magukról. A reklámszolgáltatóknak nehéz ellenőrizni, hogy egy adott oldal rosszindulatú-e, mivel a legtöbb hirdetés tartalmaz átirányítást a promótált termékre. [10]

6.9 Gonosz-iker támadás („Wiphishing")

Ez az adathalász módszer a vezeték nélküli hálózatot használja, melynél beférkőzik az áldozat és a valódi hozzáférési pont közé úgy, hogy ugyanazt az SSID-t és frekvenciát használja, mint az eredeti hálózat. A csaló így képes figyelni a hálózati forgalmat, és hozzáfér a továbbított információkhoz. Ez a támadási technika gyakori az ingyenes Wifi hotspotokon, melyek például szállodák, kávézók vagy utazási központokon érhetők el.

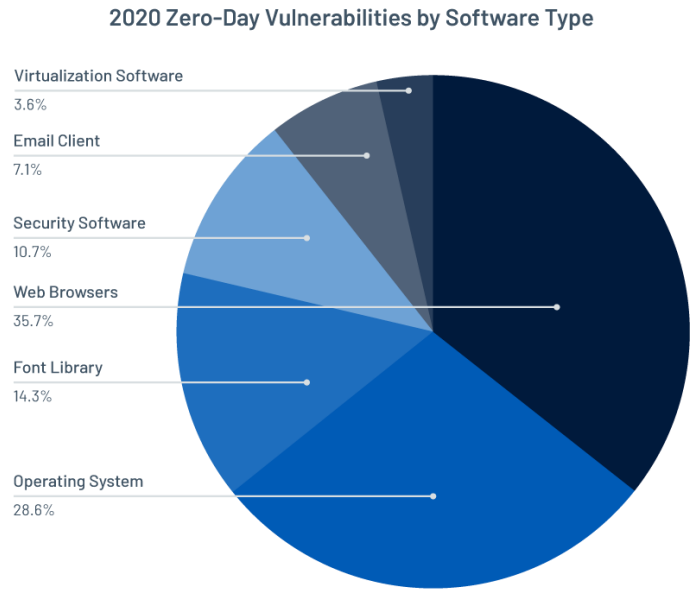
6.10 Webböngésző sérülékenység

A böngészők különböző tartalmakat szöveget, képek, videót, fájlokat tárolnak, melyeket a csalók manipulálhatnak, így adatokat szerezhetnek a felhasználóktól. Különböző böngészők különböző mértékben sebezhetők a különböző típusú támadásokkal szemben. Egyetlen böngésző sem igazán biztonságos a tervezési problémák és hibáknak köszönhetően. [10]



6.4. ábra - Böngészők sebezhetőségének aránya [38]

A „zero-day” sérülékenységek az egyik legveszélyesebbek, mivel ezek olyan sebezhetőségek, amik még nem kerültek publikálásra, nem érhető el még biztonsági frissítés rájuk. Egy 2021-es publikáció szerint a 2020-as „zero-day” sérülékenységek leginkább webböngészőknél jelentek meg.



6.5. ábra - „Zero-day” sérülékenységek aránya [39]

6.11 „Tab-Napping”

Ez a kifejezés a “tab” és a “kidnapping” vagyis a böngészőben megjelenő oldalak és az emberrablás szóból származik. A támadók kihasználják, hogy a felhasználók egyszerre több oldalt nyitnak meg a böngészőjükben, és az épp nem nézett megnyitott oldalakon

parancsfájlokat futtatnak az adatok kinyerése érdekében. Például az áldozat bejelentkezik a Facebook fiókjába, ahol lát egy érdekes linket és rákattint. Amíg a felhasználó ezt az oldalt nézi egy másik tab-ban, egy script fut le, mely átirányítja a facebook oldalt egy hamis bejelentkező felületre. Mikor az áldozat visszatér az első felületre, feltételezi, hogy kijelentkezett munkamenet időtúllépés miatt, ezért újra beírja a facebook bejelentkezési adatait. Ez után átirányítja a felhasználót az előző munkamenetre, aki nincs tudatában, hogy bejelentkezési adatait elküldte az adathalásznak. [10]

6.12 „Typo Squatting”

Ez a technika egy olyan típusú URL eltérítés, mely kihasználja, ha a felhasználó rosszul ír be egy webcímet. Például a Facebook.com helyett a Facebok.com címet használja, mely az adathalász tulajdonában van. A hamis weboldal úgy néz ki, mint az eredeti. A bejelentkezést követően a csalók megszerzik a felhasználó adatait, valamint képesek rosszindulatú szoftver telepítésére is. [10]

6.13 „Sound Squatting”

Ez a módszer a hang alapú felhasználói felületeket célozza meg. A virtuális asszisztensek a felhasználó hangjára nyitnak meg alkalmazásokat, weboldalakat. Ezt a csalók kihasználhatják egy hamis weboldal regisztrálásával, melynek a címének kiejtése hasonlít egy hiteles oldaléhoz. Így mikor a felhasználó kéri az adott webhely megnyitását, a virtuális asszisztens a hamis oldalt nyithatja meg, melynek köszönhetően a már sokszor említett módszerekkel információk lophatók el, rosszindulatú alkalmazások telepíthetődnek. [10]

6.14 „Click Jacking”

Ebben a támadási típusban a hackerek több réteget használnak egy gombra való kattintásakor. Ezek a rétegek lehetnek átlátszóak is, melyek interakció után megnyitnak egy rosszindulatú alkalmazást tartalmazó weboldalt, vagy váratlan művelet elvégzésére kényszerítik a felhasználót. [10]

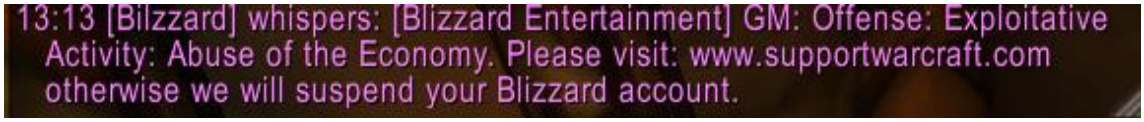
6.15 Rosszindulatú böngésző bővítmények

A böngészőbővítmények olyan szoftverek, melyek más szoftveralkalmazásokhoz hasonlóan futnak, de nem közvetlenül a számítógépre vannak telepítve, hanem a böngészőbe. A webáruházakból letölthető bővítmények nincsenek megfelelően átvilágítva, így a hackerek könnyen publikálhatnak rosszindulatú példányokat. Mivel a böngésző megbízható alkalmazás, így a víruskeresőnek nehéz felismerni ezeket a rosszindulatú bővítményeket. Ezek telepítéséhez általában a felhasználó engedélye szükséges, sok böngésző alapértelmezettként engedélyezi az interakciót a felhasználó megkérdezése nélkül. [10]

7. Adathalász támadás példák

7.1 Játékokban

Az adatok megszerzése különböző internetes játékoknál is elterjedt. A csaló, a hivatalos cégtől származott üzenetnek álcázva veszi rá a felhasználókat egy weboldalra való belépéshez, különben különböző megtorlásokban részesül a játékos.



7.1. ábra - Az adathalász üzenet játékon belül - saját kép

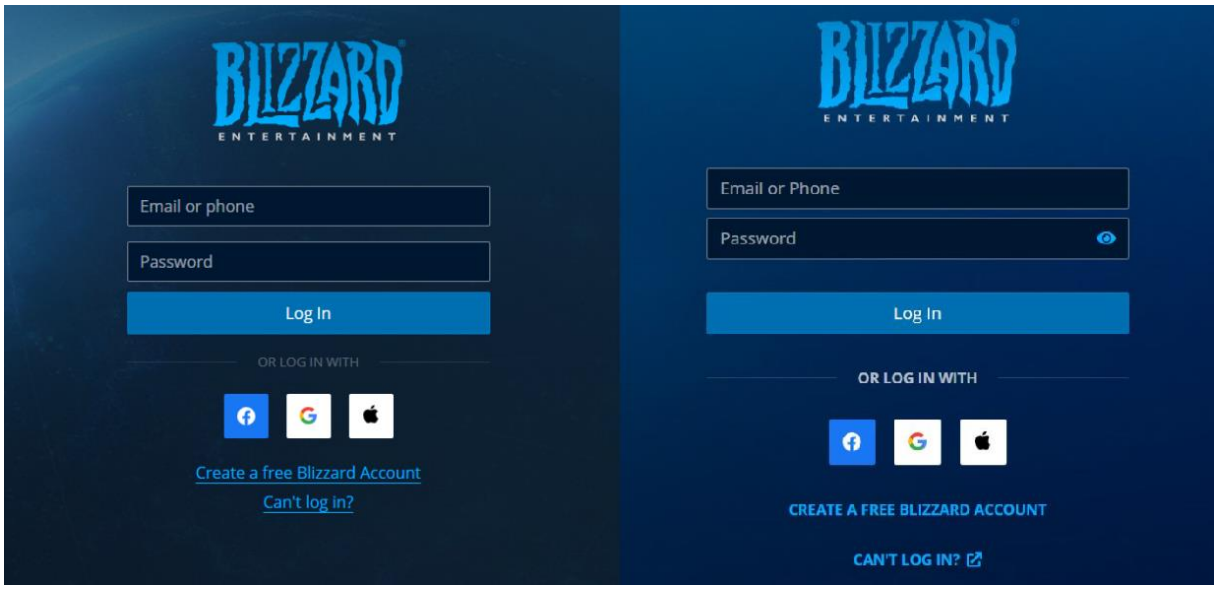
Egy World of Warcraft-ból való példánál, a csaló, a játékon belüli hivatalosnak tűnő üzenetek küldésével próbálja rávenni a közösséget egy adathalász oldal meglátogatására. A hivatalosságot sugallja a „Blizzard Entertainment”, vagyis a játékot fejlesztő cég nevének beírása a levélbe, valamint a „Bilzzard” név használata, mint feladó. Az üzenet ösztönzi a játékosokat a link megnyitására, különben a játékos fiókjuk felfüggesztésre kerül.

7.2. ábra - A feladó nem admin, hanem egy 1-es szintű karakter - saját kép

7.3. ábra - Valódi "GM" beszélgetés [41]

A csalás kiszűrése ez esetben egyszerű, mivel a név rákeresésére látni, hogy egy valószínűleg frissen készült egyes szintű karaktertől jött a levél. Egy valódi „Game Master”-től jövő üzenetnél a képernyőnk jobb felső sarkában megjelenik egy ablak, mely jelzi nekünk a beszélgetési szándékot. Az üzenetre rákattintva egy külön chat ablak jelenik meg, ahol létrejön a kommunikáció. A hivatalosságot még az is jelzi, hogy a valódi „GM”-től jövő üzenet mellett a cég logója is megjelenik a képen látható módon.

A csaló weboldalon látható [7.1. ábra] hogy ugyan olyan színeket és ábrákat használ, mint az eredeti. Apróbb különbségek vannak. Ezek fel se tűnnének, ha a két képet nem egymás mellett néznénk.



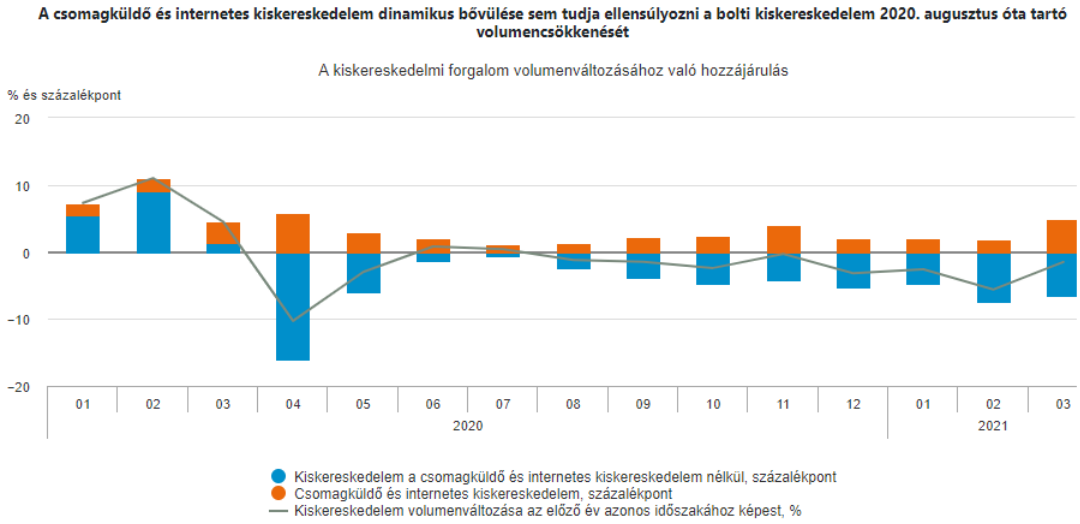
7.4. ábra - Az adathalász (bal) és a hivatalos oldal (jobb) [40] - saját kép

7.2 Flubot

Magyarországon 2021 márciusban terjedt el SMS formájában egy kártékony hivatkozást tartalmazó kéretlen szöveges üzenet, amely látszólag egy csomagküldő szolgáltatótól érkezett. Az üzenet megpróbálja rávenni a címzettet a link megnyitására, mely egy valódi cég weboldalának másolata.

Az üzenetek tartalma*: „Megérkezett a csomagja, kövesse nyomon itt: https://<változó hivatkozás>”.*

A link megnyitását követően egy másolt weboldal bejelentkezési felületét látjuk, mely készteti a felhasználót egy alkalmazás telepítésére, mellyel a rendelt csomagot nyomon tudja követni. A KSH adataiból kimutatható, hogy a COVID miatti lezárások alatt (2020-2021) az e-kereskedelem is megugrott. A több online rendelés miatt valószínűleg még több ember lett áldozata ennek a technikának. Kattintás után meglátva az ismerős weboldalt, melynek színei, logója, képei teljesen megegyeznek az eredetivel, a bizalom is növekszik az először gyanúsnak tűnt SMS láttán. Viszont az úgynevezett csomagkövető alkalmazás telepítésével egy trójai vírus kerül az adott eszközre, melynek köszönhetően a támadó hozzáfér minden adatunkhoz. Az adatlopó tulajdonságokkal rendelkező alkalmazás hozzáférést nyújt például az SMS írás, küldés, telefonkönyv, Internet, Bluetooth és még sok mindenhez a telefonon. A csalók képesek a fertőzött eszközről hasonló üzenetet küldeni más hívószámra, mely a kimeneti üzenetek között nem lesznek láthatóak, így a felhasználó észre se veszi a tevékenységet.



7.5. ábra - Csomagküldő internetes kereskedelem növekedése [42]

A FluBot variánsa, melyet pénzügyi szolgáltatások és banki adatok megszerzésére hoztak létre, képes egyszer használatos jelszavak ellopására is.

Főleg az Android eszközök vannak kitéve ennek a támadásnak, de hasonló SMS-ek iOS készülékeken is megjelentek, melyekben iPhone készülék nyerési lehetőséggel próbálják rávenni az embereket adatok megadására.

Az alkalmazás telepítése után a FluBot folyamatosan figyeli az adott készüléket, majd mikor pénzügyi alkalmazás indítását észleli, egy eredetivel majdnem azonos adathalász felületet nyit meg, mely az ide megadott adatokat képes kinyerni és továbbítani a támadónak. Fertőzés után javasolt az eszközön gyári visszaállítást elvégezni.

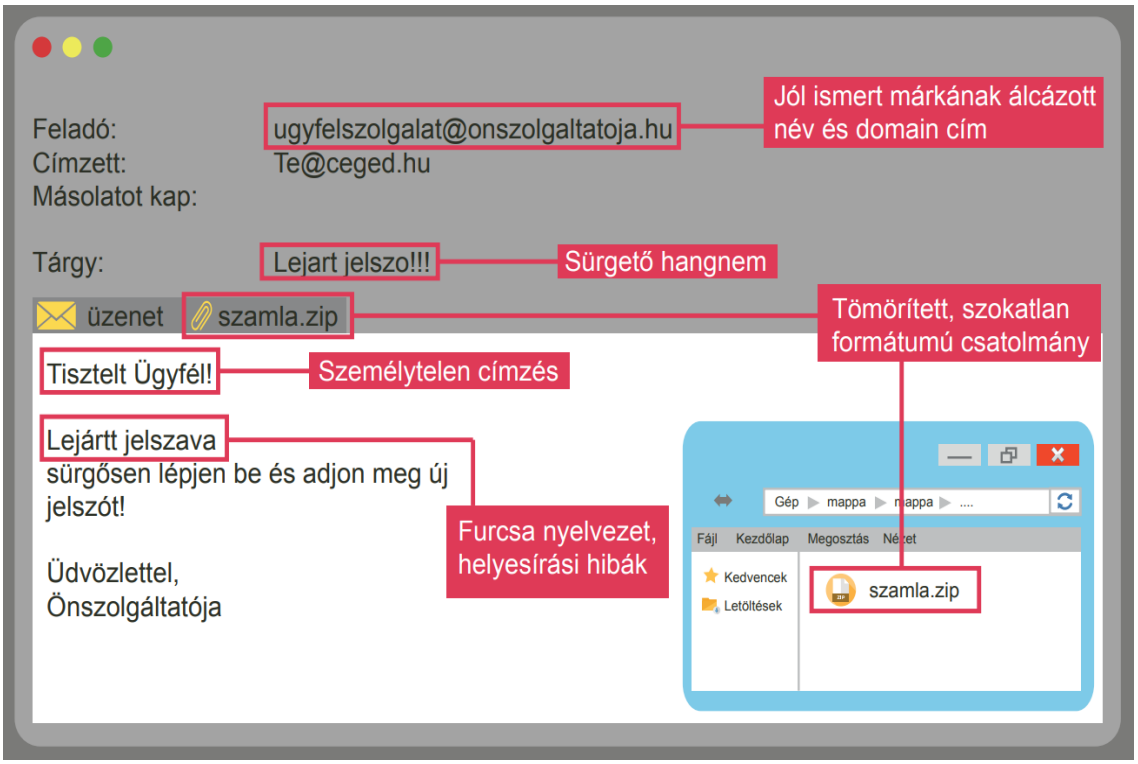
Ez volt az első kimondottan magyarokat célzó malware, melynek híre sokakhoz eljutott, így a jövőben talán sokkal elővigyázatosabban fogják kezelni a hasonló üzeneteket. [23] [24]

7.6. ábra - FluBot SMS – saját ábra

8. Mitől lesz sikeres az adathalászat?

A sikerességnek az első lépése egy jó ötlet kitalálása. Egy figyelemfelkeltő üzenet kreálása, mely a megcélzott közösséget tettre készteti. Lehet ez félelem generálással vagy valamilyen nyeremény megszerzésének kecsegtetésével, a lényeg, hogy a célszemély kiadja adatait.

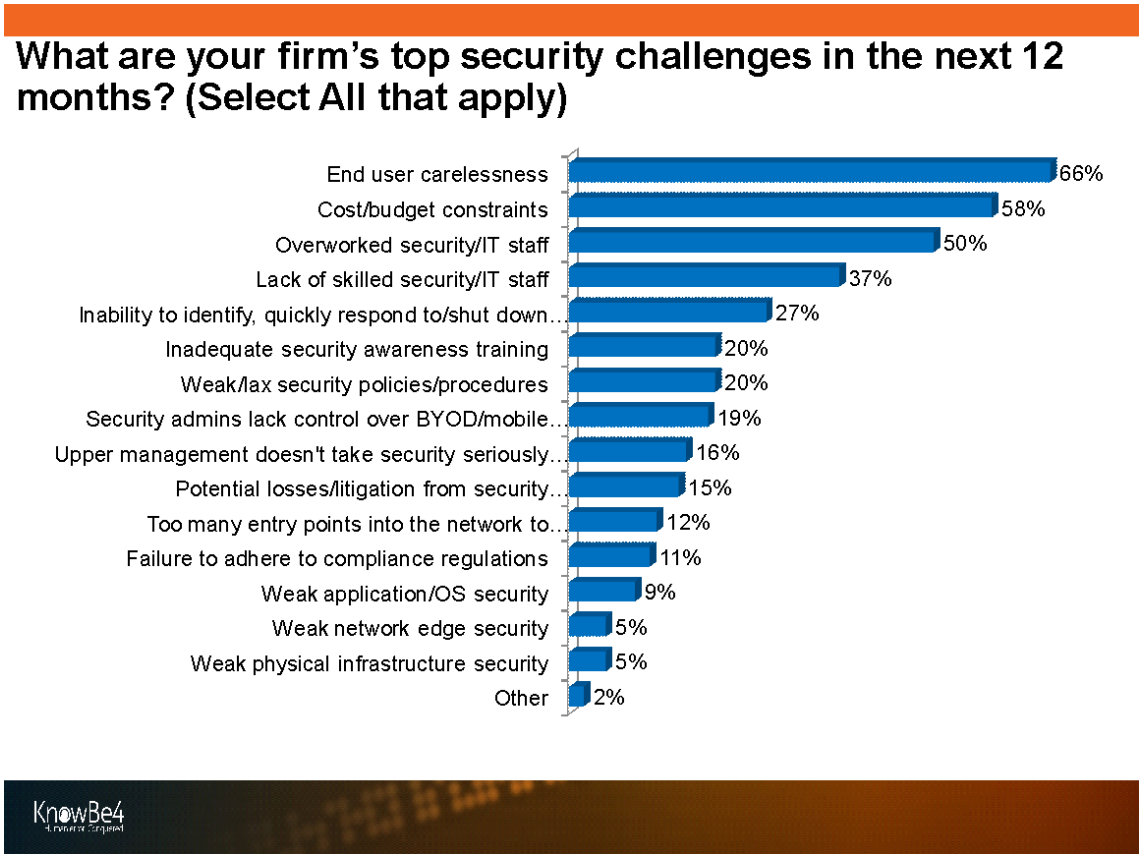
Az adathalász gyanús e-maileknek több jele is lehet. A csalók gyakran a jól ismert név és domain címeket hamisítják akár egy vagy két karakter átírásával, ami először fel se tűnhet a felhasználónak. A furcsa nyelvezeti hibák is gyanút kelthetnek egy levélben, valamint a sürgető hangnem, felszólítás például egy lejárt jelszó megváltoztatására. Az e-mail csatolmányát a támadók tömörítve küldhetik el, így csak letöltés és kicsomagolás után derül ki a tényleges formátum. Beágyazott káros kódot is tartalmazhat a levél, mely megnyitása esetén felugrik egy párbeszédablak a makrók engedélyezésére .doc, .xls, .ppt, stb. formátumok esetén. Ha adathalász gyanús az e-mail, ezen makrók engedélyezése nem ajánlott. [25]



8.1. ábra - Adathalász-gyanús e-mail felismerése [25]

9. Intézkedések és védelem

Összességében mind felhasználói, mind vállalati szinten szükség van módosításokra, melyek alkalmazásával az adathalászat egy sokkal áttekinthetőbb és könnyebben leküzdhető jelenséggé válhat. Fontos a dolgozók taníttatása, felkészítése az esetleges támadásokra. Ahogy ezt a lenti ábrán is láthatjuk, a „KnowBe4" által megkérdezett cégek kétharmada szerint a végfelhasználó a legkritikusabb elem.



9.1. ábra - A végfelhasználó a legkritikusabb elem a cégek szerint [32]

9.1 Nagyvállalati védelmi intézkedések

Multinacionális környezetben manapság gyakran szerveznek tudatosító („awareness") kampányokat, a felhasználók veszélytudatának felmérésére, javítására. Ezeken való részvételi arányt ajándékokkal például pólóval, naptárral lehet növelni, így még több emberhez eljut az üzenet. Az offline kampányoknál gyakori a standos módszer, mikor a felhasználók 5-6 állomást járnak be, melyek különböző IT biztonsági témákhoz kapcsolódnak. A résztvevők így megismerhetik a veszélyeket, felismerési módszereket és támadás esetén kisebb eséllyel válnak áldozattá. Hátránya ezeknek a kampányoknak, hogy sok előkészületet igényelnek és sok ember bevonása kell a megszervezéshez. Előnye a személyes találkozás, melynél a felhasználók kötetlenül beszélgethetnek a témában, feltehetik kérdéseiket.

Az online kampányoknál a vállalat e-mailben küldhet ki információkat információbiztonsági témákról, vagy konferenciabeszélgetésre invitálhatják a dolgozókat. Saját tapasztalatom alapján a Deutsche Telekom System Solutions Hungary Kft.-nél népszerű a saját fejlesztésű „16 Minutes" nevű kampány, melynek neve is sugallja, hogy csak tizenhat percből áll. A rövid idő miatt ezen az emberek sokkal szívesebben részt vesznek, mint a több órás beszélgetéseken és konferenciákon. Ebben a bő negyedórában különböző érdekes IT biztonsági kérdések bemutatására kerül sor, melyek felkeltik a felhasználók figyelmét a témával kapcsolatban és sokkal elővigyázatosabbak lesznek.

A poszter kampánynál érdekes, tanulságos üzenetek vannak elhelyezve a munkahely több részén. A rövid üzenetek sokkal jobban megemészthetőek a dolgozók számára a sok oldalas leírásokkal szemben.

Az adathalász kampány a cég által létrehozott támadás szimulálása, melynél a felhasználóknak kiküldött figyelemfelkeltő e-mailben adatok megadását kérik. Az esetleges bizalmas adatok vagy jelszavak megadása és elküldése után elemezhető a dolgozók biztonságtudatossága. Statisztikák felfedik, hogy hányan nyitották meg a levelet, kattintottak rá a gyanús linkre, kik adtak meg személyes adatokat.

Ezek a rendezvények a felhasználókat tudatosabbá teszik, ellenállóbbak lesznek az információbiztonsági támadásokkal szemben.

9.2 Biztonságtudatosság már fiatalkorban

Manapság egyre sokoldalúbb és nehezen felismerhető támadások miatt érdemes már fiatalkorban a biztonságtudatosság tanítására törekedni. Célszerű lenne a nagyvállalatokhoz hasonlóan az iskolákban is rendszeres kampányokat, előadásokat tartani, melyektől már fiatalon megtudhatjuk az interneten leselkedő veszélyeket.

Az egyik legfontosabb, hogy megtanuljunk a jelszavakkal bánni, ne adjuk ki barátainknak se őket, valamint fontos az erős jelszó választása. A jó jelszóban nem szerepel értelmes szó, legalább 8-12 karakter hosszú, tartalmaz kis- és nagybetűt, számot, speciális karaktert. Ezek alapján egy ideális jelszó például „Kd5/uH78wl3E". A mai világban rengeteg weboldalra regisztrálunk. Sok internethasználónak 50-80 helyre is van regisztrált fiókja, melyeknél legtöbben ugyan azt a jelszót használják sok helyre. Egy 2019-es Google által készített kutatásból kiderül, hogy az emberek 52%-a ugyanazt a jelszót használja több bejelentkező felületre is. Ez nagyon veszélyes, mivel, ha egy jelentéktelen oldalról kiszivárognak jelszavak, ezek felhasználhatóak lesznek fontosabb weboldalaknál, e-maileknél, banki fiókoknál. Így a csalók a biztonságosnak vélt helyekre is bejuthatnak a nevünkben, üzenetet küldhetnek, adatokat lophatnak el. Fontos tehát a jelszavak rendszeres cserélése, erős és különböző jelszavak használata minden webhelynél. Ebben segítséget nyújtanak a jelszó menedzser programok, mint például a „KeePass", melynél elég egy mesterjelszót megjegyeznünk, a többit tárolja az alkalmazás. [26]

Szükségét látom a fiatalok megtanítását arra is, hogy ne adjanak ki magukról sok adatot a közösségi oldalakon. Manapság nagyon elterjedt a képek, érdeklődési körök, helyszínek megosztása egyes oldalakon, így a csalók ezeket felhasználhatják ellenünk egy esetleges támadási kísérletnél.

Meg kell tanulni, hogy ne adjuk ki adatainkat bárkinek, ne bízzunk meg senkiben se az interneten. Kerüljük a gyanúsnak tűnő weboldalakat, ne töltsünk le megbízhatatlan oldalakról. Egy rossz kattintás súlyos károkat okozhat, mely az adataink kikerülését vagy elvesztését is jelentheti.

Fontos az operációs rendszer és a programok frissítése, így elkerülhetők a régi verziókon levő sérülékenységek felhasználása a gépünk ellen.

Sok mindent elkövethetünk adataink és magunk védelmében, de a támadások legsérülékenyebb szereplője maga a felhasználó. Ezért is ilyen népszerűek és eredményesek az adathalász támadások. Egy figyelemfelkeltő, sürgető vagy nyereményt ígérő e-mail sok embert megtéveszthet.

Egy nagy veszély a piaci szereplők körében az elhallgatott biztonsági események száma. A nagyvállalatok jóhírüket féltve sokszor nem jelentik a bajt, ezzel másoknak akár komoly károkat okozva. Egyébként kötelességük lenne ezeket jelenteni az Általános Adatvédelmi Rendelet (GDPR) szerint.

9.3 A naiv idős korosztály

Az idősebb emberek hamarabb lesznek célpontok a hackerek számára, mivel nem töltenek annyi időt az interneten, így könnyebb átverni őket. Manapság használt manipulatív adathalász támadások még a képzett szakembereket is be tudják csapni. Az időseket még jobban lehet manipulálni, sokkal kiszolgáltatatottabbak a támadásokkal szemben a technikai újdonságok és kellő tapasztalat hiánya miatt. Nehéz nyomon követni, hogy ők milyen gyakran válnak kibertámadás áldozatává. Az FBI internetes bűnüldözéssel kapcsolatos panaszközpontjának 2018-as kimutatása szerint több mint 62.000 csalási panaszt jelentettek be a hatvan év feletti állampolgárok. A károk összege 649 millió dollár volt, mely ebben az évben a károk majdnem 50%-át tette ki, miközben a 60 év feletti korosztály csak a bejelentések 24%-t tette ki. Az AARP kutatása szerint Amerikában az időseket különösen a pénzügyi csalások sújtják. [27] [30] [31]

Victims		
Age Range[14]	Total Count	Total Loss
Under 20	9,129	$12,553,082
20 - 29	40,924	$134,485,965
30 - 39	46,342	$305,699,977
40 - 49	50,545	$405,612,455
50 - 59	48,642	$494,926,300
Over 60	62,085	$649,227,724

9.2. ábra - 2018-ban az FBI által jelentett adathalász támadások az USA-ban [27]

Vannak források, melyek segíthetnek az idősebbeknek a káresetek elkerülésében. Az amerikai „Cybersecurity & Infrastructure Security Agency" (CISA) készített egy listát, hogy mire figyeljenek igazán az online biztonság megőrzése érdekében. Ilyen például az erős és nem könnyen kitalálható jelszavak használata és ezek nem többszöri felhasználása. Egy internetes linkre kattintás előtt mindig gondolják át, hogy vajon rejthet-e veszélyt. Ne osszanak meg bármit az interneten a közösségi médiában, valamint az internetes vásárlásnál is figyeljenek, milyen oldalról rendelnek. Természetesen ezen pontok betartása nem csak az idős korosztálynak ajánlott, de ők hajlamosak ezeknek az alapvető elveknek figyelmen kívül hagyására. [28]

10. Adathalász támadás megtervezése

Egy adathalász támadásnál az egyik legfontosabb a megfelelő téma kiválasztása a megcélzott csoport érdeklődési körének megfelelően. Az e-mail témája lehet egy aktuális hír, melyre az emberek sokkal fogékonyabbak, nagyobb a kattintási esély. Például korona vírussal kapcsolatos téma jó választás, vagy évszaknak megfelelően télen Mikulásos, nyáron nyaralásos nyereményjátékok a dolgozóknak. A lényeg, hogy valamivel rá kell venni a felhasználót, hogy rákattintson a megadott linkre, és megadja az adatait.

Ha megvan a téma, jöhet az e-mailcímek gyűjtése. Ez lehet külső forrásból. A közösségi oldalak, például a LinkedIn, rengeteg címet tartalmaznak. Van, hogy elég a dolgozók nevét megszerezni. A nagyvállalatok sokszor név alapján generálnak munkahelyi e-mailcímeket egy bizonyos minta alapján. Ha megvan a minta, onnantól össze lehet állítani a nevekből egy listát, mely a lehetséges e-mailcímeket tartalmazza.
A levelek kiküldésénél érdemes figyelni, hogy ne egyszerre történjenek, mivel az gyanús lehet, így általában pár napos csúszásokban, hullámokban küldik ki az adathalász e-maileket.

Az adathalász teszt után jelentés készül, mely tartalmazhatja a levelet megnyitott személyek számát, linkre kattintások számát, hányan adtak meg adatokat, hányan jelentették a levelet adathalász gyanúval. Következtetéseket lehet vonni, hogy a dolgozók mennyire vannak felkészülve a támadások felismerésére. A megvalósított adathalász kísérlet után tarthatók a 9.1. alfejezetben már említett „awareness” kampányok digitális és személyes rendezvények formájában. A következő adathalász teszt után össze lehet hasonlítani az új és a régi eredményeket, meg lehet figyelni, hogy mennyit fejlődött a felhasználók biztonságtudatossága.

Egy multinacionális cégcsoporton belül már elvégzett adathalász kutatás során a 2020-as tudatossági kampány témája egy koronavírus maszk igénylése volt. A felmérésben különböző arányban vettek részt az egyes vállalatok. A teszt során az előre vártnál több volt a kattintások száma, 43%-a volt. Az adathalászat gyanúját csak 5% jelentette a hivatalos folyamat szerint. Ebből az következett, hogy a szervezeten belül egy ráerősítő kampány lett elvégezve, illetve utánkövetésképpen 2021-ben megnézik, hogy hogyan változik ez az arány. Az eredmények arra sarkallták a szervezőket, hogy az utánkövetés során az egyes vállalatokat teljes valójukban vizsgálják.

A 2021-es adathalász e-mail kiküldését a német anyacég végezte, melyre ősszel került sor. Az eredmények még nem jelentek meg, de várhatóan jobbak lesznek a 2020-as felkészítő kampányoknak köszönhetően.

11. **Saját adathalász kampány megvalósítása**

Lehetőségem volt belelátni egy multinacionális cég tudatossági felmérésébe, mely rengeteg előkészületet és kommunikációt igényel. Célom egy hasonló teszt saját megvalósítása volt az Óbudai Egyetemen. A tesztben egy belülről kiküldött, sürgető e-mail ösztönzi a célpontot a levélben szereplő link (http://elearning.uni-obuda.tk/) megnyitására, mely a Moodle oldal egy másolata. A belépési adatok és bejelentkezés gomb megnyomása után az adatok egy adatbázisban kerülnek. Ezen adatok az IP, user agent, felhasználónév és jelszó. Természetesen a megadott jelszavakat sózva, hashelve kerülnek tárolásra, mely gyakorlatilag visszafejthetetlen. A felhasználónevek hashelését is szükségesnek láttam, mivel az éles kivitelezésnél így a kitöltő személy anonim maradhat.

Ezen kívül megvalósítottam a jelszavak hosszának tárolását (6-nál rövidebb, 9-10 közötti, 11+ karakter), tartalmaz-e a jelszó nagybetűt, számot, speciális karaktert. Ezzel szerettem volna vizsgálni, hogy a tesztben szereplő célpontok mennyire használnak biztonságos jelszavakat. A jövőben megvalósítandó éles kivitelezés során ez az információ hasznos lesz abban, hogy a diákok és az alkalmazottak egyetemi fiókjához tartozó jelszavak biztonságossága felmérhető legyen.

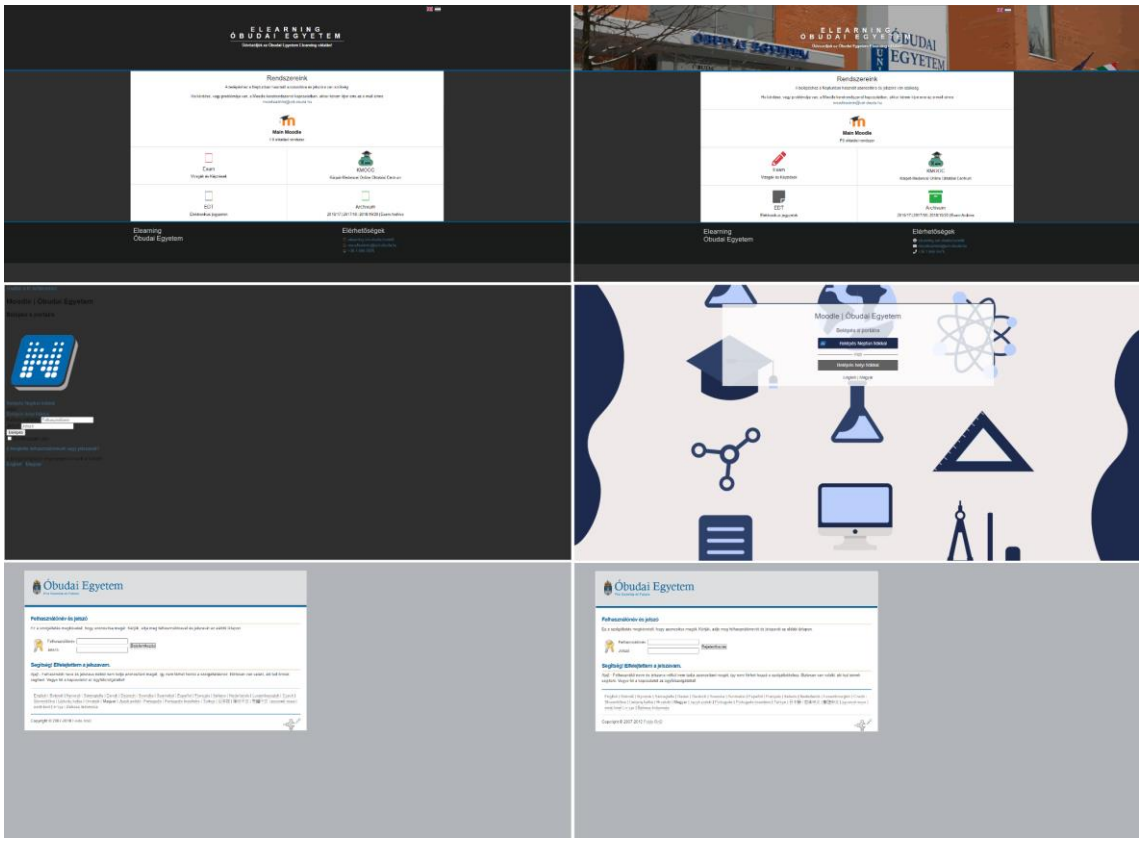
A teszt célja, hogy fel lehessen mérni az egyetemi oktatók/hallgatók mennyire fogékonyak egy ilyen támadásra.

A kiküldést követően az adatok gyűjtésére körülbelül 1 hetet tervezek, majd az utolsó e-mailek kiküldése után két héttel elküldésre kerül egy második e-mailt is, mely beszámol a teszt eredményéről, és felhívja a figyelmet erre a veszélyre. Így egy valós támadásnál kevesebben adják majd meg adataikat.

11.1 **Weboldal elkészítése**

Az adathalász teszt elvégzéséhez az egyetemen használt Moodle oldalt választottam (https://elearning.uni-obuda.hu/). Itt három oldal megvalósítására volt szükség. Az első az egyetem e-learning oldala, melyen a “Main Moodle” gombra kattintva eljutunk a második oldalra, majd a “Bejelentkezés Neptun fiókkal” gomb átirányít minket a bejelentkező felületre. A cél az volt, hogy ezen oldalak másolata minél jobban hasonlítson az eredetihez. [48]

Először az oldalak lettek lementve HTML formátumban, melyek az 11.1. ábra bal oldalán láthatóak a kezdő állapotban. A jobb oldalra az adott oldal eredeti kinézete került. Összehasonlítva az oldalakat látjuk, hogy a bejelentkező website másolata jól sikerült, viszont a másik kettőnél vannak elcsúszások, valamint hiányoznak képek. Ezek javítása volt a következő lépés.

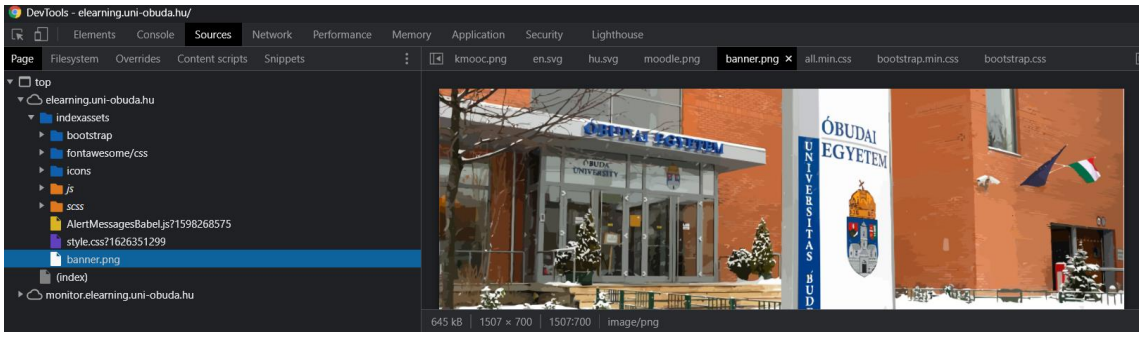


11.1. ábra - Lementett HTML oldalak (balra) és az eredeti oldalak (jobbra) [48] - saját kép

Az eredeti oldalak forráskódjából elérhetőek a hiányzó képek. A középső oldal bonyolultsága miatt a másoláshoz felhasználtam a wayback machine downloader oldalt mely segített az weboldal klónozásában. [45]

Az után csak a háttérkép beállítására és a hivatkozások átírására volt szükség a forráskódban, hogy ne az eredeti moodle-re, hanem a másolatra irányítson át kattintáskor.

Az oldal működéséhez nem szükséges tartalmak a másolt oldalak forráskódjából törlésre kerültek.



11.2. ábra - Háttérkép lementése az eredeti oldalról [48]

A szerver oldalt PHP nyelven valósítottam meg. A kódban először meg kellett adni az adatbázis kapcsolódási adatokat: hostnév, port, adatbázis neve, tábla neve, felhasználónév

és jelszó, valamint a mentett felhasználónevek és jelszavak hasheléséhez használt só, az alábbi példához hasonló módon.

```
$db_host = "localhost";
$db_port = 3306;
$db_database = "adatbázis_neve";
$db_table = "tábla_név";
$db_username = "felhasználónév";
$db_password = "jelszó";

$password_salt = "jelszó_só";
$username_salt = "felhasználónév_só";
```

11.3. ábra - Adatbázis kapcsolódási adatok - saját kép

```
// SQL csatlakozás
$conn = mysqli_connect($db_host, $db_username, $db_password, $db_database, $db_port);

// Check connection
if (!$conn) {
  die("Connection failed: " . mysqli_connect_error());
}
//echo "Connected successfully";
```

11.4. ábra - Adatbázis csatlakozás - saját kép

A weboldalra beírt adatok és bejelentkezés után lekérdezhető az IP cím és a User agent, valamint a felhasználónév és jelszó hasheket az alábbi kód végzi.

```
$ip_address = $_SERVER['REMOTE_ADDR'];
$user_agent = $_SERVER['HTTP_USER_AGENT'];
$username = hash("sha256", $_POST['username'].$username_salt);
$password_hash = hash("sha256", $_POST['password'].$password_salt);
```

11.5. ábra - Weboldalra beírt adatok mentése - saját kép

A jelszó karakterisztikát különböző módon vizsgáltam. Eltároltam a jelszavak hosszának kategóriáját. “low” jelzést kaptak a 6 karakternél rövidebb jelszavak, “medium”-ot a 6 és 10 karakter közöttiek, és “good”-ot a 11 karakternél hosszabbak. A 6 karakternél kisebb jelszavak azért is számítanak rossznak, mivel szinte azonnal feltörhetők. 8 karakteres jelszó 24 órán belül törhető, így a közepes kategóriába soroltam. Jelszóválasztásnál érdemes azt figyelembe venni, hogy minden növelt karakterszámmal exponenciálisan csökken annak az esélye, hogy az adott jelszót meg lehessen fejteni. [50]

```php
$pw = $_POST['password'];
$specCharNumber;
$pwLength = strlen($pw);
if($pwLength<6)
    {
        $password_lengthCategory = "low";
    }
    else if ($pwLength>=6 && $pwLength<11)
        {
            $password_lengthCategory = "medium";
        }
        else
        {
            $password_lengthCategory = "good";
        }
```

11.6. ábra - Jelszó hossz kategória - saját kép

Tárolásra került a jelszavak összetétele is, vagyis az, hogy tartalmaz-e nagybetűt, számot vagy speciális karaktert.

```php
//spec karakter (password_specialCharExist)
if (preg_match('/\W/u', $pw) == 1)
{
    $password_specialCharExist = "true";
}
else
{
    $password_specialCharExist = "false";
}

//nagybetűk (password_capitalLetterExist)
if (preg_match('/\p{Lu}/u', $pw) == 1)
{
    $password_capitalLetterExist = "true";
}
else
{
    $password_capitalLetterExist = "false";
}

//szám (password_numberExist)
if (preg_match('/\d/u', $pw) == 1)
{
    $password_numberExist = "true";
}
else
{
    $password_numberExist = "false";
}
```

11.7. ábra - Jelszó tartalmazásvizsgálat - saját kép

A következő lépés az adatok az adatbázisba mentése volt.

```php
$sql = "INSERT INTO ".$db_table." (ip_address, user_agent, username, password_hash, password_lengthCategory, password_specialCharExist,
password_capitalLetterExist, password_numberExist) VALUES (?, ?, ?, ?, ?, ?, ?, ?)";
```

11.8. ábra - Adatok adatbázisba mentése - saját kép

Az adatbázis használata során figyelmet fordítottam az SQL injection kiszűrésére, mellyel hozzá lehetne férni az adatbázishoz, a beviteli mezőbe való megfelelő SQL lekérdezés írásával. Ezért az utasítást (prepare függvény) és az adatot (bind_param függvény) szeparáltan küldtem, így megakadályoztam ennek a sérülékenységnek a kihasználását. A prepare függvényben került előkészítésre az SQL utasítás. A bind_param függvényben kerülnek átadásra a változók, az első paraméterként megadott karaktersorozat által meghatározott típusokkal (s=string). A fenti függvényekkel elkészített utasítást ezután az execute függvény hajtja végre. [51]

```
//sql injection kiszűrése
$statement = $conn->prepare($sql);
$statement->bind_param("ssssssss", $ip_address, $user_agent, $username,
$password_hash, $password_lengthCategory, $password_specialCharExist,
$password_capitalLetterExist, $password_numberExist);

//lekérdezés végrehajtása
if ($statement->execute() === TRUE) {
  //echo "New record created successfully";
} else {
  echo "Error: " . $sql . "<br>" . $conn->error;
}

$conn->close();
```

11.9. ábra - SQL injection kiszűrése - saját kép

11.2 Weboldal tesztelése

A kezdeti tesztelést helyi gépen XAMPP segítségével oldottam meg, Apache és MySQL használatával, mely egy hasonló környezetet biztosít, mint a végleges webtárhely. A weboldalak és a hozzá tartozó fájlok bemásolása (C:\xampp\htdocs) után a http://localhost/-ot a böngészőbe beírva értem el a weboldalt, és teszteltem, hogy az oldalakon a hivatkozások jó helyekre irányítanak-e át, illetve minden úgy jelenik-e meg, mint az eredeti oldalon.

A domaint a Freenom oldalról igényeltem, ami ingyenesen elérhető .tk végű url-t biztosít. A másolt weboldal címe uni-obuda.tk lett.

A következő lépésben élesben is tesztelnem kellett az oldalakat. Kezdetben a 000webhost tárhelyét használtam. A fájlok feltöltése, az adatbázis létrehozása és szerkezetének kialakítása után a weboldal készen állt a használatra. Az oldalra beírt felhasználónév és jelszó a bejelentkezés gomb megnyomása után bekerült az adatbázisba.

Későbbiekben a Hostinger oldalra váltottam a prémium befizetése után, mely lehetővé tette az aldomainek létrehozását, (elearning.uni-obuda.tk és idp.uni-obuda.tk) valamint az SSL tanúsítványok hozzáadását.

11.3 SSL

Hogy az adathalász teszt minél hitelesebb legyen szükségem volt SSL tanúsítványokra a weboldalhoz, melyeket ingyenesen meg tudtam igényelni az Sslforfree oldalról. A Hostinger webtárhely oldalon prémium befizetése után lehetett feltölteni a tanúsítványokat. Ezek igényléséhez szükséges a domain birtoklásának igazolása, amit

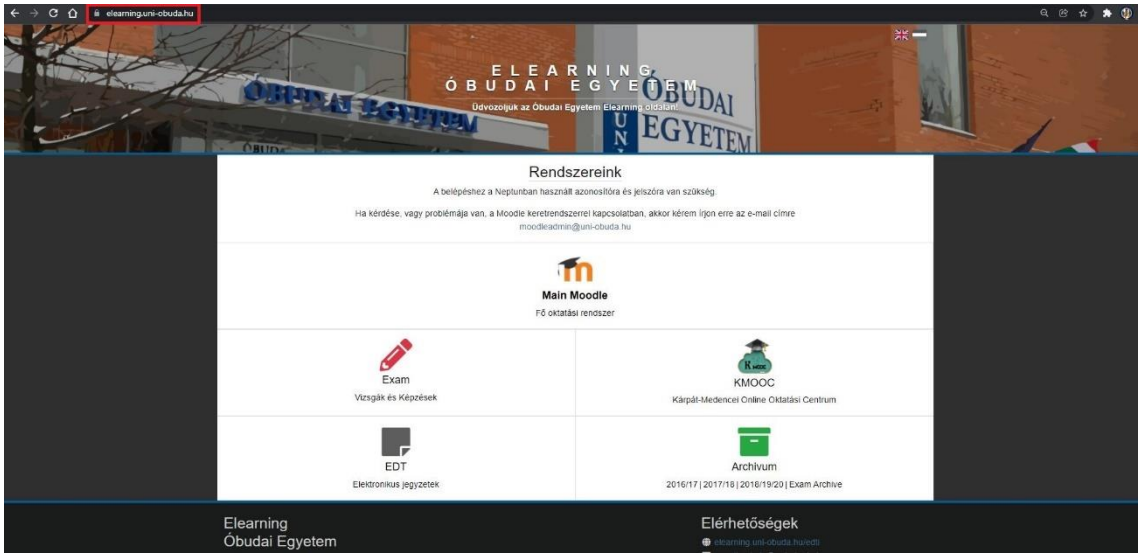
XM recordok létrehozásával és megerősítő e-mail segítségével tettem meg. A lépések elvégzése után letölthetővé váltak a tanúsítvány fájlok, amelyeket a Hostinger oldalán importáltam. Ezek után már a HTTPS protokollon keresztül is megnyitható az oldal, és a böngészőben is megjelenik a jól ismert lakat ikon az URL mellett. [44] [47] [49]

Domain	SSL Type	Status	Expires At	Created at		
uni-obuda.tk	SSL Certificate Activation	Active	2022-02-02	2021-11-04	Uninstall	Force HTTPS
elearning.uni-obuda.tk	SSL Certificate Activation	Active	2022-02-02	2021-11-04	Uninstall	Force HTTPS
idp.uni-obuda.tk	SSL Certificate Activation	Active	2022-02-02	2021-11-04	Uninstall	Unforce HTTPS

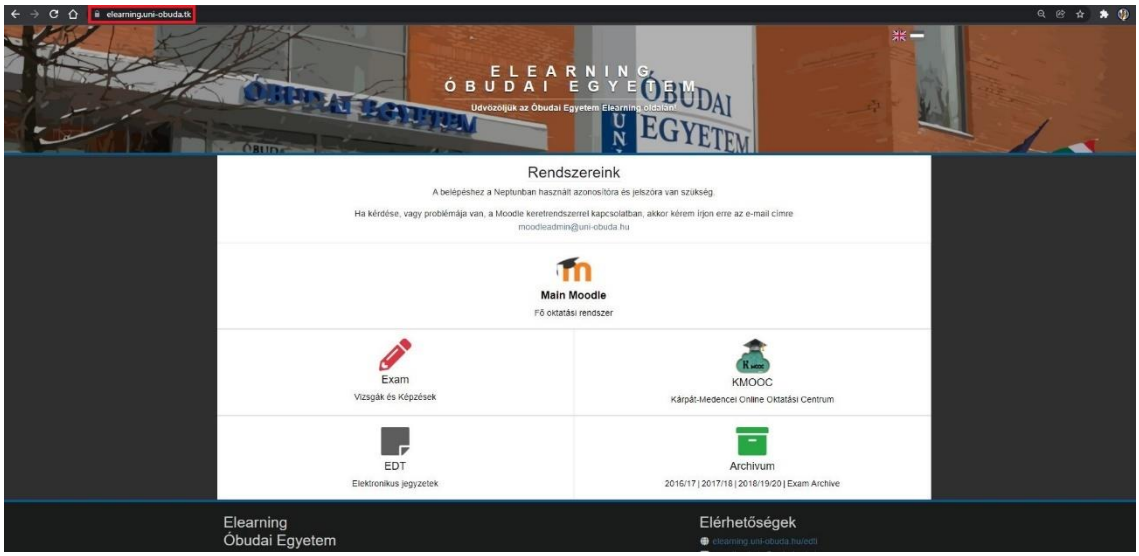
11.10. ábra - SSL tanúsítványok az oldalakhoz - saját kép

11.11. ábra - Az oldal már HTTPS protokollon keresztül is megnyitható - saját kép

Az eredeti és a másolt oldalak között végül alig lehet észrevenni a különbséget. Kinézetükben teljesen megegyeznek, kivéve az adathalász oldalnál az URL-ben .hu helyett .tk domain látható. A 11.12. ábrán látható az eredeti, és a 11.13 képen a hamis oldal.



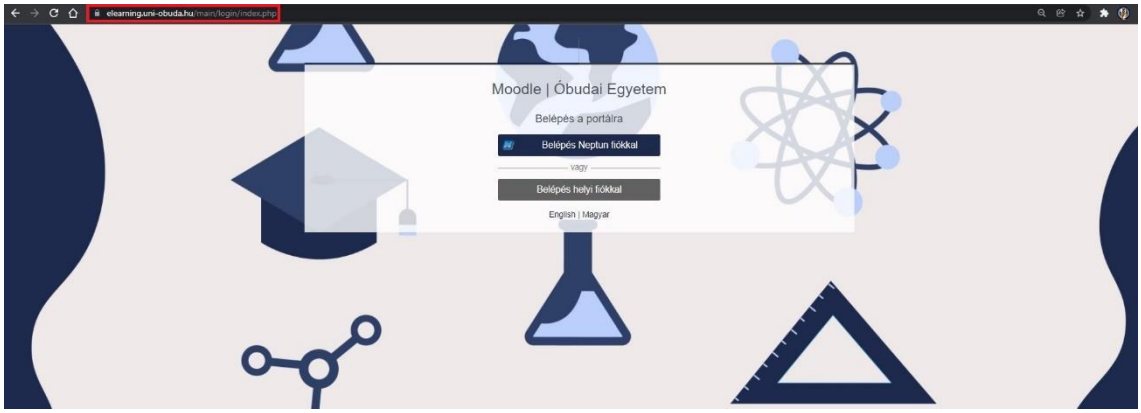
11.12. ábra - Eredeti kezdőoldal [48] - saját kép



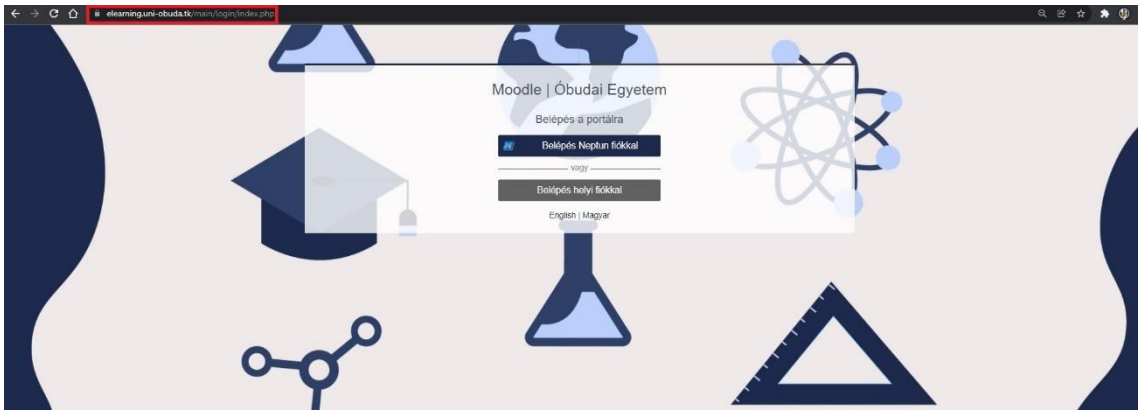
11.13. ábra - Adathalász kezdőoldal - saját kép

A Main Moodle feliratra kattintva a következő oldalnál még kevésbé feltűnő a különbség, a hosszabb URL miatt. A mappaszerkezetet és a fájlok elnevezését szándékosan úgy hoztam létre, mint ahogy az az eredeti sávban látható. Ez igaz a harmadik oldalunkra is, mely a Belépés a Neptun fiókkal gombra kattintva érünk el.

Mindhárom oldalnál a kinézetben a különbség csak az említett két betű az URL-ben, így a hasonlóság sokakat megtéveszthet.

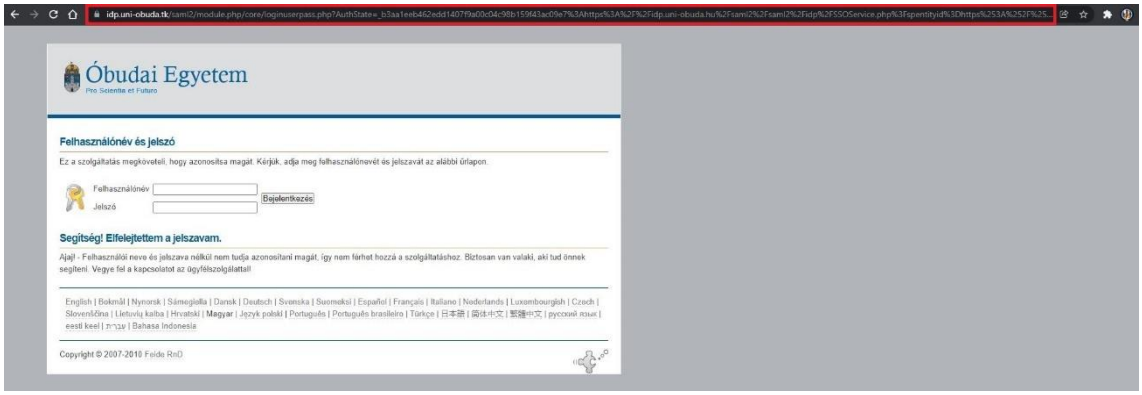


11.14. ábra - Eredeti középső oldal [48] - saját kép



11.15. ábra - Adathalász középső oldal - saját kép

11.16. ábra - Eredeti bejelentkező oldal [48] - saját kép

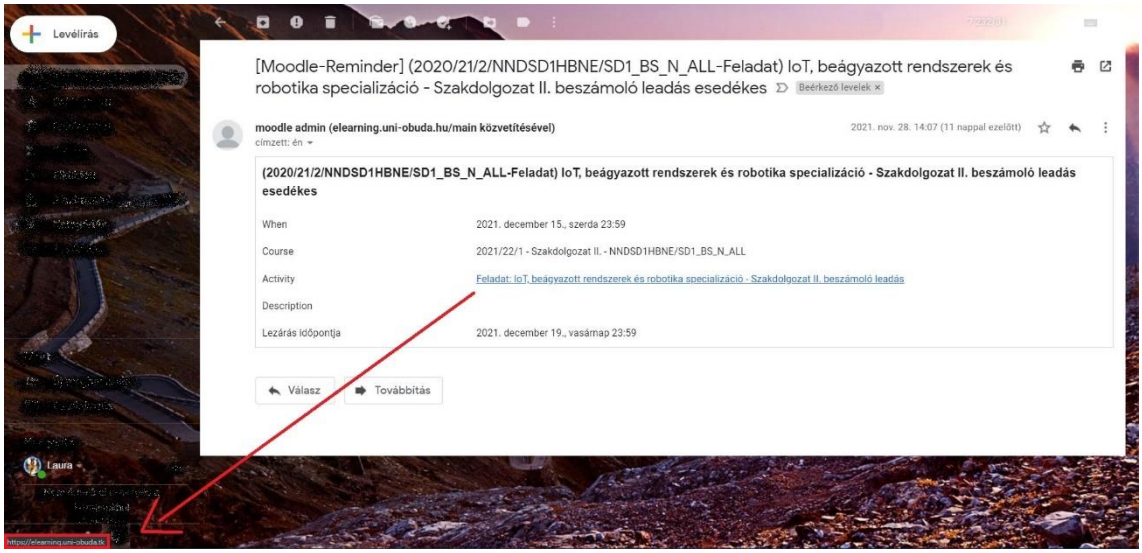


11.17. ábra - Adathalász bejelentkező oldal - saját kép

11.4 **E-mail küldés**

Engedély hiányában sajnos nem volt mód az adathalász teszt megvalósítására az egyetemen, azonban a teljes phishing folyamat végig futtatásra került, pusztán a címzettek tértek el. A kiküldött e-mailek tartalma tetszőleges lehet, a cél az, hogy az áldozat a benne található linkre kattintson. Emiatt érdemes valamilyen sürgető tartalommal feltölteni.

Az általam készített e-mail szövege a Szakdolgozat II. kurzus egy feladatának beadási határidejére figyelmeztet. Az adathalász oldal URL-je egy valódinak tűnő hivatkozásban van elrejtve a képen látható módon.

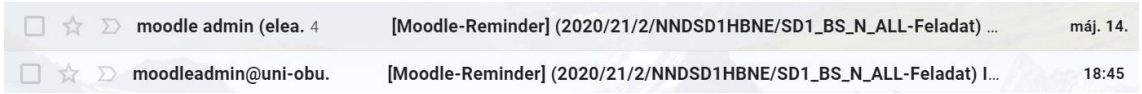


11.18. ábra - Adathalász e-mail - saját kép

A linkre kattintva betöltődik az adathalász weboldal, mely szinte teljesen megegyezik az eredetivel, így az ide látogatók nyugodtan írják majd be adataikat az adott mezőbe.

11.19. ábra - Eredeti moodle e-mail - saját kép

A 11.18. ábrán látható a hamisított, a 11.19.-en az eredeti beérkezett üzenet, valamint a 11.20. képen a megnyitatlan üzenetek láthatók.



11.20. ábra - Eredeti (fent) és a hamis (lent) beérkezett e-mailek - saját kép

Eredeti terv szerint az e-mailek kiküldése az egyetemről ment volna egy erre létrehozott címről. Mivel az éles teszt nem valósult meg, így saját gmail címről valósítottam meg a kiküldést. Az adathalász üzenetet kettő e-mailről küldtem ki. Egyik egy régebben

létrehozott, gyakran használt fiók, másik egy direkt erre a célra létrehozott e-mail cím, mely a moodle-hoz köthető (moodleadnin@gmail.com). A rendszer tesztelése önkéntesek bevonásával történt, akik megadták az e-mail címüket. A régebben létrehozott fiókról küldött e-mailek a beérkezett üzenetekhez kerültek, míg az új e-mailcím levelei 100%-ban a spam mappában végezték a gmail esetében. Freemail és Protonmailre küldötteknél mindegyik levél a beérkezett üzenetekhez ment, egyik se került spam mappába. A Freemail szolgáltató esetében bár a levél nem került spambe, figyelmezteti a címzettet, hogy erről az e-mail címről még nem kaptunk levelet.

12. Tesztelés és adatok kiértékelése

Az adathalász üzenetben szereplő linkre kattintva eljuthatunk az adathalász oldalra, ahol a bejelentkezés után az adatbázisba kerülnek adataink, mely a 12.1. ábrán látható. Természetesen a jelszavaknak csak a hashelt változata kerül elmentésre, viszont a hashelés előtt különböző információkat nyerhetünk ki belőle.

A "password_lengthCategory" mezőben a jelszó hosszúságának kategóriáját vizsgáltam. A táblázatban látható, hogy melyik jelszó tartalmaz nagybetűt, számot, speciális karaktert. Ezek részletes vizsgálatának és statisztika kielemzésének az éles tesztnél lesz szerepe, ahol megtudhatjuk, hogy a felhasználók valódi jelszavai milyen erősségűek. Szükségét éreztem a felhasználónevek hashelésének is, mivel az éles tesztnél ez a neptunkód lenne. Így az adott tanár/diák anonim maradhat. Az ismétlődések szűrése is megoldható, ha valaki többször is próbálkozna, mivel így a felhasználónév hash értéke ugyanaz lesz. Az ismétlődések szembetűnnek és adott esetben szűrhetőek a hiteles statisztikai elemzés támogatásához, valamint a torzítások elkerülése végett. Erre látható példa a 12.1. képen az utolsó két sornál.

id	timestamp	ip_address	user_agent	username	password_hash	password_lengt	password_spec	password_capit	password_num
1	2021-11-27 22:33:41	134.255.88.23	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	b6f939fe2t	838a4a0568e12649	good	true	true	true
2	2021-11-27 22:34:43	134.255.88.23	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	deb96a8c3	e6138021377cd24fc	good	false	false	true
3	2021-11-28 00:45:18	71.79.46.87	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	7a30cf946	d96edeced7caae72	medium	false	false	true
4	2021-11-28 12:30:57	178.48.105.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	fec4c002e2	7996667344051e33	medium	false	true	true
5	2021-11-28 12:32:22	2a02:ab88:59	Mozilla/5.0 (Linux; Android 11; SAMSUNG SM-A505FN)...	cd3c1be68	6ffd3727dbefe8de27	good	true	true	true
6	2021-11-28 13:56:45	95.169.204.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	cfa651cfe8	286bbbabd021e49e	good	false	false	true
7	2021-11-28 14:07:27	94.21.105.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	6afb80e0e	3341c9ad98dd2391	good	true	false	true
8	2021-11-28 14:18:12	94.21.105.12	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWeb...	6afb80e0e	c66997b1583dbd55	good	true	true	true

12.1. ábra - Adatbázisba mentett adatok - saját kép

A tesztelést kétféleképpen végeztem el. Először az adatbázis önkéntesek bevonásával lett feltöltve, majd végeztem két tesztet először 1.000 majd 10.000 adatsorral, hogy megbizonyosodjam arról, hogy a statisztikai modul az éles kivitelezés során is használható marad. Az utóbbiakat lokális adatbázisba töltöttem fel. A PHP kód átírásával majd az oldal megnyitásával a leggyakoribb jelszavak egy text fájlból kerültek az adatbázisba, melynek szerkezete megegyezik az eredetivel.

12.1 Valóságot megközelítő adatok kiértékelése

A tesztben résztvevő személyek feladata volt a hasonló erősségű jelszó megadása, mint amit használni szoktak. Ebben az esetben 20 adatot vizsgáltam és értékeltem ki. Először a jelszó hosszának vizsgálatára térnék ki, melyet három kategória segítségével jelenítettem meg. A beküldött adatoknál 65 % jó, 35 % közepes jelszó került megadásra. 6 karakternél rövidebb jelszót egyik tesztelő se adott meg. Ez a 12.2. diagramon látható. A jelszóban a különböző karakterek meglétét igaz "true" és hamis "false" jelzéssel jelöltem az adatbázisban. Speciális karaktert az emberek 30 %-ának jelszava tartalmazott, nagybetű esetén is 30% százalék lett az eredmény. Számok esetében a tesztelők 75%-a kapott "true" jelzést az adatbázisban. Az eredmények egy része látható a 12.1. ábrán.

12.2. ábra - Statisztika saját adatokból - saját szerkesztés

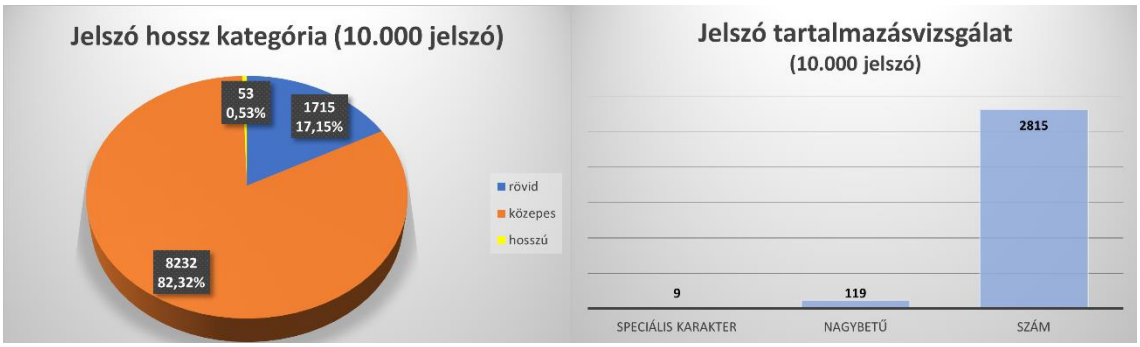
12.2 **Generált adatbázis kiértékelése**

Megvalósításra került két nagyobb, saját kezűleg generált adatbázis elemzése is. Itt a világ leggyakoribb 1.000 és 10.000 jelszavát töltöttem fel a lokális adatbázisba és elemeztem ki. [52] Így képet kaphatunk arról, hogy általában a felhasználók mennyire adnak meg erős és biztonságos jelszavakat.

A világon leggyakoribb 1.000 jelszó 84,3% (843) közepes kategóriába került, 15,5% (155) 6 karakternél rövidebb. 10-nél több karaktert csak 2 jelszó tartalmazott, vagyis 0,2%. A jelszavak 18,3%-a (183) tartalmazott számot, 0,4%-a (4) nagybetűt. Speciális karaktert egyik jelszó se tartalmazott.

A leggyakoribb 10.000 jelszónál 82,32% (8232) került a közepes, 17,15% (1715) pedig a rövid kategóriába. Hosszú jelszó hosszt csak 0,53% (53) érte el. A jelszavak 28,15%-a (2815) tartalmazott számot, 1,19%-a (119) nagybetűt, valamint 0,09% (9) tartalmazott speciális karaktert.

12.3. ábra - 1.000 jelszó statisztika - saját szerkesztés



12.4. ábra - 10.000 jelszó statisztika - saját diagram

Összességében láthatjuk, hogy a saját adatgyűjtésnél jobb eredmények lettek jelszó hossznál és tartalmazásvizsgálatnál is. A világon leggyakoribb 10.000 jelszavánál nagyobb százalékban alkalmaztak nagybetűt, számot és speciális karaktert, mint az első 1000-ben. Ez valószínűleg azért van, mert az első 1000 jelszóban a legegyszerűbbeket használják az emberek. Sokan már erősebb jelszavakat használnak, viszont világszinten a leggyakoribb jelszavak még gyengének mondhatók. Ez azért is lehet, mivel sok helyen még nem követelik meg az erős jelszavak használatát. Viszont egyre több iparági szabvány például: NIST, BSI előírja a minimum jelszókövetelményeket, ezzel növelve a felhasználói adatok biztonságát. [53] [54]

13. **Összegzés**

Dolgozatommal szerettem volna felhívni a figyelmet az adathalászatra, mely a digitális világunkban egy globális probléma. Sokféle támadási felület és technika létezése ismert, ezek bemutatására is sort kerítettem. A szakirodalmi kutatásaim és a saját tapasztalataim is megerősítették, hogy leggyengébb láncszem a felhasználó. Ha nem vagyunk eléggé felkészültek és éberek, megszerezhetik fontos adatainkat „fehérgalléros bűnözők" melyből anyagi kárunk keletkezhet, sőt munkahelyi környezetben komoly gazdasági veszteséget is okozhatunk.

A szakdolgozatomban fő célom egy saját adathalász kampány tervezése és megvalósítása volt, mellyel felmértem a tesztben szereplő személyek biztonságtudatosságát. Megvalósításra került egy adathalász támadási felület, és a hozzá tartozó adatbázis felépítése. Ehhez az Óbudai Egyetem Moodle rendszerének nyitóoldalait választottam.

A támadó weblap URL-je és kinézete szinte teljesen megegyezik az eredetivel, így az megtéveszthetti a felhasználót. Eredeti tervemben az egyetemi oktatók és hallgatók biztonsági felmérése lett volna a cél, belső címről kiküldve. Ez az egyetem számára is hasznos információval szolgált volna, de erre végül nem kaptam meg az engedélyt. Ezért önkéntesek bevonásával valósítottam meg a vizsgálatot. Az adathalász e-mailek saját gmail címekről kerültek kiküldésre, majd a kísérletben szereplők megadták adataikat az oldalon. A bejelentkezést követően mentésre került az IP cím, a user agent, valamint a hashelt felhasználónév és a jelszó.

A megszerzett adatokból jelszóhossz- és tartalmazásvizsgálat statisztika is készült, így képet kaptam arról, hogy általában a felhasználók mennyire adnak meg erős és biztonságos jelszavakat. A válaszadók többsége véleményem szerint ezt kielégítő módon megtette. Az eredmények jobbak lettek, mint a világ 10.000 leggyakoribb jelszavának statisztikájában.

Számomra a legnehezebb volt az oldal pontos és működő másolatának elkészítése, mivel nem rendelkeztem PHP programozási ismeretekkel, így meg kellett tanulnom egy új nyelvet annak megvalósításához. Meglepő számomra, hogy sok ember nem foglalkozik megfelelő mértékben az adataik biztonságával, ezért lenne szükség valós környezetben elvégzett tesztekre, amely ráirányítaná az emberek figyelmét a megfelelően biztonságos jelszóhasználat fontosságára.

Bár az eredetileg tervezett adathalász tesztet még nem hajtották végre az Óbudai Egyetemen, a vezetőség jövőre tervezi ennek megvalósítását.

14. Conclusion

With my thesis, I wanted to draw attention to phishing, which is a global problem in our digital world. The existence of a wide variety of attack surfaces and techniques are known and have been presented in the first half of my thesis. Both my literature research and my own experience has confirmed that the user is the weakest link in the information security chain. If we are not prepared and vigilant enough, “white-collar criminals” can obtain our important data, which can result in material damage and even serious economic loss in the workplace.

In my dissertation, my main goal was to design and implement my own phishing campaign to assess the security awareness of the individuals in the test. A phishing attack interface and its database have been implemented. For this, I chose the landing page of the Moodle system of the University of Óbuda.

The URL and appearance of the attacking web page is almost identical to the original, so it can mislead the user. In my original plan, the goal would have been to carry out a security test among university faculty staff and students. It was planned to use an internal mail address as the sender, to make the test even harder to detect as such. This would have provided useful information for the university as well, but in the end, I did not get permission to do so. Therefore, I carried out the study with the involvement of volunteers. Phishing e-mails were sent from my own two gmail addresses, and the volunteers provided their details on the page. After pressing login, their IP address, user agent, and hashed username and password were saved.

Password length and content analysis statistics were also compiled from the data obtained, so I got an idea of how strong and secure passwords are usually provided by users. The majority of respondents did so in my opinion in a satisfactory manner. The results were better than the statistics for the 10,000 most common passwords in the world.

The most challenging part of my work was to make an accurate and working copy of the page because I didn’t have PHP programming skills, so I had to learn a new language to make it happen. It’s surprising to me that a lot of people don’t deal adequately with the security of their data. There is a need for tests in a real-world environment that would draw people’s attention to the importance of using a secure password properly.

Although the phishing test originally planned has not yet been performed at the University of Óbuda, the management plans to implement it next year.

15. Irodalomjegyzék

[1] Confense, „History of Phishing” [Online]. Available: https://cofense.com/knowledge-center/history-of-phishing/. [Hozzáférés dátuma: 14 05 2021].

[2] P. H. O'Neill, „Ransomware may have cost the US more than $7.5 billion in 2019,” 2019. [Online]. Available: https://www.technologyreview.com/2020/01/02/131035/ransomware-may-have-cost-the-us-more-than-75-billion-in-2019/. [Hozzáférés dátuma: 14 05 2021].

[3] T. Burt, „Microsoft report shows increasing sophistication of cyber threats,” 29 09 2020. [Online]. Available: https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/.

[4] P. Gillin, „The history of phishing,” [Online]. Available: https://enterprise.verizon.com/resources/articles/s/the-history-of-phishing/. [Hozzáférés dátuma: 14 05 2021].

[5] K. Rekouche, „Early Phishing,” 2011. [Online]. Available: https://arxiv.org/ftp/arxiv/papers/1106/1106.4692.pdf. [Hozzáférés dátuma: 14 05 2021].

[6] FBI, „Internet crime report 2020,” [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf. [Hozzáférés dátuma: 14 05 2021].

[7] S. I. Five, „Ransomware Facts, Trends & Statistics for 2020,” [Online]. Available: https://securityinfive.com/ransomware-facts-trends-statistics-for-2020/.

[8] K. Skiba, „Scams Spike on Instagram, Other Social Media Sites Amid COVID-19,” [Online]. Available: https://www.aarp.org/money/scams-fraud/info-2020/social-media-scams-spike-pandemic.html. [Hozzáférés dátuma: 14 05 2021].

[9] A. Shankar, R. Shetty és B. Nath, „A Review on Phishing Attacks,” 2019. [Online]. Available: https://www.ripublication.com/ijaer19/ijaerv14n9_15.pdf. [Hozzáférés dátuma: 14 05 2021].

[10] R. Alabdan, „Phishing Attacks Survey: Types, Vectors, and Technical Approaches,” 2020. [Online]. Available: https://www.mdpi.com/1999-5903/12/10/168/htm#B24-futureinternet-12-00168. [Hozzáférés dátuma: 14 05 2021].

[11] K. Hausken és G. Levitin, „Review of systems defense and attack models,” *International Journal of Performability Engineering,* pp. 355-366. , 2012.

[12] E. O. Yeboah-Boateng és P. M. Amanor, „Phishing, SMiShing & Vishing: An Assessment of Threats against,” *Journal of Emerging Trends in Computing and Information Sciences,* 2014.

[13] E. D. Frauenstein és S. V. Flowerday, „Social Network Phishing: Becoming Habituated to Clicks and Ignorant to Threats?,” *Information Security for South Africa (ISSA),* p. 98–105, 2016.

[14] M. Jakobsson, „The Human Factor in Phishing,” [Online]. Available: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.8721&rep=rep1&type=pdf. [Hozzáférés dátuma: 14 05 2021].

[15] M. Global, „mmaglobal,” [Online]. Available: https://www.mmaglobal.com/research/mobile-internet-usage-continues-climb.

[16] D. D. Caputo, S. L. Pfleeger, J. D. Freeman és M. E. Johnson, „Going spear Phishing: Exploring Embedded Training and Awareness,” *IEEE Security & Privacy,* pp. 28 - 38, 2014.

[17] D. Oliveira, H. Rocha, H. Yang, D. Ellis, S. Dommaraju, M. Muradoglu, D. Weir, A. Soliman, T. Lin és N. Ebner, „Dissecting Spear Phishing Emails for Older vs Young,” *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems,* 2017.

[18] T. Lin, D. E. Capecci, D. M. Ellis, H. A. Rocha, S. Dommaraju, D. S. Oliveira és N. C. Ebner, „Susceptibility to Spear-Phishing Emails,” *ACM Transactions on Computer-Human Interaction,* pp. 1-28, 2019.

[19] Biztonságportál, „Milliárdos károkat okoznak a levelezgető csalók,” [Online]. Available: https://biztonsagportal.hu/milliardos-karokat-okoznak-a-levelezgeto-csalok.html. [Hozzáférés dátuma: 14 05 2021].

[20] C. Joshi, „QR Codes in E-commerce: 7 ways Amazon is getting it right!,” 2019. [Online]. Available: https://blog.beaconstac.com/2019/04/qr-codes-in-e-commerce-ways-amazon-is-getting-it-right/. [Hozzáférés dátuma: 14 05 2021].

[21] T. Vidas, E. Owusu, S. Wang, C. Zeng, L. F. Cranor és N. Christin, QRishing: The Susceptibility of Smartphone Users to QR Code Phishing Attacks, 2013.

[22] M. Hasan, N. Prajapati és S. Vohara, „Case Study On Social Engineering Techniques for Persuasion,” *International journal on applications of graph theory in wireless ad hoc networks and sensor networks 2.2,* pp. 17-23, 2010.

[23] N. S. N. K. Intézet, „Riasztás Csomagküldő szolgáltatók nevével visszaélő, káros kód terjesztéssel összefüggő SMS üzenetekkel kapcsolatban,” 2021. [Online]. Available: https://nki.gov.hu/figyelmeztetesek/riasztas/riasztas-csomagkuldo-szolgaltatok-nevevel-visszaelo-malware-terjesztessel-osszefuggo-sms-uzenetekkel-kapcsolatban/. [Hozzáférés dátuma: 14 05 2021].

[24] N. S. N. K. Intézet, „Rendkívüli tájékoztató Csomagküldő szolgáltatók nevével visszaélő, malware terjesztéssel összefüggő SMS üzenetekkel kapcsolatban FluBot blokkolása / eltávolítása,” [Online]. Available: https://nki.gov.hu/figyelmeztetesek/tajekoztatas/rendkivuli-tajekoztato-sms-uzenetek-utjan-terjesztett-flubot-kartevovel-kapcsolatban/?fbclid=IwAR1yR7iZasJHeJ-1NHY8gdBI1I2XLLUZ5sj0WR1B0OqrnSmKi4v5izAENvo. [Hozzáférés dátuma: 14 05 2021].

[25] NKI, „NKI tájékoztató az adathalászatról," [Online]. Available: https://nki.gov.hu/wp-content/uploads/2019/03/NKI-t%C3%A1j%C3%A9koztat%C3%B3-az-adathal%C3%A1szatr%C3%B3l-2018.09.13..pdf. [Hozzáférés dátuma: 14 05 2021].

[26] Google és Harris Poll, „Online Security Survey," 2019. [Online]. Available: https://services.google.com/fh/files/blogs/google_security_infographic.pdf. [Hozzáférés dátuma: 14 05 2021].

[27] FBI, „Internet Crite Report 2018," [Online]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2018_IC3Report.pdf.

[28] CISA, „Stop think connect older american resources," [Online]. Available: https://www.cisa.gov/publication/stopthinkconnect-older-american-resources. [Hozzáférés dátuma: 14 05 2021].

[29] N. Gelernter és A. Herzberg, „Tell Me About Yourself: The Malicious CAPTCHA Attack," 2016.

[30] Sophos, „Cyberattacks and Seniors – How to Protect Vulnerable Users Online," [Online]. Available: https://home.sophos.com/en-us/security-news/2020/senior-citizen-cyber-attack.aspx. [Hozzáférés dátuma: 14 05 2021].

[31] K. Skiba, „Older Americans Hit Hard by Financial Fraud," 2019. [Online]. Available: https://www.aarp.org/money/scams-fraud/info-2019/cfpb-report-financial-elder-abuse.html. [Hozzáférés dátuma: 14 05 2021].

[32] S. Sjouwerman, „KnowBe4 2019 Security Threats and Trends Report – October 2019," [Online]. Available: https://blog.knowbe4.com/knowbe4-2019-security-threats-and-trends-report-october-2019. [Hozzáférés dátuma: 15 05 2021].

[33] Kaspersky, „Spam and phishing in Q1 2019," [Online]. Available: https://securelist.com/spam-and-phishing-in-q1-2019/90795/. [Hozzáférés dátuma: 15 05 2021].

[34] pingdom, „The incredible growth of the Internet since 2000," [Online]. Available: https://www.pingdom.com/blog/incredible-growth-of-the-internet-since-2000/. [Hozzáférés dátuma: 15 05 2021].

[35] M. Rosenthal, „Must-Know Phishing Statistics: Updated 2021," [Online]. Available: https://www.tessian.com/blog/phishing-statistics-2020/. [Hozzáférés dátuma: 15 05 2021].

[36] F. Koczka, „Az adathalászatról," [Online]. Available: https://koczka.com/informaciobiztonsag/_static/adathalaszat/adathalaszat.html. [Hozzáférés dátuma: 15 05 2021].

[37] cloudflare, „What is a phishing attack?," [Online]. Available: https://www.cloudflare.com/es-es/learning/access-management/phishing-attack/. [Hozzáférés dátuma: 15 05 2021].

[38] statista, „Chrome Most Vulnerable Browser," 2017. [Online]. Available: https://www.statista.com/chart/7451/chrome-most-vulnerable-browser/. [Hozzáférés dátuma: 15 05 2021].

[39] S. Narang, „CVE-2021-21148: Google Chrome Heap Buffer Overflow Vulnerability Exploited in the Wild," [Online]. Available: https://www.tenable.com/blog/cve-2021-21148-google-chrome-heap-buffer-overflow-vulnerability-exploited-in-the-wild. [Hozzáférés dátuma: 15 05 2021].

[40] E. Blizzard. [Online]. Available: https://eu.battle.net/login/en/. [Hozzáférés dátuma: 15 05 2021].

[41] [Online]. Available: http://forum.warmane.com/showthread.php?t=385662. [Hozzáférés dátuma: 15 05 2021].

[42] ksh, „KSH HETI MONITOR," [Online]. Available: https://www.ksh.hu/heti-monitor/kereskedelem.html. [Hozzáférés dátuma: 15 05 2021].

[43] Freenom. [Online]. Available: https://my.freenom.com/clientarea.php. [Hozzáférés dátuma: 08 12 2021].

[44] Hostinger, „How to Install Free SSL From Let's Encrypt on Shared Hosting," [Online]. Available: https://www.hostinger.com/tutorials/ssl/how-to-install-free-ssl-from-lets-encypt-on-shared-hosting. [Hozzáférés dátuma: 08 12 2021].

[45] Waybackmachinedownloader. [Online]. Available: https://www.waybackmachinedownloader.com/en/. [Hozzáférés dátuma: 08 12 2021].

[46] 000webhost, „Free Web Hosting," [Online]. Available: https://www.000webhost.com. [Hozzáférés dátuma: 08 12 2021].

[47] Hostinger. [Online]. Available: https://www.hostinger.hu. [Hozzáférés dátuma: 08 12 2021].

[48] Moodle. [Online]. Available: https://elearning.uni-obuda.hu. [Hozzáférés dátuma: 08 12 2021].

[49] SSL For Free. [Online]. Available: https://manage.sslforfree.com/login. [Hozzáférés dátuma: 08 12 2021].

[50] J. Alexander, „Why does a minimum password length of 6 characters exist," [Online]. Available: https://www.quora.com/Why-does-a-minimum-password-length-of-6-characters-exist. [Hozzáférés dátuma: 08 12 2021].

[51] PHP. [Online]. Available: https://www.php.net/manual/en/mysqli-stmt.bind-param.php?fbclid=IwAR2EAReb0G4VYWcvpltnoo-bNkqJ6Fz9O_9o7u01eLCiNVS7b2IbQpH6izA. [Hozzáférés dátuma: 13 12 2021].

[52] Wikipedia, „10,000 most common passwords," [Online]. Available: https://en.wikipedia.org/wiki/Wikipedia:10,000_most_common_passwords. [Hozzáférés dátuma: 08 12 2021].

[53] Dan Piazza, „NIST Password Guilelines in 2020.” [Online]. Available: https://stealthbits.com/blog/nist-password-guidelines/. [Hozzáférés dátuma: 10 12 2021].

[54] BSI, „BSI insights for strengthening your passwords on World Password Day.” [Online]. Available: https://www.bsigroup.com/en-GB/about-bsi/media-centre/press-releases/2020/may/bsi-insights-for-strengthening-your-passwords-on-world-password-day/. [Hozzáférés dátuma: 08 12 2021].

16. Ábrajegyzék

17. Mellékletek

[a] weboldalt tartalmazó mappa

[b] processor.php

[c] teszt.txt

[d] top_1k_pw.txt

[e] top10000password.txt

[f] weboldal_bemutato.mkv