CTI Jelentés

Adathalászat

- a leghatékonyabb kiberfegyver

1996
NEMZETBIZTONSÁGI SZAKSZOLGÁLAT
Fortes fortuna adiuvat

NEMZETI
KIBERVÉDELMI INTÉZET

Tartalomjegyzék

Bevezetés 3

Egy kis "adathalász történelem" 5

Az adathalászat főbb típusai 11

- Tömeges e-mail adathalászat 11
- Szigonyozás (Spearphishing) 12
- Bálnavadászat (Whaling) 13
- Klónozott adathalászat 14
- SMS adathalászat (Smishing) 14
- Hangalapú adathalászat (Vishing) 15

Adathalász technikák 16

- Link manipuláció 16
- Pszichológiai manipuláció)Social engineering) 17

Új trendek 18

Hazai helyzetkép 25

Az NBSZ NKI javaslatai az adathalász támadások elkerülése érdekében 26

Bevezetés

Napjaink legkomolyabb információbiztonsági fenyegetései közé tartozik az adathalász (phishing) tevékenység. Még a legszofisztikáltabb, legösszetettebb kibertámadás, – ami informatikai rendszerek, hálózatok összeomlásához, vagy a szervezetek legféltettebb belső információinak kiszivárgásához is vezet – a legtöbb esetben egyetlen e-maillel kezdődik. Kijelenthetjük, hogy kiberbiztonság, sem szervezeti, sem személyes szinten nem létezik anélkül, hogy az adathalászat veszélyeit ne értenénk meg, és ezzel szemben ne hoznánk védelmi intézkedéseket.

Ez a fajta csalásmód évről évre növekvő tendenciát mutat. A Cisco 2021-es jelentése szerint[1] az összes adatszivárgási incidens 90%-a adathalász támadásokhoz kapcsolódik. A Forbes kutatása során egyenesen arra jutott, hogy az összes kiberincidens 80%-a adathalász támadáshoz köthető.

1 https://learn-umbrella.cisco.com/ebook-library/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

Jelen dokumentum célja, hogy ismertesse az adathalászat veszélyeit, főbb típusait, leggyakoribb felhasználási módjait, valamint hogy bemutassa azt, hogy hogyan érdemes az adathalászat ellen védekezni. Amennyiben bizonyos jellegzetességekre odafigyelünk, lényegesen minimalizálhatjuk annak az esélyét, hogy egy ilyen típusú támadás áldozataivá váljunk. Az adathalászat manapság már nem ismer határokat, bármilyen szektorban megjelenhet, ahol direkt vagy indirekt módon célt szolgáltat anyagi vagy más jellegű haszonszerzés reményében, akár egy későbbi támadáshoz felhasználva a megszerzett információkat. Gyakran célozza a banki és pénzügyi szférát, jellemzően speciálisan egy-egy szervezet vagy cég ellen indított adathalász kampány során, azonban komoly fenyegetettségnek vannak kitéve a magánszemélyek is a mindennapos internethasználat során.

A phishing kifejezés a „password" és a „fishing" szavakból tevődik össze, amely annyit jelent, mint jelszavakra halászni. A támadókat első sorban az érzékeny adatok megszerzése motiválja, például a felhasználók hitelkártya adatai vagy bizonyos platformokra történő bejelentkezési adatai. Az adathalászat azért népszerű a kiberbűnözők körében, mert lehetővé teszi számukra, hogy pénzügyi és személyes információkat lopjanak el anélkül, hogy át kellene törniük a számítógép vagy a hálózat biztonsági védelmét.

Az adathalászathoz a támadók változatos módszereket használnak. Ilyen például az e-mail és weboldal hamisítások, ezzel próbálják rávenni a felhasználókat a bizalmas adatok (jelszavak, hozzáférési adatok, bankkártyaadatok, speciális céges adatok) kiszivárogtatására, amelyet a későbbiekben a támadó felhasználhat.

Egy kis "adathalász történelem"

Számtalan híres, vagy pontosabban szólva hírhedt esetről tudunk, amit adathalász technikával hajtottak végre. Az eddigi egyik legnagyobb csalást egy litván férfi, Evaldas Rimas Rimasauskaski követte el 2013 és 2015 között, amikor a világ két legnagyobb techóriásától, a Google-től és a Facebooktól 100 millió dollárt csalt ki hamis számlákkal. Rimasauskas észrevette, hogy mindkét vállalat a tajvani székhelyű Quanta Computerrel üzletel, ezért alapított egy olyan céget, amely ennek a szervezetnek adta ki magát. A csalás során Rimasauskas és társai hamis e-mail fiókok segítségével olyan hamis számlákat tartalmazó adathalász e-maileket küldtek a Facebook és a Google munkatársainak, amelyek úgy tűntek, mintha a valódi Quanta tajvani alkalmazottaitól származnának. Az ügy eszkalációja során több mint 100 millió dollárt fizettek ki a hamis cég bankszámláira. A csalásra idővel fény derült, és Rimasauskast letartóztatták, azonban a kicsalt pénznek körülbelül csak a felét sikerült visszaszereznie a tech vállalatoknak.

1990

Az adathalászat kifejezést Khan C. Smith alkotta meg az 1990-as évek közepén, aki egy hírhedt spammer volt [2]. Egy 1995. szeptember 8-án megjelent cikkben említik először a módszert, amellyel tömegesen próbálták meg a felhasználók adatait ellopni [3].

Az 1990-es évek elején és közepén az egyetlen csatlakozási lehetőség a világhálóra a díjköteles betárcsázós internet volt. Egy alternatív megoldást nyújtott az AOL (American Online) floppylemezen keresztül történő csatlakozás, amely harmincnapos ingyenes próbaidőszakot jelentett.

2 https://www.bizjournals.com/atlanta/stories/2002/07/22/story4.html?page=all

3 https://simson.net/clips/1995/95.SJMN.AOL_Hackers.html

Néhányan megtalálták a módját, hogy úgy tűnjön, mintha ők lennének az AOL rendszergazdái, és hamis felhasználóneveket használva szereztek bejelentkezési adatokat, hogy továbbra is ingyenesen használhassák az internetet.

Az AOL-on történő adathalászat a warez (software szóból ered, jelentése: jogvédett tartalmak illegális terjesztése) csoportokkal hozható összefüggésbe. Az AOL moderátorai folyamatosan szűrték és keresték azokat a kifejezéseket, amelyek illegális tevékenységekre utaltak. A felhasználók tisztában voltak azzal, hogy keresik őket, ezért a „<><" szimbólummal helyettesítettek minden olyan kifejezést, amelyre az AOL munkatársai szűrhettek. Azért erre esett a választásuk, mert ez a HTML-ben a leggyakrabban használt szimbólum, és a szűrések hatástalannak bizonyultak ezzel szemben. Mivel a szimbólum hasonlít egy halra, ezért magát az adathalász folyamatot a „Phising" kifejezéssel illették.

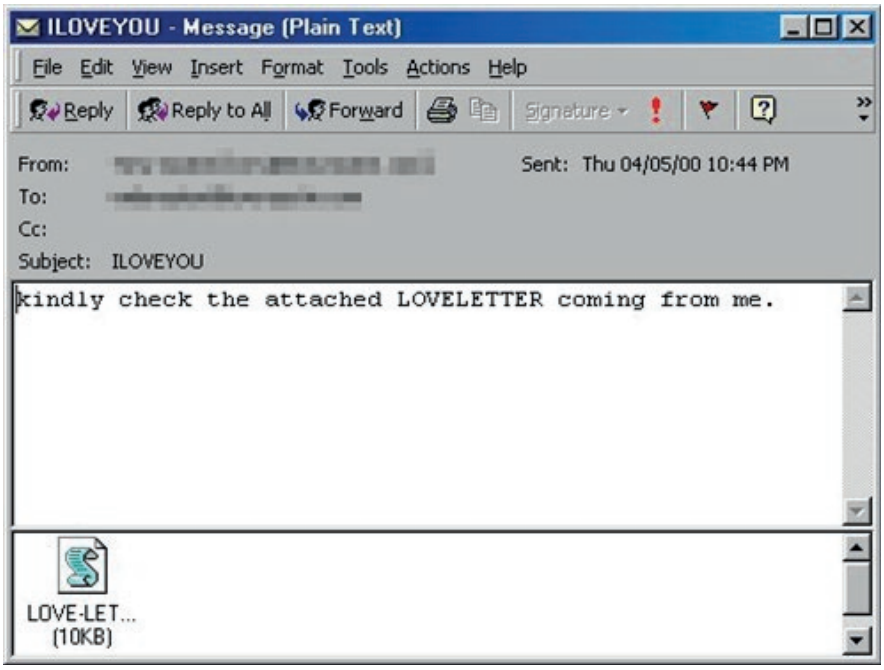
1995 márciusban kezdett terjedni az AOHell elnevezésű rosszindulatú program, amely az American Online felhasználóitól próbált érzékeny adatokat kicsalni [4].

2000

2000. május 4-én a került ki az internetre a Fülöp szigetekről induló Love Bug nevű féreg, és világszerte kaptak az emberek „ILOVEYOU" tárggyal ellátott üzeneteket. A levél szövege a következő volt: „Kérem, nézze meg a mellékelt, tőlem érkező LOVELETTER-t".

A rutintalan és kíváncsi felhasználók a mellékletet letöltve egy ártalmatlannak tűnő .txt fájlt nyitottak meg, amellyel egy kártevő került a gépre. A féreg felülírta a képfájlokat, és elküldte önmaga másolatát a felhasználó Outlook címjegyzékében szereplő összes kapcsolatának.

4 https://web.archive.org/web/20051214053144/http:/wired-vig.wired.com/news/technology/0%2C1282%2C9932%2C00.html



ILOVEYOU üzenet káros csatolmánnyal

Ez volt az első precedens arra, hogy egy spam önmagát küldte tovább. Egy jól megtervezett, az emberi pszichológiát és a technikai hiányosságokat kihasználó vírussal a rosszindulatú programok hatalmas számú áldozatot tudnak szedni. A féreg összesen 45 millió Windows PC-t támadott meg.

2004

Egy másik mérföldkő volt egy 2004-es bírósági kereset egy tinédzser ellen, aki egy internetszolgáltató weboldalát hamisította meg, hogy hozzáférjen a felhasználók banki adataihoz.

Az évtizedek során a csalók egyre precízebb módszereket és technikákat dolgoztak ki, az áldozatok száma pedig évről évre rohamosan nő. Az adathalászatot hivatalosan is a feketepiac teljesen szervezett részeként ismerik el.

2013

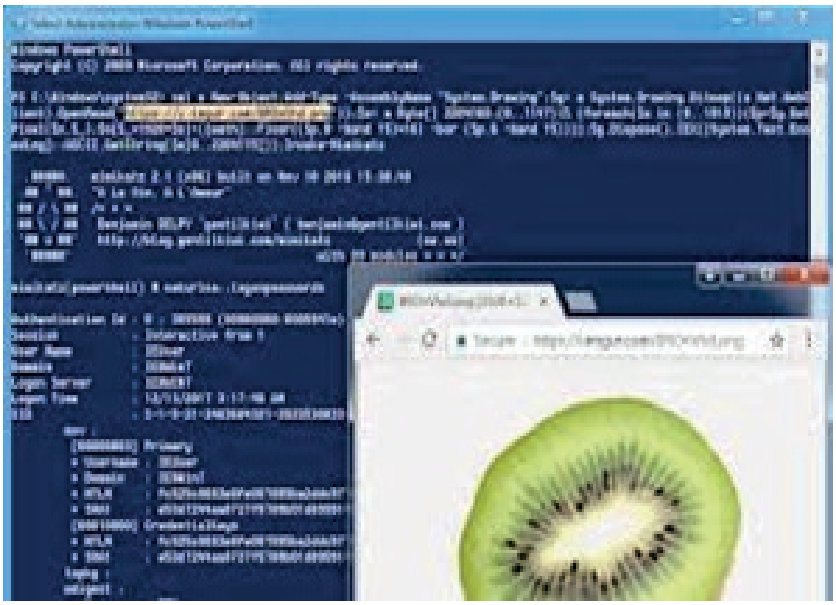
2013 szeptemberében a Cryptolocker zsarolóprogram 250 000 PC-t fertőzött meg, ezzel ez volt az első kriptográfiai kártevő, amely egy kompromittált weboldalról történő letöltéssel, és az áldozatoknak küldött két adathalász e-maillel terjedt. Az első e-mail egy becsomagolt fájlt tartalmazott, amely egy ügyfélpanasznak tűnt, és kifejezetten vállalkozásoknak szólt, a másik pedig egy rosszindulatú linket tartalmazott, amely egy csekk kiegyenlítési problémáról szóló üzenetet tartalmazott, és az átlagfelhasználókat célozta meg. A kattintás után a Cryptolocker zárolta a számítógépen lévő fájlokat, és váltságdíjat követelt a fájlok dekódolásához szükséges kulcsért cserébe.

2017

Az adathalászok 2017-től kezdődően egyre gyakrabban alkalmazzák a HTTPS-t a weblapjaikon, amely hamis biztonságérzetet nyújthat önmagában, mivel ez csak annyit jelent, hogy a szerver és a felhasználó böngészője közötti forgalom titkosított és védett a lehallgatás ellen. Természetesen semmit nem ér, ha egy adathalász oldal is ezt a protokollt használja.

2018

A 2018-as téli olimpiához kapcsolódó szervezeteket célzó adathalász kampány volt az első, amely az Invoke-PSImage nevű PowerShell eszközt használta, amely lehetővé tette a támadók számára, hogy rosszindulatú szkripteket rejtsenek el a képfájlokban, és később közvetlenül a memóriából futtassák azokat. Ezt a technikát a legtöbb esetben a hagyományos vírusirtó megoldások nem vették észre.



Kép forrása: pentesttools.net

2018-ban a kutatók felfedeznek egy új generációs adathalász szolgáltatást, amely könnyen elérhető bárki számára a Dark Weben, és aki letölti, könnyedén készíthet olyan e-maileket, amelyekkel hatékonyan képes megtéveszteni és átirányítani az embereket olyan adathalász webhelyekre, amelyek precízen másolják le a kívánt cég honlapját, és ültetik át az arculati elemeit a saját, csaló weboldalukba.

2019

A szállítói e-mail kompromittálás 2019-ben új támadástípusként jelent meg. A kiberbűnözők hozzáférést szereznek egy vállalat e-mail fiókjaihoz, amelyekkel az adott vállalat ügyfeleit célozzák meg. A támadások a globális ellátási lánccal rendelkező szervezetekre összpontosítanak, és megpróbálják a beszállító ügyfeleit hamis számlák kifizetésére rávenni. Ez a támadástípus 2019-ben világszerte legalább 500 szervezetet érintett.

2020

2020 elején jelentek meg a Covid-19-hez kapcsolódó adathalász e-mailek. A népszerű témák között szerepelnek a hamis CDC (Centers for Disease Control and Prevention - Betegségellenőrzési és Megelőzési Központ) figyelmeztetések, otthoni munkavégzés, Netflix csalások és a karanténból való kilépésért kiszabott bírságok. A világ számos országát érintik az ilyen típusú támadások.

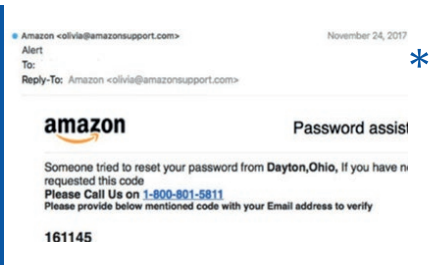
A Covid-19-hez kapcsolódó kibertámadásokról bővebben Intézetünk a „Kibertámadások a koronavírus árnyékában”[5] című jelentésében olvashat.

A támadóknak az adathalászatról való gondolkodásában bekövetkezett ilyen előrelépések a végpontok megfertőzésének vagy a hitelesítő adatok ellopásának megkönnyítése érdekében feltétlenül szükségessé teszik, hogy a szervezetek többé ne tekintsék biztonsági megoldásaikat az egyetlen védelmi vonalnak, ezért elengedhetetlen, a felhasználók tudását is naprakészen tartani a biztonságtudatosság terén.

5 https://nki.gov.hu/it-biztonsag/elemzesek/kibertamadasok-a-koronavirus-arnyekaban/

Az adathalászat főbb típusai

Tömeges e-mail adathalászat



*

*Egy olyan adathalász e-mail, amely tartalmazza az igazi vállalat nevét

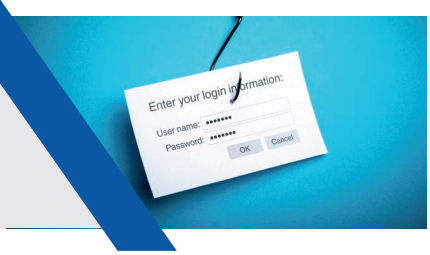
Az adathalászat leggyakoribb formája. A tényleges adathalászat azután kezdődik meg, miután a bűnözők különféle módszerekkel nagy mennyiségű valós e-mail címhez jutottak. Minden típusnál fontos a hatékonyság maximalizálása, de ebben az esetben, mivel óriási mennyiségű címzettnek küldik ki a leveleket, alacsonyabb hatékonyság is hatalmas sikerhez vezethet a támadók számára.

Ezeknek az e-maileknek a tartalma rendkívül különböző lehet, főként az áldozatoktól függ, hogy mi áll a levélben. Gyors sikert a támadók akkor érhetnek el, ha az áldozatok minél gyorsabban reagálnak a megkeresésre, ezért általában a levél tartalma nagyon sokszor sürgető (pl. mielőbbi jelszóváltoztatásra való buzdítás egy megadott linken, vagy mielőbbi vásárlás a csökkenő készletszám miatt). Szinte biztos, hogy ilyen adathalász levelekkel már mindannyian találkoztunk.

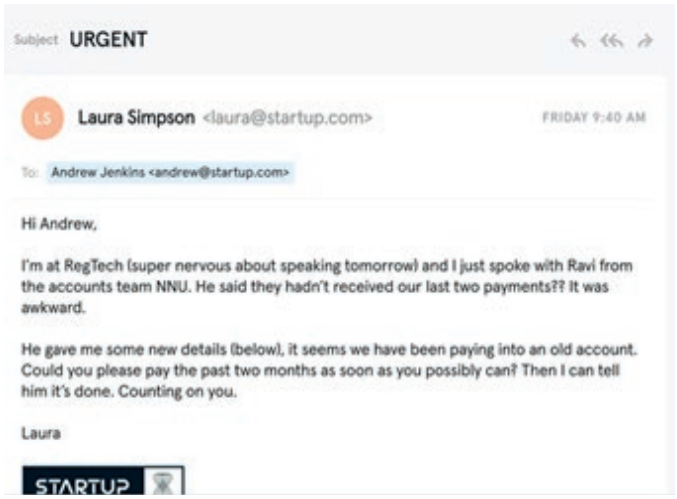
Egyik leggyakoribb célpontok a banki ügyfelek, de célozhatnak közműszolgáltatókat, telekommunikációs vállalatokat, felhőszolgáltatókat, internetszolgáltatókat, és minden olyan szolgáltatót, amely több tízezer, százezer vagy akár több milliós ügyfélkörrel rendelkezik.

A kicsalt hitelesítő adatokkal képesek közvetlenül pénzt lopni az áldozatoktól, viszont előfordul az is, hogy nem elsődleges cél az anyagi haszonszerzés, mivel a fenyegetési szereplők gyakran használják fel a megszerzett személyes adatokat későbbi támadásokhoz. Ilyen lehet például különféle kémprogramok telepítése, vagy a vállalaton belül más, magasabb beosztásban lévő személy megtámadása.

Szigonyozás (Spearphishing)



Ugyancsak gyakori módszer, azonban számát tekintve elenyésző a tömeges e-mailes adathalászathoz képest. Ezzel a módszerrel konkrét személyeket vagy vállalatokat (osztályokat, igazgatóságokat stb.) céloznak személyre szabott e-mailekkel. Ahhoz, hogy ez a technika hatékony legyen, nagy figyelmet kell fordítani az adott vállalat sajátosságaira, mint például a domainekre, megszólításra, levél aláírásra, nyelvtani helyességre és szakmai kifejezésekre.


Subject URGENT

Laura Simpson <laura@startup.com> FRIDAY 9:40 AM

To: Andrew Jenkins <andrew@startup.com>

Hi Andrew,

I'm at RegTech (super nervous about speaking tomorrow) and I just spoke with Ravi from the accounts team NNU. He said they hadn't received our last two payments?? It was awkward.

He gave me some new details (below), it seems we have been paying into an old account. Could you please pay the past two months as soon as you possibly can? Then I can tell him it's done. Counting on you.

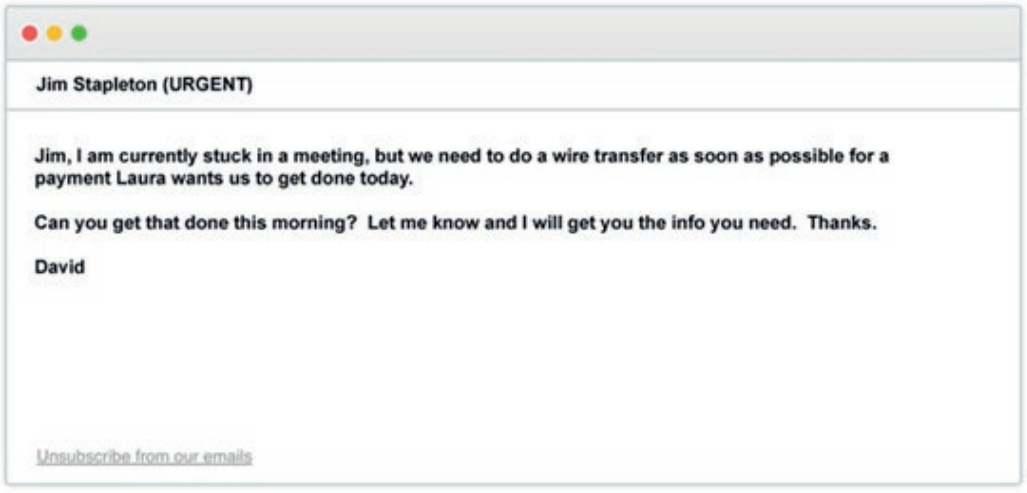
Laura

STARTUP

Az e-mail kifejezetten egy személynek szól, tehát specifikusabb, mint egy hagyományos adathalász levél

Bálnavadászat (Whaling)

A bálnavadászat alapjaiban hasonlít a szigonyozásra, annyi különbséggel, hogy itt már a legmagasabb beosztásban lévő személyeket célozzák, nem csupán egy alkalmazottat. Az e-mail úgy kerül megszerkesztésre, mintha egy másik magas rangú, befolyásos személytől érkezett volna a megkeresés. A támadók ezt a módszert előszeretettel használják pszichológiai manipulációval vegyítve, ugyanis egy munkavállaló egy hierarchikus rendszerben egy magasabb beosztásban lévő kollegától nem szívesen utasít vissza egy kérést. A támadók tudják, hogy a vezetők és a magas rangú alkalmazottak kiterjedt biztonságtudatossági képzésekben részesülhettek, ami arra készteti őket, hogy kifinomultabb és célzottabb támadásokat hajtsanak végre.



Jim Stapleton (URGENT)

Jim, I am currently stuck in a meeting, but we need to do a wire transfer as soon as possible for a payment Laura wants us to get done today.

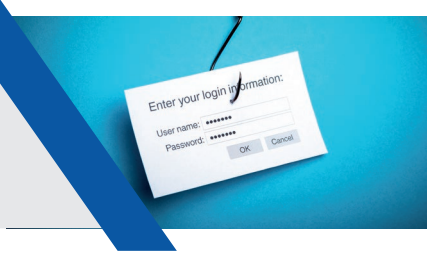
Can you get that done this morning? Let me know and I will get you the info you need. Thanks.

David

Unsubscribe from our emails

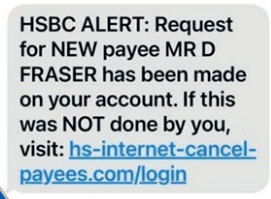
Specifikus, akárcsak a szigonyozás, azonban magasabb beosztású személyt céloz ez az e-mail

Klónozott adathalászat



A klónozott adathalász támadás során a támadó a célpontja egy korábbi e-mailjének a mellékletét vagy linkjét használja fel, hogy zsarolóprogrammal, vírussal vagy kémprogrammal helyettesítse azt. Ezek az e-mailek úgy tűnhetnek, mintha kollégáktól vagy ismerősöktől érkeztek volna, és úgy néznek ki, mintha egy korábbi üzenet újra küldése lenne. A hackerek az újraküldést az eredeti verzió frissítésének megemlítésével próbálhatják megmagyarázni.

SMS adathalászat (Smishing)



Az úgynevezett smishing az SMS-ek útján történő adathalászat. Az áldozat egy szöveges üzenetet kap, amely sokszor úgy tűnik, hogy megbízható forrásból származik (például egy bank vagy futárszolgálat), és célja, hogy személyes adatokat kérjen tőle. Ezek az üzenetek gyakran tartalmaznak egy linket (általában egy rövidített URL-t), és más adathalász támadásokhoz hasonlóan valamilyen sürgős cselekvésre ösztönzik a címzettet, hogy például azt állítva, hogy átvehetnek valamilyen nyereményt, adóvisszatérítéssel élhetnek vagy azt állítják, hogy csomagjuk érkezik, amit nyomon követhetnek.

Hangalapú adathalászat (Vishing)

A vishing a telefonhíváson keresztül történő adathalászat, amelyek általában a VoIP (Voice over IP) technológiát használják. A támadás során az áldozata egy telefonhívást (vagy hangüzenetet) kap egy csalótól, aki megbízható személynek adja ki magát, és személyes adatokat, például hitelkártya- vagy bejelentkezési adatokat próbál kicsikarni belőle.

A módszer alapvetően azt használja ki, hogy a felhasználók könnyebben dőlnek be annak — főleg az idősebb korosztály —, ha egy valósnak tűnő személy keresi meg őket, mintha egy e-mailt kaptak volna ugyanazzal a tartalommal. A fenyegetési szereplők az ilyen támadások során olyan fejlett technikákat alkalmaznak, mint például a hívószám-hamisítás, amely során úgy tűnik, hogy a hívás egy hivatalos számról érkezik, vagy a szintetikus beszédgenerátor. Gyakran tömegesen, nagy számú embert bombáznak megkeresésekkel, így növelve a sikerességüket és hatékonyságukat.

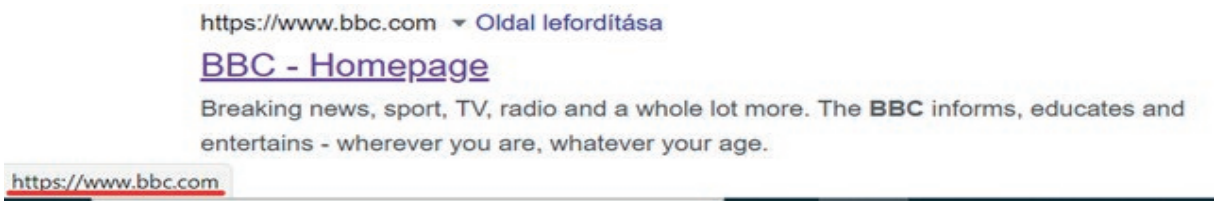
Az adathalászat főbb típusai

Alapvetően minden adathalász támadás az áldozat megtévesztésén alapszik, hogy a támadók értékes információkat tudjanak tőle kinyerni, és azt fel tudják használni a későbbiekben. Céljuk, hogy valamilyen úton módon rábírják az áldozatot, hogy kattintsanak az általuk megadott linkre, vagy válaszüzenetben (legyen az e-mail, hangalapú megkeresés) megadják a számukra szükséges személyes információkat. Az említett SMS-es és e-mailes megkeresésen felül belefuthatunk adathalász próbálkozásokba a közösségi felületeken, és akár az olyan különféle játékokban is, ahol direkt kommunikáció lehetséges a felhasználók között.

Link manipuláció

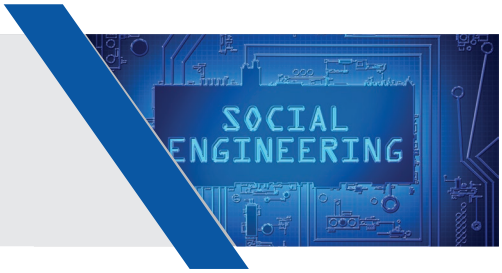
A link manipuláció az a technika, amelynek során az adathalász egy rosszindulatú weboldalra mutató webes hivatkozást küld a célpontjának. Amikor a felhasználó rákattint a megtévesztő linkre, a linkben említett weboldal helyett az adathalász weboldal nyílik meg, ahol a beviteli mezőkbe begépelt adatokat a csalók kapják meg. A hatékonyabb megtévesztés végett a bűnözők előszeretettel használnak olyan aldomaineket, amelyekre ha a felhasználó rápillant, nagy eséllyel nem tűnik fel neki, hogy az nem egy legitim cím.

Ha számítógépet használunk, és éppen egy gyanús linket nyitnánk meg, érdemes rávinni az egeret kattintás előtt, és az állapotsorra tekinteni, így tudhatjuk meg, hogy valójában milyen webhelyre is vezet a link. A legtöbb adathalász próbálkozás már ezzel a módszerrel kiszűrhető.



A link fölé húzva az egeret az állapotsorban látszódik az oldal ahová a link vezet

Pszichológiai manipuláció (Social engineering)

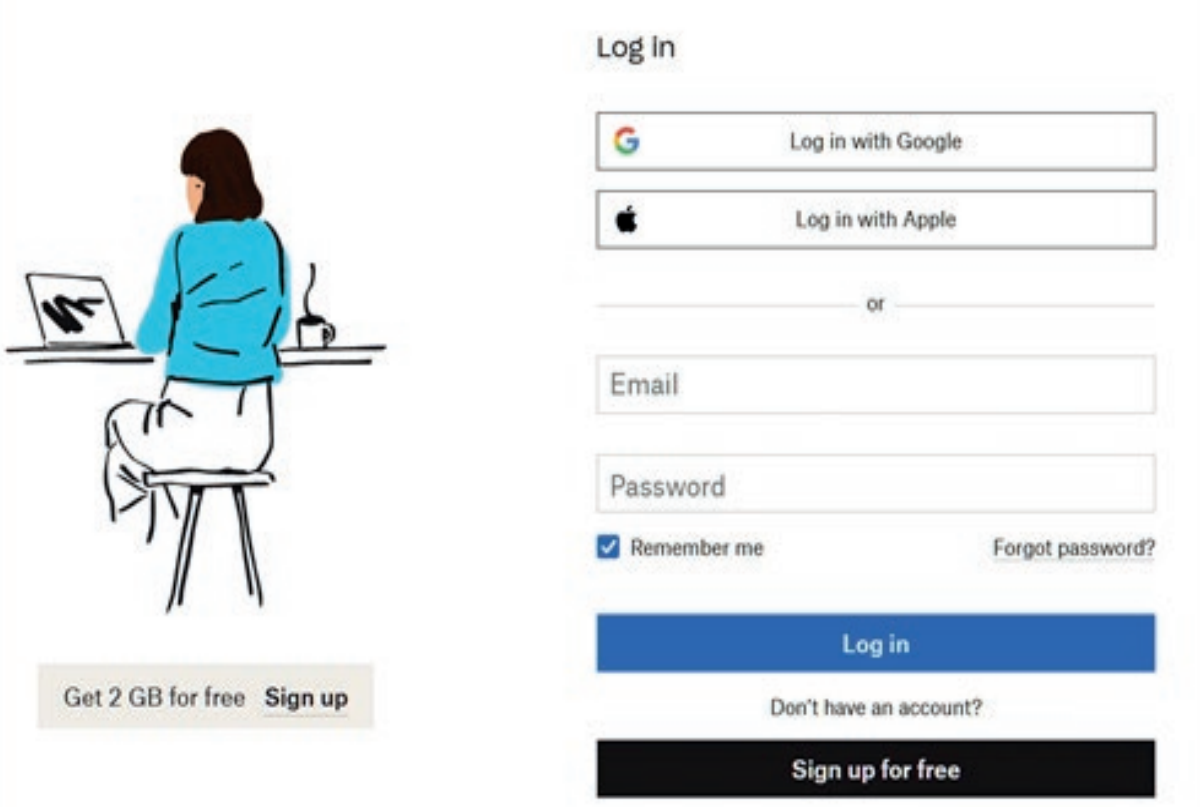


A pszichológiai manipuláció során a kiberbűnöző elsősorban nem a technikai hiányosságokra alapozva indítja a támadását, hanem az emberi hiszékenységet, mohóságot, félelmet és a segítőkészséget célozza. Célja, hogy a felhasználók biztonsági hibákat kövessenek el, és érzékeny információkat adjanak ki magukról vagy a vállalatukról. Az elkövető először információt gyűjt a kiszemelt áldozatról, hogy összegyűjtse a támadáshoz szükséges háttérinformációkat, például a gyenge biztonsági protokollokat. Ezután a támadó megpróbálja elnyerni az áldozata bizalmát, és arra próbálja ösztönözni, hogy szegje meg a biztonsági gyakorlatokat, például szolgáltasson érzékeny információkat, vagy biztosítson hozzáférést a kritikus erőforrásokhoz. Mivel a social engineering a szoftverek és operációs rendszerek sebezhetőségei helyett az emberi hibákra támaszkodik, ezért az így elkövetett hibák sokkal kevésbé kiszámíthatók, nehezebb azonosítani és meghiúsítani őket.

Új trendek

Ahogy a felhasználók egyre tudatosabbak, és a különböző szoftverek egyre komolyabb szűrőtechnikákat alkalmaznak, úgy fejlődnek az adathalász technológiák is.

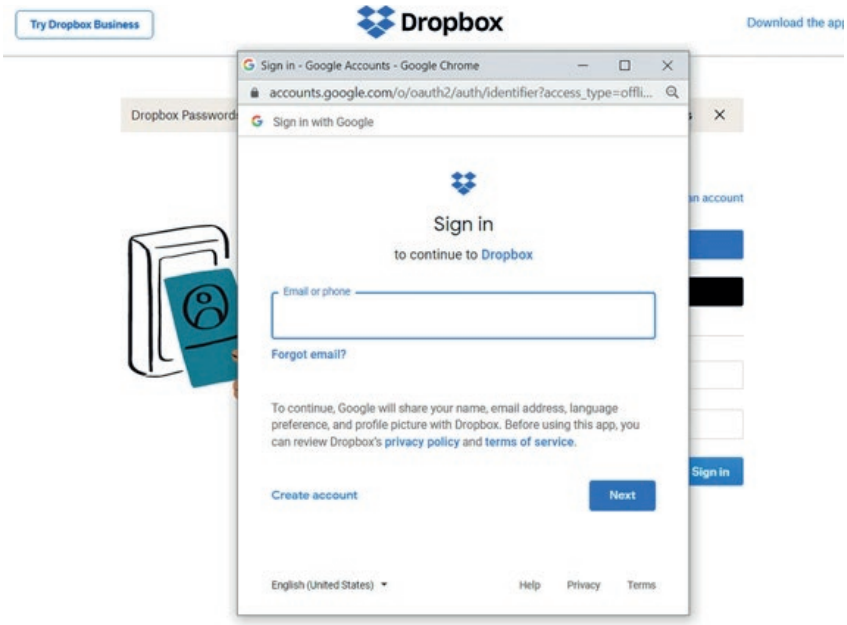
Egy nemrég felfedezett újfajta adathalász[6] eszközkészlet például lehetővé teszi, hogy bárki hamis Chrome böngészőablakokat hozzon létre. Manapság gyakran lehet látni, hogy a különféle weboldalakra a Facebook, Google, Microsoft, Apple, Twitter vagy akár a Steam felhasználói fiókunkkal is bejelentkezhetünk. A DropBox bejelentkezési űrlapja például lehetővé teszi a bejelentkezést Apple- vagy Google-fiókkal, ahogy az alábbiakban látható:



Dropbox bejelentkezési felület

6 https://www.bleepingcomputer.com/news/security/new-phishing-toolkit-lets-anyone-create-fake-chrome-browser-windows/

A Google vagy Apple bejelentkezés gombokra kattintva egy SSO (Single Sign On) böngészőablak jelenik meg, amely az áldozatot a hitelesítő adatok megadására, és a fiókkal való bejelentkezésre szólítja fel. Ezek az ablakok szándékosan le vannak csupaszítva, kizárólag a bejelentkezési űrlap és egy címsor jelenik meg, amely a bejelentkezési űrlap URL-jét mutatja.

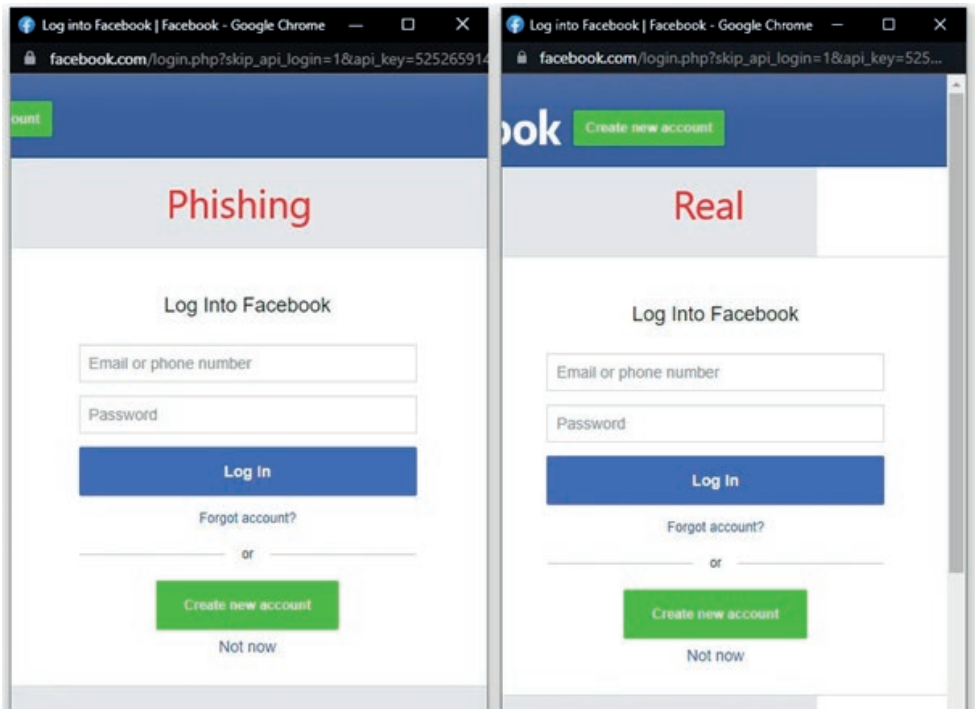


Google-lel való bejelentkezési ablak

Bár ezekben az SSO ablakokban ez a címsor ki van kapcsolva, a megjelenített URL segítségével továbbra is ellenőrizhető, hogy egy legitim google.com domainnel történik-e a bejelentkezés. Ez az URL tovább növeli az űrlap megbízhatóságát, és kényelmesebbé teszi a bejelentkezési adatok megadását.

Itt lép a képbe egy új "böngésző a böngészőben támadás" (BitB – Browser in the Browser), amely egy előre elkészített valósághű sablont és egyéni URL címet használ, és amelyet adathalász támadásokra használnak. A BitB[7] sablonokat mr.d0x biztonsági kutató készítette, és a GitHubon el is érhetők.

7 https://mrd0x.com/browser-in-the-browser-phishing-attack/



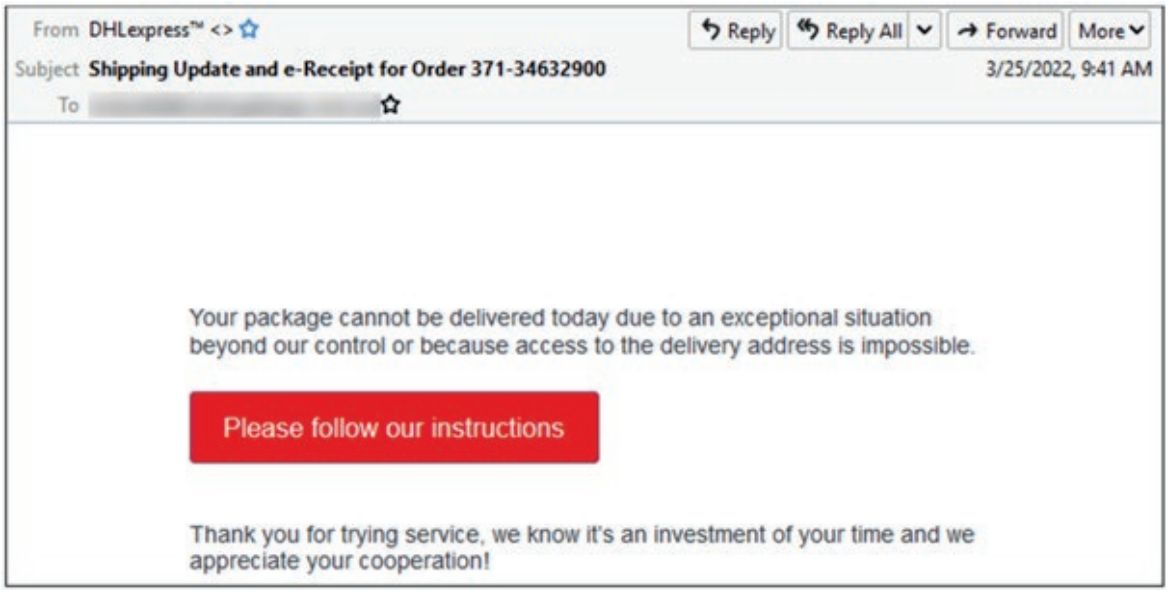
Adathalász és valós bejelentkezési felület a Facebookra

Kuba Gretzky, az Evilginx adathalász eszközkészlet készítője tesztelte az új módszert, és azt találta, hogy tökéletesen működik az Evilginx platformmal, ami azt jelenti, hogy az adathalász támadások során a 2FA kulcsok ellopására is adaptálható.

Egy másik, újonnan megjelent adathalász támadás[9] során automatizált chatbotokat használnak a felhasználók hitelesítési adataik ellopására. Ez az új megközelítés a rosszindulatú webhelyek látogatói számára a legitimitás érzetét kelti, mivel a chatbotokkal általában a valós márkák weboldalain találkozik az ember.

A folyamat egy olyan e-maillel kezdődik, amely úgy tűnik, hogy a DHL futárszolgálattól származik. A levélben az áldozat együttműködését kérik, hogy oldják meg a rendkívüli helyzetet, ami miatt nem tudják az adott napon kiszállítani a csomagot.

1 https://www.bleepingcomputer.com/news/security/phishing-websites-now-use-chatbots-to-steal-your-credentials/



DHL nevében küldött hamis e-mail

Az e-mailben található "Please follow our instructions" gombra kattintva egy PDF fájl töltődik be, amely az adathalász webhelyre mutató linket tartalmazza. Mivel a PDF dokumentumban jelenítik meg a linket, ezzel sikeresen kitudják kerülni a biztonsági szoftvereket, amely figyelmeztetne a káros webhelyre.

A link a dhiparcel-management[.]support-livechat[.]24mhd[.]com-ra vezeti az áldozatot, ahol az e-mailben leírt problémát kell megoldani. Ezen az oldalon veszi át a chatbot az irányítást.

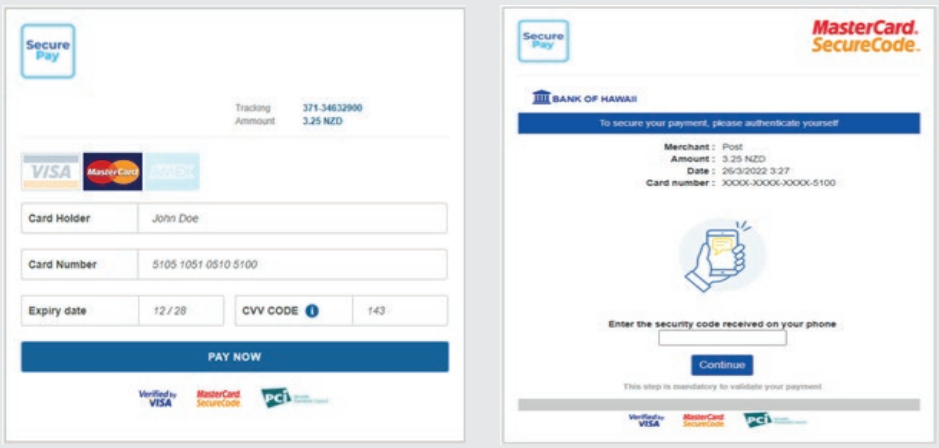
A szofisztikált támadás része, hogy itt még nem jelenítenek meg az áldozat számára semmilyen űrlapot, amellyel adatokat csalnának ki, és rögtön gyanússá válhatnának, hanem elmagyarázzák, hogy a csomag címkéjének megsérülése miatt nem tudták kézbesíteni a terméket és ennek a bizonyítására még egy fényképet is mutatnak róla.

A chatbotok előre megírt, sablon válaszokkal rendelkeznek, nincs mögöttük mesterséges intelligencia, amely specifikus választ tudna adni egy kérdésre. Ebben az esetben is így van, és mindig az állítólagos csomagunk megjelenítéséhez vezet a kommunikációs folyamat. Ezután a chatbot az áldozatot arra kéri, hogy adja meg személyes adatait (lakcím, név, telefonszám stb.) az újrakézbesítés végett.

Ezt követően a kézbesítést ütemezik, és egy hamis CAPTCHA lépést jelenítenek meg, amely tovább erősíti a felhasználóban azt az érzést, hogy nem egy rosszindulatú oldalon jár, hiszen ez egy olyan biztonsági megoldás, amivel a weboldalon pásztázó botokat tudják kiszűrni.

Ezután egy másik oldalra irányítanak át, ahol a DHL fiók hitelesítő adatainak megadását kérik az áldozattól. Végül egy fizetési lépéshez vezet, amely a felmerülő szállítási költségek fedezésére szolgál.

Az adatok megadása és a "Pay Now" gombra való kattintás után az áldozat SMS-ben kap egy egyszeri jelszót (One-time password - OTP) a megadott mobiltelefonszámra, ami tovább növeli a legitimitás érzetét.



A hamis fizetési felület és az OTP megadására felszólító form

Az OTP ellenőrzést ténylegesen megvalósították, ugyanis a véletlenszerű kódmegadás után hibát adott vissza a rendszer. A helyes kód megadása után egy "Köszönöm!" és egy megerősítő üzenet érkezik, ami megerősíti a beküldés érvényességét.

A kiberbűnözők egyre szofisztikáltabb támadásokat hajtanak végre, vagyis egyre jobban figyelnek a nyelvhelyességre, az adathalász oldalak dizájnjára, és egyre sűrűbben használnak olyan mechanizmusokat a megtévesztés fokozása érdekében, amelyeket valódi cégek használnak. Mindez azt eredményezi, hogy az embereknek egyre figyelmesebbeknek kell lenniük ahhoz, hogy ki tudják szűrni az ilyen jellegű támadásokat.

Bár talán ez az eddigi legkomolyabb adathalász akció, itt is vannak árulkodó jelek, amelyekre, ha felfigyelünk, akkor meg tudjuk kímélni magunkat egy sor kellemetlenségtől:

- Vizsgáljuk meg az URL címet! Ebben az esetben 24mhd.com domainre végződik a cím. A DHL honlapja a https://www.dhl.com/ címen, a nyomkövetési rendszerük pedig a https://mydhl.express.dhl/index/en.html címen érhető el. Fejből nem fogjuk tudni a nagyobb vállalatok weboldalának pontos címét, azonban jellemzően csak néhány karakterből áll és egyértelműen benne van a vállalat neve. Ha gyanús az URL-ben szereplő cím, semmiképpen se adjunk meg személyes adatokat.

- Ha beágyazott linkek és gombok (ezek is linkek gyakorlatilag) szerepelnek az e-mailben, azt fogadjuk mindig kétséggel!

- Ha e-mailben próbálnak bármilyen interakciót kiváltani belőlünk, a levélben szereplő oldal megnyitása helyett keressük fel mi magunk az adott céget és járjunk utána a problémának! Ez valamennyivel időigényesebb, azonban tökéletes megoldás az adathalász kampányok kiszűrésére.

Gondoljuk át az elénk tárt szituációt, és tegyünk fel magunknak pár kérdést:

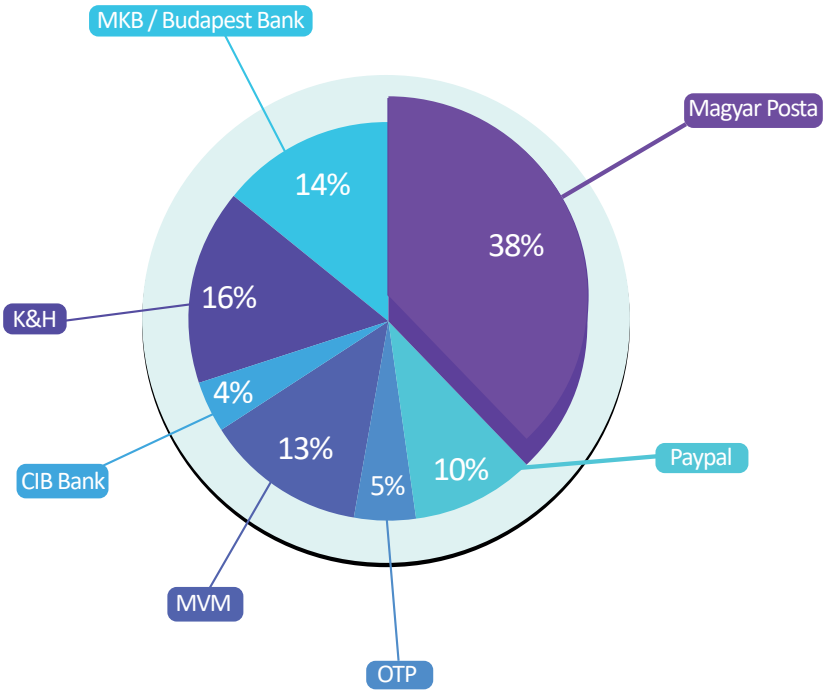
- Van bármilyen aktuális rendelésem, amivel gond adódhatott, különösképpen a DHL fogja kiszállítani a termékemet?

- Ha van is éppen futó kézbesítésem, valós lehet az, hogy a futárszolgálat hibájából velem fizettetik ki újra a szállítási költséget? Itt fontos megjegyezni, hogy nem abból a minimális, néhány dolláros szállítási költségekből fognak meggazdagodni a csalók, hanem azokat a kártyaadatainkat fogják felhasználni nagyobb összegek leemelésére, amelyet a hamis weboldalon szereplő űrlapon továbbítottunk a részükre. A kisösszegű utalás csak csali, amivel próbálják nem elrettenteni az áldozatot. 5 dollárt viszonylag gond nélkül kifizetünk, mert direkt módon nem ér nagy kár bennünket, de mi lenne a helyzet, ha 300 dolláros utalásra szólítanának fel?

Ha nem voltunk elég figyelmesek, és megadtuk a kártyaadatainkat, de utólag ráeszmélünk, hogy hibát követtünk el, azonnal hívjuk a bankunkat, és tilttassuk le a kártyánkat! Érdemes utánajárni, hogy történt-e egyéb tranzakció a számlánkon, és ha igen, tud-e a bank segíteni ennek megoldása érdekében.

Hazai helyzetkép

2021 és 2022 májusa között a NBSZ NKI Nemzeti CSIRT-nek bejelentett incidensek alapján hazai szinten a legtöbb adathalász tartalom a Magyar Postát, valamint hazai pénzintézeteket személyesítette meg.



A legtöbb adathalász támadást ért magyarországi vállalatok megoszlása az elmúlt 1 évben

A módszer tekintetében elmondható, hogy a tömeges adathalászat volt a jellemző.

Az NBSZ NKI javaslatai az adathalász támadások elkerülése érdekében

- Soha ne osszon meg senkivel jelszavakat, kódokat, tranzakciók megerősítésére használt információkat! A modern biztonsági rendszerek úgy vannak kialakítva, hogy a jelszavakat sosem manuálisan kezelik, hanem adatbázisokba mentődnek, és onnan kerülnek kiolvasásra.

- Amennyiben bármilyen felületen kaptunk egy linket (és számítógépen internetezünk), az egeret a link fölé mozgatva láthatjuk a tényleges címet, ahova a link vezet. Ezt mindig érdemes ellenőrizni, főleg abban az esetben, ha e-mailben szerepel a hivatkozás. Fontos megemlíteni, hogy bár ritkán használják, de a kiberbűnözők képesek ezt a megjelenő hivatkozást is manipulálni, így a további tanácsok betartását is javasoljuk.

- Mindig ellenőrizze az URL címeket, kimondottan az ismeretlen feladóktól kapott linkeket! A támadók gyakran használnak az eredetihez hasonló domaineket, mint például y0utube[.]com, faceb00k[.]com, official-paypal[.]com.

- Ellenőrizze a https:// meglétét azokon az oldalakon, ahol érzékeny adatokat kell megadnia! Fontos, hogy ez önmagában nem elegendő művelet, adathalász oldal is használhat ilyen protokollt.

- A legnépszerűbb böngészők már rendelkeznek beépített szűrőkkel, amelyek képesek a tömeges adathalász támadások kivédésére. Fontos, hogy tartsuk frissen böngészőnket, azonban ez nem jelenti azt, hogy minden adathalász kampányt ki fog szűrni!

- A vírusirtó programok és a spamszűrők szintén képesek jókora mennyiségű adathalász támadás kiszűrésére.

- Egyes szűrőprogramok kijátszása érdekében a támadók képként illeszthetik be a szöveget az e-mailbe. Mindig legyünk körültekintők azokkal az e-mailekkel is, amelyeket a szöveget kép formájában jelenítik meg!

- Rendkívül fontos a cégeknél valamilyen biztonságtudatossági képzés alkalmazása, ezzel naprakészen tartva a munkatársak tudását. Magánszemélyként fontos az önképzés, tájékozódjunk időnként a legújabb adathalász kampányokról, hogy ezzel is frissen tartsuk tudásunkat!

- Ha egy eddig ismeretlen személy keres fel bennünket, minden esetben kezeljük kétséggel a személyét, és győződjünk meg a hitelességéről! Például, ha a közműszolgáltatónk keres fel, és bizonytalanok vagyunk, nyugodtan keressük ki a hivatalos honlapjukon a kapcsolattartó telefonszámukat és tárcsázzunk mi magunk!

Előfordulnak olyan esetek, amikor egy valós banki ügyintéző keres fel minket egy ügyben (pl. elmaradt befizetés, biztosítás értékesítése stb.). Ilyenkor az ügyintézőnek kötelessége azonosítani az ügyfelet, nem tájékoztathatja őt azelőtt, hogy meg nem győződött arról, hogy ténylegesen a valós ügyféllel beszél. Ebben az esetben személyes adatokat fognak elkérni, mint például születési hely, születési dátum és az ügyfél édesanyjának leánykori neve, illetve a számlához köthető olyan információkat, amellyel semmilyen ügyintézést nem lehet végrehajtani. Ilyen lehet például a bankfiók címe, ahol a bankszámlát nyitotta az ügyfél, hány hitelkártya és/vagy bankkártya tartozik a számlához, van-e hitelkeret beállítva, mennyi a beállított napi készpénz felvét limit, stb.

Nagyon fontos, hogy a banki ügyintéző sosem fog elkérni olyan adatot, hogy mennyi pénz van a bankszámlán, mi a bankkártya száma, CVC kódja és lejárati dátuma.

Gondoljunk arra, hogy amikor egy online vásárlást végrehajtunk, pontosan ezek az adatok szükségesek a tranzakció lebonyolításához, így ha bárki ezeket az információkat kéri tőlünk, az több mint valószínű, hogy adathalász kísérletet próbál rajtunk végrehajtani.

Amennyiben bizonytalanok vagyunk, hogy tényleg a bank keresett-e fel minket, tegyük le a telefont, keressük ki a központi ügyfélszolgálatának a telefonszámát és tárcsázzuk! Egy authentikációt követően meggyőződhetünk arról, hogy ténylegesen a bank egyik munkatársa keresett-e bennünket, és ha igen, milyen ügyben.

Amire figyeljünk az adathalász üzenetek felismeréséhez:

- A bankok soha nem ösztönzik az ügyfeleket bejelentkezésre vagy sürgős ügyintézésre.
- Az adathalász üzenetek sok esetben nyelvtanilag helytelenek. Sok a bennük előforduló szintaktikai hiba, a megszólítás és az elköszönés sokszor nem odaillő, és a levél szövege azt az érzést kelti, mintha egy fordítóprogrammal lett volna átültetve magyar nyelvre.
- Bármilyen platformon történik a megkeresés (e-mail, telefonhívás stb.), figyeljünk a nyelvezetre! Ha például egy olyan személy hív bennünket, aki banki ügyintézőnek adja ki magát, sok esetben felkészületlen a keresztkérdésekkel szemben. Emellett sokszor nem megfelelő szakmai zsargont használ, így ha felfigyelünk egy-egy értelmetlen vagy nem odaillő kifejezésre, jó eséllyel el is tudtuk kerülni az adathalász próbálkozást.
- A levél minden része (tárgy, levéltörzs) sürgető, fokozott érzelmi állapotot próbál kiváltani a címzettből.
- A netbankolást csak a bank hivatalos honlapján vagy alkalmazásában intézze! A mai rendszerek úgy vannak kialakítva, hogyha esetlegesen mobiltelefont cserél az ügyfél, addig nem tudja újra használni az internetbankját (hiába volt már működő fiókja), amíg be nem fárad egy bankfiókba, és nem hajtják végre a szükséges lépéseket a banki ügyintézővel.

- A bankok sosem kérik különféle alkalmazások telepítését a felhasználóktól.

2022. március 31-én kivezetésre került az OTP Bank egyik mobilalkalmazása (emellett párhuzamosan már működött az új), amelyről az olyan felhasználók, akiknél telepítve volt az adott alkalmazás, hónapokon keresztül kapták az értesítéseket. Ebbe az alkalmazásba belépve szintén ez az üzenet fogadta az ügyfelet, tehát amikor ritkán történik egy ilyen volumenű átállás egy bank rendszerében, arról alaposan és részletesen tájékoztatják az ügyfeleiket, nem pedig ad-hoc jelleggel, egyszeri alkalommal.

- Amennyiben megnyitotta az e-mailben szereplő hivatkozást, és megadta az adatait, azonnal keresse fel a számlavezető bankjának ügyfélszolgálatát és függessze fel netbank jogosultságát!

NEMZETI
KIBERVÉDELMI INTÉZET

nki.gov.hu

titkarsag@nki.gov.hu

+36 (1) 325 7672

Nemzeti Kibervédelmi Intézet

@ nki.gov.hu

Kibertámadás!
podcast

2022