Malware (kártékony szoftver)

Több információ: SEC.EFF.ORG
Az Electronic Frontier Foundation Alapítvány projektje

A MALWARE egy rövid név minden olyan rosszindulatú programra, ami nem kívánatos tevékenységeket végez az eszközödön.

A kártékony szoftverek lehetnek:

- számítógépes vírusok
- programok, amik jelszavakat lopnak el
- programok, amik titokban megfigyelnek
- programok, amik titokban törlik az adataidat

Malware adathalászaton keresztül

Az adathalászat (Phising) az, amikor a támadó küld egy ártatlannak tűnő üzenetet, emailt, vagy linket, ami valójában rosszindulatú. Az adathalászat során gyakran egy általad ismert embert személyesítenek meg, vagy egy olyan weboldalt másolnak le, amiben bízol.

Megjegyzés: Az adathalászat nem minden esetben tartalmaz kártékony szoftvert. Előfordul, hogy a támadó egy szolgáltatáshoz tartozó jelszavadat szeretné ellopni, amit egy weboldal lemásolásával ér el kártékony szoftver telepítése nélkül.

Kártékony szoftverek telepítésének gyakori fajtái

Rosszindulatú csatolmány vagy fájl megnyitása	Gyakran osztanak meg rosszindulatú csatolmányokat adathalász üzenetekben.
Egy rosszindulatú linkre kattintás	Gyakran osztanak meg rosszindulatú linkeket adathalász üzenetekben.
Illegális programok letöltése	Olyan szoftver, ami nem kap biztonsági frissítéseket növeli a kockázatot (pl nem az Apple App store-ból vagy a Google Play áruházból került letöltésre)

Megfertőzött oldalak látogatása	Előfordul, hogy egyes weboldalak fölött átveszik az irányítást, és rosszindulatú tartalom szolgáltatására használják.

A kártékony szoftverek típusai

Adware (Reklámvírus)	reklámok mindenütt Ez a rosszindulatú szoftver általában reklámokat próbál megjeleníteni a felhasználónak többek között felugró ablakokkal. Egyes reklámvírusok információt gyűjtenek a felhasználóról, vagy személyes információkat szereznek meg. Más kártékony szoftverektől eltérően a reklámvírus más szoftverrel együtt is tud érkezni, gyakran nem megbízható forrásokból, mint például nem hivatalos alkalmazás letöltő helyekről, vagy nem a fejlesztőtől.
Stalkerware (megfigyelő-vírus)	amikor az eszközöd a téged megfigyelőnek segít A megfigyelővírus csendben fut, és a támadónak teljes hozzáférést biztosít az eszköz felett. Megfigyelővírust telepíthet az, akinek fizikai hozzáférése van az eszközhöz (pl családtag vagy partner, “hadd használjam a telefonodat egy pillanatra”) és egy ilyen applikációt telepít, de előfordulhat, hogy a felhasználót trükkel ráveszik egy alkalmazás letöltésére.
Trójai vírus	ajándéknak tűnik, de támadást rejteget Letöltését követően úgy működhet, mint a letölteni kívánt legitim szoftver, de valójában a háttérben rosszindulatú tevékenységet folytat. Ez gyakran illegális vagy “tört” szoftverekben található, vagy kamu vírusírtókban.

Zsarolóvírus	szoftver, ami túszként tart fogva Letöltés után ez a rosszindulatú szoftver váltságdíjat követel egy vállalat, szervezet vagy magánszemély adataiért. A zsarolóvírusok az elmúlt évtizedben váltak népszerűvé, és mára világszerte támadók több millió dolláros üzlettévé vált .
A.P.T. támadás	Fejlett tartós fenyegetés Az A.P.T támadás során az ellenségnek szofisztikált képességekkel és jelentősen több erőforrással rendelkezik a céljai eléréséhez: ami nem más, mint a rendszered megfertőzése. Az A.P.T. támadásokat gyakran használják egyidejűleg nemzetállami szereplőkkel, akik megpróbálják fenntartani a hosszú távú hozzáférést a célzott rendszerhez.

5 TIPP A KÁRTÉKONY SZOFTVEREK ELLENI VÉDEKEZÉSHEZ

1. TIPP: TARTSD FRISSEN A SZOFTVEREIDET

(ÉS ELLENŐRIZD, HOGY LEGÁLIS* SZOFTVERT HASZNÁLSZ)

A legtöbb kártékony szoftver ismert hibákat használ ki. A szoftvercégek gyakran megjavítják ezeket a hibákat, és frissítések segítségével juttatják el a felhasználókhoz.

Ebből kifolyólag a szoftverfrissítések elengedhetetlenek a felhasználó biztonságához, mert ez a legbiztosabb módja annak, hogy naprakészek maradjunk az ismert sebezhetőségek kiküszöbölésében, amelyeket a támadók kihasználhatnak.

*Ha nem tudod hogyan juthatsz legális szoftverhez, kérj tanácsot a digitális biztonsági tanácsadódtól.

2. TIPP: BIZTONSÁGI MENTÉSEK A JÖVŐ SZÁMÁRA

Csinálj biztonsági mentést ma, és a jövőbeli önmagad hálás lesz neked. Ha elveszíted az eszközödet (legyen az kártékony szoftver, lopás vagy műszaki meghibásodás miatt), nem lesz

minden veszve: a fájljaid ott lesznek a biztonsági mentéseidben. Óvd meg azokat a biztonsági mentéseket egy erős jelszó használatával és titkosítással.

3. TIPP: ÁLLJ MEG EGY PILLANATRA, MIELŐTT KATTINTASZ

A link- és fájlmegosztás egy bevett gyakorlat, de légy résen, amikor linkekkel kommunikálsz vagy megosztod őket. Mielőtt kattintasz, kérdezd meg magadtól: nem gyanús ez nekem?

FIGYELJ… RÖVIDÍTETT & LEVÁGOTT LINKEKRE

Linkek és emailek gyakran kisebb méretben jelennek meg előnézetben mint számítógépen. Link rövidítők mint a bit.ly és hasonlók rosszindulatú weboldalakra irányíthatnak át.

Tipp: használj egy olyan szolgáltatást, mint a https://unshorten.it, hogy megtekinthesd a teljes URL-t.

MEGSZEMÉLYESÍTÉS, A CSŐBEHÚZÁS LEGMAGASABB SZINTJE

Elütések, hasonló karakterek és lemásolt brand elemek célja, hogy megtévesszenek. Győződj meg róla, hogy valóban tényleges szolgáltatásról van-e szó.

Tipp: amikor egy hiteles szolgáltatáson vagy, használj könyvjelzőt: a számítógéped segít megjegyezni a hiteles weboldalak címeit.

Tipp: mentsd el a helyes linket a jelszókezelődben: egy jelszókezelő meg tudja jegyezni a kijelölt oldalakat és beírja a jelszavadat helyetted.

Figyelj oda a “social engineering”-re (pszichológiai manipuláció), például ha kapsz valakitől egy üzenetet, aki úgy tesz, mintha a barátod lenne.

Tipp: Keresd fel a barátodat egy másik kommunikációs csatornán, és győződj meg róla, hogy ténylegesen ő az.

VÉLETLEN ÉRINTÉS VAGY KATTINTÁS

Amikor linkeket tanulmányozol az eszközödön, egyetlen véletlen kattintás megnyithatja a linket!

Tipp: ha egeret használsz, használd ki, hogy ha ráviszed az egered a hivatkozásra, megmutatja a teljes linket.

4. TIPP: ÓVAKODJ A FIZIKAI HOZZÁFÉRÉSTŐL

Néha az ellenségeink általunk ismert emberek, vagy olyan emberek, akik hozzá tudnak férni az eszközeinkhez, amikor nem figyelünk oda rájuk. Ha lemeztitkosítást és erős jelszót használsz az eszköz védelmére, az segíthet megvédeni azt a nem kívánt fizikai hozzáféréstől. Légy óvatos, amikor kölcsönadod valakinek a lezáratlan telefonod. Ha bővebben szeretnél erről olvasni, látogass el a ssd.eff.org oldalra.

5. TIPP: HASZNÁLJ VÍRUSÍRTÓT

Nem mindegyik vírusírtó ugyanolyan. Némelyik sokat reklámozott vírusírtót megtévesztik a kártékony szoftverek. Vélhetően a saját eszközödhöz tartozó vírusírtót használnád. Ha másik gyártó programjait preferálnád:

- nézz utána független ajánlásoknak és
- keress rá, hogy a weboldalának van-e friss kártékony szoftver* listája azokról a típusokról melyek miatt aggódsz

*A publikált fenyegetés kutatások arra utalnak, hogy a vírusirtónak aktív csapata van, amely védekezik az ilyen típusú kártékony szoftverek ellen.

AZT HISZEM KÁRTÉKONY SZOFTVEREM VAN, MIT TEGYEK?

Valami furcsa dolog történik az eszközödön? Csak egy felhasználói felületen (pl. közösségi média), vagy a teljes eszköz érintett? Ha úgy tűnik kártékony szoftver fut, légy óvatos miként használod a fertőzött eszközt a továbbiakban - egy másik eszközről* keress szakértőt, hogy segítsen.

*A különálló eszköz ne legyen kapcsolatban a fertőzött eszközzel. Ez lehet egy könyvtári számítógép vagy egy barát telefonja például.

LÉPJ KAPCSOLATBA EGY SZAKÉRTŐVEL

Naplózd a furcsa üzeneteket az eredeti formájukban ahogy kaptad (pl. ha ez egy email, akkor továbbítsd az egész levelet, benne a fejléccel, ne csak egy képernyőképet). Legyen benne a dátum, az időpont és a leírás. Küldd ezeket egy megbízható szakértőhöz.

MÉRD FEL A KÁRT

Milyen érzékeny adat kompromitálódhatott? Érdemes jelszót vagy felhasználót váltanod? A biztonságod érdekében tervezd meg a következő lépéseidet - végezz kockázatelemzést (ld. fenyegetettségi modell).

Miért fontos a Metaadat

Utolsó frissítés: 2019. Március 11.

A metaadatot gyakran úgy definiáljuk, mint minden adat, ami a kommunikációd tartalmán túl található. A metaadatot képzelheted egy digitális borítéknak. Ahogy a boríték is megmutatja ki a feladó, a címzett és a helyet ahova küldték, úgy árulkodik a metaadat is. A metaadat információ a kommunikációdról. Néhány példa a metaadatra:

- az emailek tárgysora
- a beszélgetések hossza

- a beszélgetések időpontjai
- a kommunikációd idején a hely adataid (és annak is, akivel kommunikáltál)

Hagyományosan a metaadatokat kevesebb védelem illeti - pl. az Egyesület Államokban - mint a kommunikáció tartalmát magát. A rendőrség a legtöbb országban könnyűszerrel láthatja, hogy a múlt hónapban kikkel beszéltél, de bonyolult lenne a vonaladat lehallgatniuk.

Nem tartják jelentős dolognak a metaadatokhoz való hozzáférésüket vagy igényüket azok, akik azt gyűjtik - pl. a kormányzatok vagy a telekommunikációs cégek. Sajnos ez a megközelítés hamis. Már egy pici metaadat tartalom is bepillantást adhat egy személy életébe. Vessünk egy pillantást arra, hogy mennyit is mutat meg a metaadat a kormányzatoknak és a cégeknek melyek még gyűjtik.

- Tudják, hogy felhívtál egy szex-vonalat hajnali 2:24-kor és 18 percig hívásban voltál. De nem tudják miről beszéltél.
- Tudják, hogy hívtad az öngyilkossági segélyvonalat a Golden Gate hídról. De a beszélgetés témája titok marad.
- Tudják, hogy emailt kaptál egy HIV tesztközpontból, utána hívtad az orvosod, majd egy HIV fertőzötteket támogató központ oldalát olvastad egy órán belül. De nem tudják mi volt az emailben vagy mit beszéltél a telefonon.
- Tudják, hogy emailt kaptál egy digitális jogokat védő aktivista csoporttól azzal a tárggyal, hogy “Szólj a Kongresszusnak: Állítsák meg a SESTA/FOSTA-t” és utána hívtad a körzeted képviselőjét. A levél és a hívás tartalma biztonságban maradt a kormányzati tolakodástól
- Tudják, hogy hívtad a nőgyógyászod, beszéltetek egy félórát és később telefonáltál egy helyi abortusz klinikára.

A metaadatot elég bonyolult lenne elrejteni, mert a kommunikációd sikeréhez szüksége van hozzáférésre a harmadik félnek. Ahogy egy postás kell lássa a címzettet a borítékon a digitális kommunikációban is jelölni kell a forrást és a célját. A mobil cégeknek tudniuk kell, hogy nagyjából hol van a telefonod, hogy hívást kapcsoljanak rá.

Az olyan szolgáltatások mint a Tor a metaadatok mennyiségét igyekeznek csökkenteni az általános online kommunikációban. Amíg a törvények fejlettebben nem védik a metaadatokat és az azokat minimalizáló eszközök szélesebb körben nem terjednek el, a legjobb amit tehetsz, hogy odafigyelsz rá milyen metaadatot osztasz meg a kommunikációd során, és ahhoz ki férhet hozzá és hogyan használhatja.

A te biztonsági terved

Utoljára módosítva: 2023.10.07.

Elég megterhelő lenne, ha minden pillanatban arra kellene figyelned, hogy megvédd az adataidat. Megnyugodhatsz. Az adataidat megvédeni sokkal egyszerűbb, mint gondolnád. A biztonság az egy folyamat, amelynek során alapos tervezéssel létre tudsz hozni egy olyan tervet, ami pont neked jó. Hiszen a biztonságod nem csak a rendelkezésedre álló eszközöket és szoftvereket jelenti, hanem

azt is, hogy tisztában vagy azzal, hogy milyen veszélyek fenyegethetnek, és hogyan tudsz szembeszállni velük.

A veszélyek, amelyek a digitális eszközeid biztonságát fenyegetik alááshatják azt a törekvésed, hogy megvédd az adataidat. De azzal, hogy meghatározod, hogy mit szeretnél megvédeni, és kiktől, könnyebben szembeszállhatsz a veszélyekkel, amelyek fenyegetnek. Ezt a folyamatot, a biztonsági tervezést sokszor csak “threat modeling”-nek, azaz fenyegetettségi modellezésnek szoktuk hívni.

Ez az útmutató megtanítja neked, hogy hogyan készíts egy biztonsági tervet arról, hogy hogyan védd meg a digitális információidat, valamint segít meghatározni, hogy mik a legjobb megoldások a számodra.

Hogy néz ki egy biztonsági terv? Vegyük például, hogy szeretnéd megvédeni a házadat és a benne lévő ingóságaid. Ebben az esetben például ezeket a kérdéseket tennéd fel:

Mi van otthon, amit védeni érdemes?

Például ékszerek, elektronikai eszközök, pénzügyi papírok, útlevelek, vagy fotók.

Kiktől szeretném megvédeni ezeket?

A fenyegetettség származhat például betörőktől, szobatársaktól vagy akár vendégektől is.

Mekkora a valószínűsége, hogy valóban védenem kell ezeket a dolgokat másoktól?

Van a szomszédaimnak büntetett előélete? Máskor is betörtek már valahova? Mennyire megbízhatóak a szobatársaim/vendégeim? Milyen képességeik vannak azoknak, akik fenyegethetnek engem? Milyen kockázati tényezőket kell figyelembe vennem?

Mi történik, ha nem sikerül megvédenem?

Van olyasmi a házamban, ami pótolhatatlan? Van arra időm és pénzem, hogy ezeket pótoljam? Van biztosításom ezekre a dolgokra?

Mennyit vagyok hajlandó tenni azért, hogy megvédjem magam ezektől a következményektől?

Hajlandó vagyok venni egy széfet, hogy abban tároljam a fontos dokumentumaimat? Van időm és pénzem arra, hogy nyissak egy széfet a bankomban, hogy ott tároljam az értékeimet?

Miután megkérdezted magadtól ezeket a kérdéseket, meg tudod határozni, hogy milyen lépéseket kell tenned a biztonságod érdekében. Ha az értékeid fontosak számodra, de kicsi az esély arra, hogy betörjenek hozzád, akkor nem biztos, hogy túl sok pénzt fogsz költeni egy vagy több plusz lakatra a házadon. De ha a betörés esélye nagy, akkor a legjobb lakatot akarod megvenni a házadra a piacon, és talán egy riasztó rendszert is telepíteni fogsz.

A biztonsági terv elkészítése segít neked, hogy tisztábban lásd a rád egyedileg leselkedő veszélyeket, felbecsüld az értékeidet, felmérd a rád leselkedő fenyegetéseket, a fenyegetők képességeit, és a valószínűségét a lehetséges kockázatoknak.

Hogyan készíthetem el a saját biztonsági tervemet? Hogyan kezdjek neki?

A biztonsági tervezés lehetővé teszi számodra, hogy felismerd és meghatározd a számodra értékes dolgokat, és a szereplőket, akiktől meg akarod védeni ezeket. Amikor biztonsági tervet készítesz, tedd fel magadnak a következő kérdéseket:

- Mit szeretnék megvédeni?
- Kitől szeretném megvédeni ezeket a dolgokat?
- Mennyire súlyosak a következmények, ha nem sikerül megvédenem?
- Mennyire valószínű, hogy meg kell majd védenem ezeket a dolgokat?
- Mennyi problémát vagyok hajlandó vállalni a következmények elkerülése érdekében?

Nézzük meg közelebbről a fenti kérdéseket.

Mit szeretnék megvédeni?

Az “erőforrás” egy olyan dolog, amit értékesnek tartasz és védesz. A digitális biztonság területén ez általában valamilyen információ. Például az emailjeid, a névjegyeid, a chat üzeneteid, a földrajzi helyzeted, vagy dokumentumaid is lehetnek ilyen erőforrások. Bizonyos értelemben az elektronikai eszközeid ezek.

Készíts egy listát az ilyen erőforrásaidról: milyen adatokat őrzöl, hol tárolod ezeket, kinek van hozzáférése, és mi akadályoz meg másokat, hogy hozzáférjenek ezekhez.

Kitől szeretném megvédeni ezeket a dolgokat?

Ahhoz, hogy ezt a kérdést megválaszoljuk, nagyon fontos meghatározni, hogy ki akarhat megcélozni téged vagy az információidat. Azt a személyt vagy szervezetet, aki veszélyt jelent számodra, fenyegető nevezzük. Ilyen fenyegető lehet például a főnököd, a korábbi partnered, a versenytársad, a kormányod, vagy egy hacker a hálózatról.

Készíts listát a potenciális fenyegetőkről, akik esetleg rá akarhatják tenni kezüket az erőforrásaidra. Ez a lista tartalmazhat személyeket, állami szerveket, vagy vállalatokat.

A fenyegetők jellegétől függően ezt a listát érdemes lehet megsemmisíteni a a biztonság terved elkészítését követően.

Mennyire súlyosak a következmények, ha nem sikerül?

A fenyegetők sokféle módon veszélyeztethetik az adataidat. Például elolvashatják a privát üzeneteidet amíg átmegy a hálózaton keresztül, tönkre tehetik, törölhetik az adataidat.

A fenyegetők motiváció és taktikái egyaránt sokfélék lehetnek. Egy kormány megpróbálhatja megelőzni egy videó terjedését, amin rendőri erőszak szerepel a videó egyszerű törlésével vagy az elérhetőségének korlátozásával. Ezzel szemben egy politikai ellenfél szerethetné megszerezni titkos tartalmat és publikálni azokat, a tulajdonos tudta nélkül.

A biztonsági terv készítése magában foglalja azt is, hogy átgondoljuk, mennyire súlyos következményei lehetnek, ha a fenyegetések megvalósulnak, és átveszik a hatalmat az erőforrásaink fölött. Ahhoz, hogy ezt meghatározzuk, figyelembe kell venned a fenyegetők képességeit. Például a mobilszolgáltatódnak hozzáférése van mobilhívásaid adataihoz. Egy hacker egy nyilvános Wifi hálózaton keresztül hozzáférhet a nem titkosított kommunikációdhoz. Egy kormánynak viszont valószínűleg erősebb képességei és eszközei lehetnek.

Írd le, hogy mire akarhatják felhasználni a privát adataidat a támadók.

Mennyire valószínű, hogy meg kell majd védenem ezeket a dolgokat?

Kockázatnak nevezzük, hogy egy bizonyos erőforrás elleni bizonyos fenyegetés mennyi eséllyel fog valóban megtörténni. A kettő kéz a kézben jár. A mobilszolgáltatódnak megvan a lehetősége, hogy hozzáférjen az összes adatodhoz. Annak az esélye viszont, hogy ezeket közzéteszi a tekintélyed csorbítása érdekében, nagyon alacsony.

Fontos felismernünk a különbséget aközött, hogy mi az, ami megtörténhet, és hogy mennyi az esélye, hogy valóban meg is történik. Például, lehet az is egy fenyegetés, hogy összeomlik a házad, viszont ez jóval valószínűbb mondjuk San Francisco-ban (ahol gyakoriak a földrengések), mint Stockholmban (ahol nem túl gyakoriak ugyanezek).

A kockázatok értékelése személyes és szubjektív folyamat. Sokan bizonyos veszélyeket elfogadhatatlannak tartanak, függetlenül attól, hogy milyen valószínűséggel fognak bekövetkezni, mert a veszély puszta jelenléte bármilyen valószínűség mellett sem éri meg a költségeket. Más esetekben az emberek figyelmen kívül hagyják a magas kockázatokat, mert nem tekintik a fenyegetést problémának.

Írd le, hogy mely fenyegetéseket érdemes komolyan venned, és melyek azok, amelyek vagy túl ritkák vagy ártalmatlanok lehetnek ahhoz (vagy túl nehéz ellenük küzdeni), hogy aggódj miattuk.

Mennyit vagyok hajlandó befektetni abba, hogy megvédjem magam a következményektől?

Az embereknek nem ugyanazok a prioritásai, az aggodalmai, és a hozzáférési lehetőségei sem az egyes forrásokhoz, ami természetes. Pont ezért a te saját kockázatfelmérésed, ami a te adataidról és környezetedről szól, teszi igazán lehetővé azt, hogy megtervezd a megfelelő stratégiát saját magad, magatok számára, egyensúlyozva a költségek, a felvállalt kellemetlenségek, és az adatok védelme között.

Például amikor az ügyvéd a kliensét egy nemzetbiztonsági ügyben védi, akkor többet akarhat megtenni a kommunikációja védelméért az üggyel kapcsolatban, mint például az email titkosítás, mint egy családtaggal, aki időnként macskás videókat küld.

Írd le, hogy milyen lehetőségeid vannak arra, hogy csökkentsd azokat a veszélyeket, amelyek téged fenyegethetnek. Jegyezd fel, ha valamilyen gazdasági, technikai vagy társadalmi korlátokba ütközhetsz.

Biztonság a mindennapok részeként

Tartsd észben, hogy a saját biztonsági terveid is folyton változhatnak, ahogy a helyzeted és a körülményeid is folyton változnak. Ezért érdemes gyakran felülvizsgálni azokat.

Ne felejtsd el a saját biztonsági tervedet mindig a saját szituációd és körülményeid alapján megtervezni, és mindig azokhoz szabni! Amikor pedig elkészültél vele, ne felejtsd el bejelölni azt a dátumot a naptáradban, amikor legközelebb felül fogod vizsgálni!

Credit for translation and localization goes to Journalist Security Fellowship fellows in partnership with Localization Lab.

This content is distributed under a CC-BY-SA 4.0 license. It is adapted from the following resources, all licensed under a CC-BY 3.0 license:

- Malware: https://www.securityeducationcompanion.org/files/sec/upload/file/37/SEC-malware-handout.pdf
- Why metadata matters: https://ssd.eff.org/module/why-metadata-matters
- Your security plan: https://ssd.eff.org/module/your-security-plan

In partnership with

LOCALIZATION LAB