EUIPO
EURÓPAI UNIÓ SZELLEMI TULAJDONI HIVATALA

ROSSZINDULATÚ PROGRAMOK AZONOSÍTÁSA ÉS ELEMZÉSE KIVÁLASZTOTT, FELTÉTELEZETTEN SZERZŐI JOGOT SÉRTŐ WEBOLDALAKON

VEZETŐI ÖSSZEFOGLALÓ

2018. szeptember

Kivonat

A feltételezetten szerzői jogot sértő tartalmak jelentős mértékű szellemitulajdonjog-sértésnek minősülnek. Vannak olyan weboldalak, amelyek nyilvánosan osztanak meg ilyen tartalmakat – akár ingyen is –, regisztráció nélkül. Ezekkel a tartalmakkal együtt a weboldalak gyakran különféle rosszindulatú programokat és potenciálisan nemkívánatos programokat (PUP-ok) terjesztenek, rábírva a felhasználókat a fájlok letöltésére és elindítására. A tanulmány áttekintést nyújt a feltételezetten szerzői jogot sértő weboldalakon található rosszindulatú programok és PUP-ok legfrissebb példáiról. Ezek a programok megtévesztő technikákat és pszichológiai manipulációt használnak – például üres játéktelepítőket és látszólag „hasznos” szoftvereket –, hogy a végfelhasználókból érzékeny információkat csaljanak ki. A vizsgálat során különböző PUP-okat fedeztek fel, mint például „hasznos” szoftvereket, hamis játéktelepítőket, valamint videostreamelő platformokhoz való klienseket. Ez a szoftver nem feltétlenül jelent közvetlen veszélyt a felhasználó szoftverére vagy hardverére. Azonban pszichológiai manipulációs trükkök révén a felhasználót meg lehet győzni arról, hogy nyilvánosságra hozzon érzékeny személyes adatokat vagy a bankkártyaadatait. Ezenkívül a számítógépre vonatkozó információkat kiszivárogtathatják más felek számára a felhasználó kifejezett hozzájárulása nélkül.

Kutatócsoport

A kutatócsoport tagjai: Francesca Bosco, UNICRI programfelelős és Andrii Shalaginov, PhD kutató az információbiztonság területén, a Norvég Tudományos és Technológiai Egyetem (NTNU) informatikai és villamosmérnöki karának információbiztonsági és kommunikációs technológiai tanszékén (digitális kriminalisztikai csoport).

Jogi nyilatkozat

Ebben a kontextusban hangsúlyozni kell, hogy a kutatás egyedüli célja az volt, hogy meghatározza a vizsgálat során talált rosszindulatú programok és PUP-ok technikai jellemzőit, amelyekkel az internetfelhasználók is találkozhatnak feltételezetten szerzői jogot sértő tartalmak keresésekor. A dokumentált rosszindulatú programok és PUP-ok mintái nem tekinthetők kimerítőnek, továbbá a tanulmány (vagy annak eredményeinek) célja sem az volt, hogy felmérje a rosszindulatú programokkal és PUP-okkal való fertőzöttség – amellyel az internetfelhasználók is találkozhatnak a feltételezetten szerzői jogot sértő anyagok keresésekor – általános valószínűségét vagy kockázatát.

Előszó

A feltételezetten online szerzői jogot sértő tevékenységeket többféle módon lehet finanszírozni, beleértve az előfizetési díjakat, adományokat, kiegészítő szolgáltatásokért történő fizetést, valamint az online hirdetések megjelenítéséből származó bevételt.

Azonban nem minden finanszírozási eszköz olyan ártalmatlan, mint a megadott példák. A rosszindulatú programokkal való fertőzöttség és a potenciálisan nemkívánatos programok (PUP-ok) egyéb formáinak terjesztése évek óta kulcsfontosságú a feltételezetten szerzői jogot sértő tevékenységek interneten történő finanszírozása tekintetében.

Az átlagos internetfelhasználók kezdik felismerni a feltételezetten szerzői jogot sértő weboldalak vagy mobilalkalmazások elérésekor jelentkező fertőzés kockázatát.

Az EUIPO 2015-ös, a szellemi tulajdon és a fiatalok témájával foglalkozó eredménytáblája (IP Youth Scoreboard) szerint a fiatalok 52%-a fontosnak tartja a weboldalak biztonságosságát online tartalmak elérésekor. Összesen a fiatalok 78%-a jelentette ki, hogy kétszer is meggondolná, mit tegyen, ha tisztában lenne annak kockázatával, hogy a számítógép vagy az eszköz vírusokkal vagy rosszindulatú programokkal fertőződhet meg. Összesen 84%-uk mondta azt, hogy kétszer is meggondolná, mit tegyen, ha tisztában lenne annak kockázatával, hogy hitelkártya-adatait ellophatják.

A jelen tanulmány keretében végzett kutatás során a Hivatal egy technikailag igen nagy kihívást jelentő feladatra vállalkozott, nevezeten azoknak a rosszindulatú programok és PUP-ok példáinak felderítésére és dokumentálására, amelyekkel az internetfelhasználók is találkozhatnak, amikor népszerű kalózfilmekhez, zenékhez, videójátékokhoz és televíziós főcímekhez próbálnak hozzáférni.

Ebben a kontextusban hangsúlyozni kell, hogy a kutatás egyedüli célja az volt, hogy meghatározza a vizsgálat során talált rosszindulatú programok és PUP-ok technikai jellemzőit, amelyekkel az internetfelhasználók is találkozhatnak feltételezetten szerzői jogot sértő tartalmak keresésekor. A dokumentált rosszindulatú programok és PUP-ok mintái nem tekinthetők kimerítőnek, továbbá a tanulmány (vagy annak eredményeinek) célja sem az volt, hogy felmérje a rosszindulatú programokkal és PUP-okkal való fertőzöttség – amellyel az internetfelhasználók is találkozhatnak a feltételezetten szerzői jogot sértő anyagok keresésekor – általános valószínűségét vagy kockázatát.

A kutatást több fázisban végezték el az Europol Számítástechnikai Bűnözés Elleni Európai Központjával (EC3) szorosan együttműködve.

Az eredmények azt mutatják, hogy számos különböző rosszindulatú program és PUP-fenyegetés létezik, amelyekkel az internetfelhasználók feltételezetten szerzői jogot sértő tartalmak keresésekor találkozhatnak. A dokumentált rosszindulatú programok és PUP-ok nagy része trójai programként vagy egyéb nemkívánatos szoftverként írható le, amely képes jogosulatlanul hozzáférni az internetfelhasználók személyes adataihoz. Ezek a példák nemcsak a szellemitulajdonjog-birtokosok közösségének relevánsak és érdekesek, hanem a végrehajtó hatóságoknak, és nem utolsó sorban azoknak a fogyasztóknak is, akik aggódnak amiatt, hogy személyes adataikhoz engedélyük nélkül férnek hozzá.

Vezetői összefoglaló

A tanulmány áttekintést nyújt a feltételezetten szerzői jogot sértő weboldalakon található rosszindulatú programok és potenciálisan nemkívánatos programok (PUP-ok) legfrissebb példáiról. Ezek a programok megtévesztő technikákat és pszichológiai manipulációt használnak – például üres játéktelepítőket és látszólag „hasznos” szoftvereket –, hogy a végfelhasználókból érzékeny információkat csaljanak ki.

Jelen tanulmány célja, hogy felfedezze és dokumentálja a kártékony vagy egyéb módon nemkívánatos szoftvereket, amelyeket feltételezetten szerzői jogot sértő weboldalakon terjesztenek, továbbá hogy a talált mintákat kategorizálja a különböző rosszindulatú programok taxonómiái szerint. Ebben a kontextusban hangsúlyozni kell, hogy a tanulmány egyedüli célja az volt, hogy meghatározza a vizsgálat során talált rosszindulatú programok és PUP-ok technikai jellemzőit, amelyekkel az internetfelhasználók is találkozhatnak feltételezetten szerzői jogot sértő tartalmak keresésekor. A dokumentált rosszindulatú programok és PUP-ok mintái nem tekinthetők kimerítőnek, továbbá a kutatás (vagy annak eredményének) célja sem az volt, hogy felmérje a rosszindulatú programokkal és PUP-okkal való fertőzöttség – amellyel az internetfelhasználók is találkozhatnak a feltételezetten szerzői jogot sértő anyagok keresésekor – általános valószínűségét vagy kockázatát. Jelen tanulmány céljából a televíziós műsorokat, filmeket, zenéket és videojátékokat szerzői jogi védelem alatt álló tartalmaknak tekintjük.

A tanulmány eredményei

A feltételezetten szerzői jogot sértő tartalmak jelentős mértékű szellemitulajdonjog-sértésnek minősülnek. Vannak olyan weboldalak, amelyek nyilvánosan osztanak meg ilyen tartalmakat – akár ingyen is –, regisztráció nélkül. Az ilyen tartalmakkal együtt a weboldalak gyakran különféle rosszindulatú programokat és PUP-okat terjesztenek, amelyek rábírják a felhasználókat az ilyen fájlok letöltésére és elindítására. Az Alexa Top 500 rangsorolásán, valamint a jól ismert keresőmotorok – például a Google, a Yahoo és a Bing – segítségével végzett átlagos felhasználói keresések szimulációján alapuló weboldal-azonosítás során azt tapasztalták, hogy a weboldalak köre a tanulmány két fordulója között megváltozott. Ez a változás valószínűleg a keresőmotorok arra irányuló erőfeszítéseinek eredménye, hogy eltávolítsák a feltételezetten szerzői jogot sértő weboldalakra mutató linkeket, míg új, gyanús weboldalak jelennek meg. A weboldal azonosítása terén egy érdekes megállapításra jutottak, mely azzal a ténnyel kapcsolatos, hogy a weboldalak túlnyomó többségét az Amerikai Egyesült Államokban hosztolják, vagy olyan doménnevekkel rendelkeznek, amelyek USA-beli hosztolással hozhatók összefüggésbe. Ezzel szemben csak néhány található EU-n belüli szervereken. Továbbá a .com és a .net a leggyakrabban használt legfelső szintű doménnév a feltételezetten szerzői jogot sértő weboldalakon. Ezt az okozhatja, hogy az országspecifikus doménektől eltérően ezek nem feltétlenül teszik szükségessé a felhasználó azonosítását útlevél vagy egyéb személyazonosító okmány által. Átlagosan az új webhelyek 20%-át adták hozzá és a régi webhelyek 20%-át távolították el a két azonosítási forduló között. Továbbá a mindkét fordulóban azonosított webhelyek közel 8%-át minősítette a VirusTotal platform kártékonynak. A különböző tartalomkezelő rendszerek segítségével szinte erőfeszítés nélkül lehet létrehozni weboldalakat, valamint tartalmakat – a kártékony alkalmazásokat is beleértve – szolgáltatni a felhasználóknak.

A rosszindulatú programok gyűjtését megelőzően e tanulmány keretében áttekintésre kerültek a 2017-ben rosszindulatú programokkal való fenyegetettségek, továbbá ezeket a legkorszerűbb módon kategorizálták. Ezt az ismeretanyagot a rosszindulatú programok elemzésénél is felhasználták, hogy kövessék a közösség által elfogadott elveket a rosszindulatú programok típusai és a programcsaládok azonosítása terén. Összesen 106 fájl került összegyűjtésre a két adatgyűjtési forduló során. Ezek közé tartoznak a közvetlenül a feltételezetten szerzői jogot sértő weboldalakról letöltött fájlok, valamint a letöltött fájlok végrehajtása során létrehozott fájlok. A

vizsgálat során különböző PUP-okat fedeztek fel, mint például „hasznos” szoftvereket, hamis játéktelepítőket, valamint videostreamelő platformokhoz való klienseket. Az ilyen szoftver nem feltétlenül jelent közvetlen veszélyt a felhasználó szoftverére vagy hardverére. Azonban pszichológiai manipulációs trükkök révén a felhasználót meg lehet győzni arról, hogy nyilvánosságra hozzon érzékeny személyes adatokat vagy a bankkártyaadatait. Ezenkívül a számítógépre vonatkozó információkat kiszivárogtathatják más felek számára a felhasználó kifejezett hozzájárulása nélkül.

Az összegyűjtött rosszindulatú programokat kezdetben nyílt forráskódú eszközök segítségével elemezték a belső logika megértése, a lehetséges kártékony tevékenységek felderítése és ezek relevanciájának a jelen rosszindulatú programokról szóló tanulmány szempontjából történő értékelése céljából. A nyílt forráskódú eszközöket használó előzetes elemzés mellett az összegyűjtött rosszindulatú programok mintáit az Europol Malware Analysis Solution (EMAS) platformja is elemezte. Ez különböző termékek és kártékony tevékenységek nagy számban történő felfedezéséhez vezetett. Az EMAS-jelentések tartalmazzák a fájlok átfogó elemzését az MS Windows négy változatának felhasználásával, ahol a hálózati forgalmat, a funkcióhívásokat és a lemez tevékenységeit részletesen naplózzák további elemzés céljából. Ezenkívül a platform kiemeli a fájlvégrehajtási gyakorlatok során észlelt gyanús tevékenységeket. Az összes jelentés elemzését követően az EMAS a kártékony tevékenységek 35 típusát jegyezte fel, amelyeket a kártékony események 17 osztályába összesítettek. Ezek az általános rendellenességektől (például rendszerprocesszorok indítása vagy folyamatok felkutatása memóriákban) az összetéveszthetetlenül kártékony tevékenységekig terjednek (például billentyűzetfigyelő, rootkit vagy a hálózati forgalom hamisítása).

Általánosságban az összegyűjtött rosszindulatú programok és PUP-ok bináris mintái néhány különböző általános üzleti modellt fedtek fel: „hasznos” programok, amelyek a felhasználó számítógépének a régi fájloktól történő megtisztítását ígérik az előfizetést követően; olyan játéktelepítő szimulátorok, amelyek kérik a felhasználó személyes adatait; és olyan ingyenes programok, amelyek hozzáférést kínálnak kalóztartalmat terjesztő platformokhoz, például BitTorrent tracker segítségével. A weboldalak azonosításának és a rosszindulatú szoftverek gyűjtésének két fordulója ígéretes eredményekkel szolgált az érzékeny személyes és azonosítható információk kicsalására szolgáló rosszindulatú programok terjesztésének és a pszichológiai manipuláció módszereinek megértésében. Továbbá az elmúlt években a mobilkészülékek növekvő népszerűsége nyilvánvalóvá vált a feltételezetten szerzői jogot sértő tartalommegosztó platformokon keresztül elérhető Android OS-re tervezett számos PUP észlelésének fényében. Az elemzések korrelációjának eredményeképpen arra a következtetésre jutottunk, hogy a szerzői jogot sértő weboldalakon keresztül terjesztett rosszindulatú programokkal való fenyegetettségek kifinomultabbak, mint amilyennek első pillantásra tűnhetnek. A felfedezett szoftverek közül néhány besorolható az alábbi kategóriákba: trójai program, reklámprogram, backdoor program vagy ügynök. Ezt súlyosbítja az a tény is, hogy számos speciális rosszindulatú programcsalád, mint például a WisdomEyes, a DealPly és a FileRepMalware is feltűnt. Továbbá az ilyen átfogó kategorizálás nemcsak a Microsoft Windowsra, hanem az Android platformra is egyaránt érvényes. A felhasználói eszközöket számos fenyegetés veszélyezteti, ideértve többek között az érzékeny hitelesítő adatok, személyes adatok, hardverkonfigurációs adatok ellopását, valamint a hálózati forgalom módosítását. Ezért az azonosított szoftverek hatással lehetnek a felhasználókra még akkor is, ha PUP-ok, különösen olyan esetekben, amikor olyan átlagos felhasználókról van szó, akik esetleg nem ismerik teljes mértékben az alapvető online biztonsági gyakorlatokat és intézkedéseket.

A tanulmány eredményeinek egyik példáját az alábbiak szemléltetik.

3. weboldal	9. weboldal	
A weboldal ráveszi a felhasználókat, hogy hamis játéktelepítőt használjanak; a felhasználó érzékeny információinak megszerzésének teljes folyamata megváltozott a rosszindulatú programok gyűjtésének első és második fordulója között. A szolgáltatás felhasználója olyan archívumot tölt le, amely játékkal kapcsolatos fájloknak álcázott tartalmakat tartalmaz, és nem egy kifejezetten binárisan végrehajtható fájl, amelyet bármilyen vírusirtó kártékonyként észlelhet. A titkosított archívum csak fájlnevekhez biztosít hozzáférést, nem pedig a fájlok lényegi tartalmához.	A weboldal szoftveres eszköz segítségével hozzáférést kínál torrent trackereken keresztül elérhető bármely videotartalomhoz. Ez az eszköz kevesebb felhasználói interakciót igényel a többi BitTorrent trackerhez képest. Csak néhány kattintás szükséges ahhoz, hogy ismeretlen forrásokból töltsön le tartalmat, miközben a felhasználó nincs védve, és azt sem tudja ellenőrizni, hogy mit tölt le.	(Android) A weboldal regisztráció nélkül biztosít hozzáférést számos ingyenes mobilalkalmazáshoz. Az egyik alkalmazás korlátlan hozzáférést biztosít tévéműsorok és filmek streameléséhez. Nincs kifejezett kérés arra vonatkozóan, hogy a felhasználó érzékeny adatokat vagy fizetési adatokat szolgáltasson a szerzői jogi védelem alatt álló videókhoz való hozzáférés megvásárlásához. A felhasználónak azonban ki kell kapcsolnia a biztonsági beállításokat, amely lehetővé teszi a nem hivatalos alkalmazáspiacról származó alkalmazások telepítését.

Módszertan

A kutatás elvégzéséhez megbízható módszertant kellett alkalmazni a címek és weboldalak kiválasztásának, valamint a rosszindulatú programok és PUP-ok példáinak észlelése és dokumentálása által előidézett, technikailag kihívást jelentő feladat kezelésére. A módszertan rövid áttekintését az alábbiakban ismertetjük:

1. Az UNICRI kutatásának I. fázisában a szellemi tulajdoni jogsértések európai megfigyelőközpontjával (a továbbiakban: megfigyelőközpont) együttműködve létrehoztak egy szakértői támogató csoportot annak érdekében, hogy tanácsot adjon a kutatás módszertanával, az elemzéshez használt weboldalak kiválasztásával, valamint a kutatás a projekt megvalósításának minden fázisában történő kiértékelésével kapcsolatban. A szakértői támogató csoport a megfigyelőközpont érdekeltjeinek, a jogosult szervezetek, a tudományos körök, a bűnüldözés és az uniós ügynökségek képviselőiből állt.

2. Ezzel párhuzamosan kiválasztották a kutatócsoportot. E jelentés keretében nem volt technikailag lehetséges[1] a kutatás elvégzése az összes uniós tagállamban, ezért a II. fázisban a 28 uniós tagállam közül véletlenszerűen 10 országot vettek mintául.

3. A III. fázisban népszerű filmek, televíziós műsorok, dalok és videojátékok kerültek azonosításra. A népszerűség magában foglalta az adatgyűjtési időszak kezdetén, 2017. június 23-án az egész világon elért népszerűséget, valamint a 10 mintául vett ország közül csak egy vagy több országban elért népszerűséget is. A tanulmány későbbi fázisaiban ezeket a mintául vett címeket módszeresen használták az online webes keresésekhez annak

[1] A kiválasztott országok száma közvetlen hatással van az elemzésre kiválasztott, feltételezetten szerzői jogot sértő weboldalak és az ezekhez tartozó bináris fájlok számára (növeli azt). Ezért az a döntés született, hogy csak az országok egy mintájára koncentrálnak, hogy képesek legyenek a tanulmány gyakorlati részének sikeres elvégzésére egy adott időkereten belül.

érdekében, hogy szerzői jogot sértő webhelyeket és mobilalkalmazásokat találjanak. Minden cím az alábbi kritériumok közül kettőnek vagy többnek felelt meg:

- népszerű az adatgyűjtés idején az Unió tagállamaiban;
- világszerte népszerű az adatgyűjtés idején;
- történelmileg világszerte népszerű; és
- filmnek, televíziós műsornak, dalnak vagy videójátéknak minősül.

Öt filmcímet, öt tévéműsorcímet, öt zeneszámcímet és öt videojátékcímet választottak ki, amely összesen 20 mintául vett címet eredményezett. Alapos figyelmet fordítottak az egyes címek népszerűségének azonosításához használt forrásokra, amely egy szisztematikus kiválasztási folyamatot foglalt magában annak biztosítására, hogy a forrásadatok elérhetőek legyenek az összes vagy a legtöbb tagállam számára.

4. A IV. fázisban azokat az internetes oldalakat azonosították, amelyek feltételezetten szerzői jogi védelem alatt álló, világszerte és/vagy a mintául vett 10 országban 2017. június 26-án – a rosszindulatú programok gyűjtésének első fordulójában – népszerű anyagokhoz biztosítottak illegális hozzáférést. A tanulmány egy későbbi fázisában ezeket a weboldalakat elemezték rosszindulatú programok és potenciálisan nemkívánatos programok jelenlétének kimutatása céljából.

   A feltételezetten szerzői jogot sértő weboldalak azonosítására szolgáló módszertant az I. fázisban meghatározott szakértői támogató csoport közreműködése, valamint az UNICRI által a meglévő szakirodalom áttekintése alapján fejlesztették ki. Kifejezetten úgy dolgozták ki, hogy olyan weboldalakat tartalmazó mintát hozzon létre, amelyek:

   - népszerűek az EU különböző tagállamaiban, széles körű földrajzi lefedettséget biztosítva;
   - a feltételezetten szerzői jogot sértő webhelyek különböző típusait jelentik, beleértve a streamelő weboldalakat, az összekötő weboldalakat, a hosztoló weboldalakat, a cyberlockereket és a torrentweboldalakat;
   - a feltételezetten szerzői jogot sértő tartalmak széles skáláját jelentik, beleértve a filmeket, tévéműsorcímeket, zenéket és videojátékokat; továbbá
   - azokat az internetes oldalakat jelentik, amelyekkel az átlagos internetfelhasználó találkozhat, amikor megpróbál feltételezetten szerzői jogot sértő anyaghoz hozzáférni.

   A feltételezetten szerzői jogot sértő weboldalak kiválasztására öt lépést alkalmaztak. Az első három lépést úgy tervezték, hogy azonosítsa a népszerű, feltételezetten szerzői jogot sértő weboldalakat az EU tagállamaiban. Ez a módszer azokat a forgatókönyveket utánozta, amelyek szerint egy átlagos felhasználó felkereshet feltételezetten szerzői jogot sértő weboldalakat anélkül, hogy megadná például egy film vagy dal címét. Az utolsó két lépést úgy alakították ki, hogy azonosítsa a feltételezetten szerzői jogot sértő weboldalakat, amelyekkel egy átlagos felhasználó találkozhat, amikor annak lehetőségét keresi, hogy egy konkrét népszerű címet töltsön le a weboldal meghatározása nélkül. Ez a lépés különösen fontos volt, tekintettel a keresési eredmények mérgezésében részt vevő, feltételezetten kártékony webhelyek jelenlétére, amelyek segítségével – a keresőmotorok optimalizálásán keresztül – kihasználják a népszerű témákat. A két megközelítés együtt lefedte a különböző módszereket, amelyekkel egy átlagos internetfelhasználó megpróbálná megtalálni a feltételezetten szerzői jogot sértő anyagot online.

   Hangsúlyt fektettek az eszközökön, például okostelefonokon és táblagépeken lévő mobilalkalmazásokra jellemző rosszindulatú programok és PUP-ok egyidejű elemzésére, amely az egyik legfontosabb, elterjedőben lévő számítástechnikai bűnözés általi fenyegetettség. Az elemzés az Android-eszközökre korlátozódott, mivel a meglévő szakirodalom szerint a rosszindulatú programok nagyobb számban vannak jelen az Androidos alkalmazás-áruházakban (pl. Google Play), mint az Apple iTunes áruházában. A módszertant úgy dolgozták ki, hogy olyan mobilalkalmazásokat tartalmazó mintát hozzon létre, amelyek:

- világszerte népszerűek az adatgyűjtés idején;
- különböző alkalmazástípusokat tartalmaznak (beleértve a streamelő alkalmazásokat, a torrentalkalmazásokat és a hosztoló alkalmazásokat);
- feltételezetten szerzői jogot sértő tartalmak széles skáláját tartalmazzák, illetve ezekhez hozzáférést biztosítanak (beleértve a filmeket, tévéműsorcímeket, zenéket és mobiltelefonos játékokat); továbbá
- megfelelnek annak, amivel egy átlagos mobilkészülék felhasználója találkozhat, amikor olyan alkalmazásokat próbál meg letölteni vagy használni, amelyek hozzáférést biztosítanak feltételezetten szerzői jogi védelem alatt álló tartalmakhoz.

5. Az V. fázisban rosszindulatú programokat és PUP-okat, valamint mobilalkalmazásokat gyűjtöttek az azonosított weboldalakon, amelyeket megfelelő kategorizálás céljából egy későbbi szakaszban vizsgálnak meg. Az adatgyűjtési fázis magában foglalta a 2017 nyarán végrehajtott rosszindulatú programok gyűjtésének és elemzésének két fordulóját. A rosszindulatúprogram-gyűjtés első fordulója 1 054 egyedi doménnevet eredményezett, a második forduló pedig 1 057 egyedi doménnévvel szolgált az EU 10 kiválasztott tagállamban. A rosszindulatú programokat az átlagos felhasználói élmény szimulálása érdekében manuálisan és automatikusan is gyűjtötték.

Manuális gyűjtés Ez a módszer az előző fázisban azonosított domének manuális áttekintését foglalta magában. A manuális gyűjtés segítségével a szakértő hirdetésekre való kattintás és adatokat igénylő weboldalakkal való interakció által képes volt egy átlagos internetfelhasználó élményének szimulálására.

Automatikus gyűjtés Ennek a módszernek keretében egy szakértő által tervezett automatikus keresőrobotot alkalmaztak, hogy kövesse a kijelölt, feltételezetten szerzői jogot sértő weboldalon lévő összes elérhető linket. Először, minden weboldal esetében, a keresőrobot információkat gyűjtött a kezdőlap linkjeiről. Másodszor a keresőrobot követte az összes másodlagos weboldalra mutató linket. Harmadszor a keresőrobot követte az összes harmadlagos weboldalra mutató linket. Minden egyes lépésnél a keresőrobot lekérdezte azokat a bináris fájlokat, amelyek érdekesnek bizonyultak a későbbi manuális elemzéshez, beleértve a lehetséges vagy feltételezett rosszindulatú programokat és potenciálisan nemkívánatos programokat. Ez a folyamat weboldalanként 1 000 linkig folytatódott.

6. A bináris fájlok összegyűjtését követően azokat egy biztonságos számítástechnikai környezetben elemezték, hogy megértsék belső funkcionalitásukat, továbbá hogy megfelelően kategorizálják őket. Nyílt forráskódú eszközök segítségével előzetes elemzésre került sor annak érdekében, hogy összevessék az eredményeket a kiberfenyegetettségi jelentésekkel. Az összegyűjtött szoftvermintákat az EMAS-nak továbbították elemzés céljából, az EMAS elemzését pedig ezt követően összehasonlították az előzetes eredményekkel.

A módszertan áttekintése

Észlelt rosszindulatú programok és PUP-ok mintái

2017. július 28-ával 5 240 (1 054 egyedi) weboldalt ellenőriztek automatikusan az első fordulóban, amely során összesen 617, összesen 47 GB-nyi releváns fájlt (zene, videó, torrentfájlok és szoftverek) kértek le. Ez a szétválogatás nélküli fájlkészlet további elemzést igényelt annak eldöntésére, hogy a gyűjtött fájlok közül melyek relevánsak a vizsgálat szempontjából. A szerzői jogot sértő weboldalak mintái mind a 10 mintául vett országban hasonlóak voltak az összes médiatípus (televíziós műsorok, filmek, zenék és videojátékok) esetében. Ennek eredményeként Belgiumot véletlenszerűen választották ki a mintául vett országok közül, és minden, Belgiumban szerzői jogot sértő weboldalként azonosított weboldalt manuálisan ellenőriztek kártékony vagy egyéb módon nemkívánatos szoftverek jelenlétének kimutatása céljából. 2017. augusztus 10-én, a második gyűjtési forduló után összesen 3 665 fájlt kértek le automatikusan minden ország weboldaláról, összesen 167 GB-nyi terjedelemben. Az összes ország esetében kinyert egyedi URL-ek száma az 5 606 weboldalból összesen 1 057 volt, ami lehetetlenné tette ezek manuális ellenőrzését.

Az összegyűjtött fájlok előzetes elemzése után 106 egyedi bináris fájlt nyertek ki MS Windows-ra, Androidra és Mac OS-re a rosszindulatú programok gyűjtése mindkét fordulójának eredményeképp. Pontosabban az első fordulóban 41 fájlt választottak ki, a második fordulóban pedig 65-öt: 2-t Mac-re, 15-öt Androidra és 89-et MS Windows-ra. Ezekből a fájlokból 21 jól ismert kártékony programnak tekinthető, mivel több vírusirtógyártó is a VirusTotal platformon összegyűjtöttként jelöli ezeket. Ezek közé tartoznak a közvetlenül a kiválasztott, feltételezetten szerzői jogot sértő weboldalakról letöltött fájlok, valamint a letöltött fájlok végrehajtása során létrehozott fájlok. Ezt követően az összegyűjtött szoftvermintákat védett környezetben elemezték, majd továbbították az EMAS-nak a lehetséges kártékony tevékenységek magasabb szintű elemzése céljából. Összesen 821 különböző kártékony eseményt fedeztek fel négy EMAS-jelentésben (Windows 7 SP1, Windows 7 SP1 64 bit, Windows 10 64 bit, Windows XP SP3) az

összes bináris fájl esetében. Néhány jelentésben nem szerepeltek gyanús tevékenységek, és néhány közülük akár 10 korábban ismert kártékony tevékenységet is tartalmazott. A tanulmány utolsó szakaszában az előzetes elemzés és az EMAS-jelentések eredményeit vetették össze. Az eredmények mennyiségi összefoglalása az alábbi táblázatban található.

	1. forduló	**2. forduló**
Dátum	2017. július 28.	2017. augusztus 10.
Az EU 10 tagállamában felfedezett weboldalak	5 240	5 606
Egyedi weboldalak	1 054	1 057
Releváns fájlok	617	3 665[2]
A releváns fájlok mérete, GB	47	167
Továbbítva az EMAS részére		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Teljes méret, bájtok	175 600 117	522 991 095

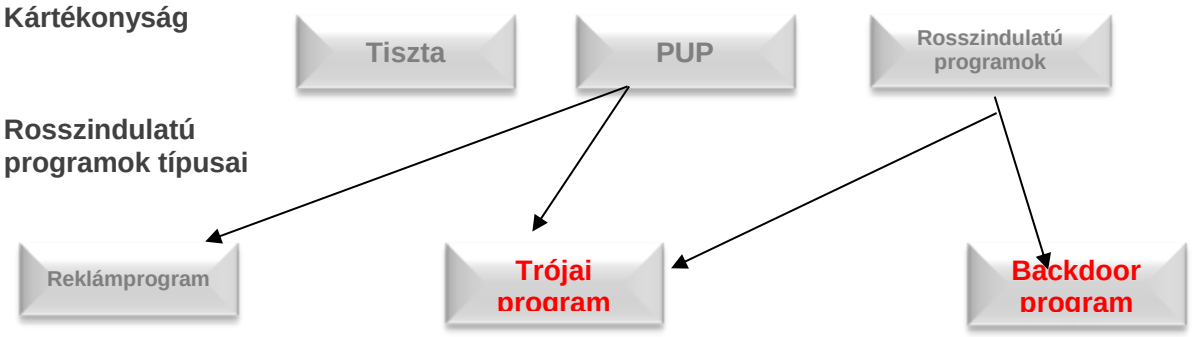
Europol Malware Analysis Solution (EMAS)

Az Europol Malware Analysis Solution (EMAS) egy dinamikus, automatizált, rosszindulatú programok elemzésére szolgáló megoldás, amelyet az Europol az Unió tagállamai számára biztosít. Az EMAS lehetőséget nyújt elemzésekről szóló jelentések készítésére, de a legforradalmibb jellemzője, hogy információt szolgáltat a rendőrnyomozók számára. Az automatikus keresztellenőrzések kapcsolatot mutathatnak a különböző országokban történt támadások és ugyanazzal a rosszindulatú programmal vagy ugyanazon rosszindulatú programcsalád mögött álló bűnszervezet által történő elkövetés között, amelyek ugyanazon doménekhez köthetők és az EU-n belül vagy kívül elvégzett különböző nyomozásokhoz kapcsolódnak. 2015-ben az EMAS teljes mértékben automatizálttá vált annak érdekében, hogy közvetlen hozzáférést biztosítson azon bűnüldöző szervek számára, amelyekkel az Europol működési megállapodást kötött. 2015-ben az EMAS-ban 525 108 fájlt elemeztek, amelyek közül 356 863-at kártékonynak minősítettek.

Amint az alábbi ábrán látható, az összegyűjtött bináris fájlokat általánosságban kártékonyságuk szerint a jóindulatú fájlok (fájlok, amelyek nem okoznak kárt), a PUP-ok és a kártékony, rosszindulatú programok kategóriáiba sorolták. Továbbá a PUP-okat nemcsak a Microsoft Windows-ban fedezték fel; az Android és a Mac OS esetében is megtalálták őket, ami azt jelentheti, hogy a rosszindulatú programok fejlesztői a lehető legtöbb felhasználóra próbálnak hatással lenni különböző platformokat használva. A PUP-ok és a rosszindulatú programok további kategóriákba sorolhatók a főbb rosszindulatú programtípusok (trójai programok, reklámprogramok és backdoor programok) alapján. A megtalált szoftverek többsége a PUP-ok kategóriájába esett. A PUP-ok működését a következő üzleti modellek egyikével lehet összefüggésbe hozni: személyes és bankszámlaadatokat igénylő hamis játéktelepítők, „hasznos” programok letöltése, amelyek arra kényszerítik a felhasználókat, hogy előfizessenek a fizetett verzióra, illetve ingyenes programok telepítése szerzői jogot sértő platformokhoz való hozzáférés céljából. Ezek az alkalmazások veszélyeztethetik a felhasználók személyes adatait, valamint a számítógép konfigurációját.

[2] Az 1. és a 2. forduló közötti számbeli különbség magyarázata, hogy az automatizált gyűjtés 2. fordulója során voltak olyan weboldalak, amelyek mindegyik weblapjukon több fájlkészletet is közzétettek.

Pszichológiai manipulációs trükkök révén különféle típusú személyes adatokat, például bankkártyaadatokat, személyazonosításra alkalmas adatokat és közösségimédia-fiókokra vonatkozó hitelesítő adatokat is közzétehetnek. Hasonlóképpen a kutatás 15 Androidos alkalmazást azonosított harmadik féltől származó alkalmazáspiacokról, és az előzetes elemzés után arra a következésre jutottak, hogy az ilyen alkalmazások részt vehetnek a szerzői jogot sértő tartalmak terjesztésében és a személyes adatok közzétételében.



Végfelhasználókat fenyegető veszélyek

A weboldal azonosításának és a rosszindulatú programok elemzésének két fordulója során nem találtak zsaroló bináris fájlokat. Általánosságban az összegyűjtött rosszindulatú szoftverek többsége trójai programként jellemezhető, ami azt jelenti, hogy a weboldalakon jóindulatú, általánosan használt vagy népszerű szoftverként jelenhetnek meg, míg a valóságban képesek ellopni vagy nyilvánosságra hozni a személyes információkat. A tapasztalatlan felhasználó nagyfokú bizalmat tanúsíthat a szoftver iránt, és lehet, hogy nem vesz észre semmilyen rendellenességet. Ráadásul az ilyen szoftver statikus analízise és dinamikus viselkedési megfigyelései nem feltétlenül fedik fel a teljes funkcionalitást forráskód nélkül. A rosszindulatú programok előzetes elemzését követően az EMAS-elemzés konkrétabb kártékony tevékenységeket mutatott. Jelentős hatása lehet a szoftver végfelhasználó számítógépére történő telepítésének, ami nemcsak anyagi veszteségeket okoz, hanem személyesadat-lopást és egyéb nemkívánatos hozzáférési és ellenőrzési kockázatokat is magával vonhat. Ezek a tevékenységek várhatóan személyes adatok gyűjtését és továbbítását eredményezik harmadik felek számára titkosított vagy nyílt szövegformátumban. Ilyen adatok lehetnek például a böngészőből származó bankszámla-hitelesítő adatok, a számítógép hardver- és szoftverkonfigurációjának részletei vagy lényegében bármi, ami a billentyűzeten kerül begépelésre.

ROSSZINDULATÚ PROGRAMOK AZONOSÍTÁSA ÉS ELEMZÉSE KIVÁLASZTOTT, FELTÉTELEZETTEN SZERZŐI JOGOT SÉRTŐ WEBOLDALAKON

VEZETŐI ÖSSZEFOGLALÓ

2018. szeptember