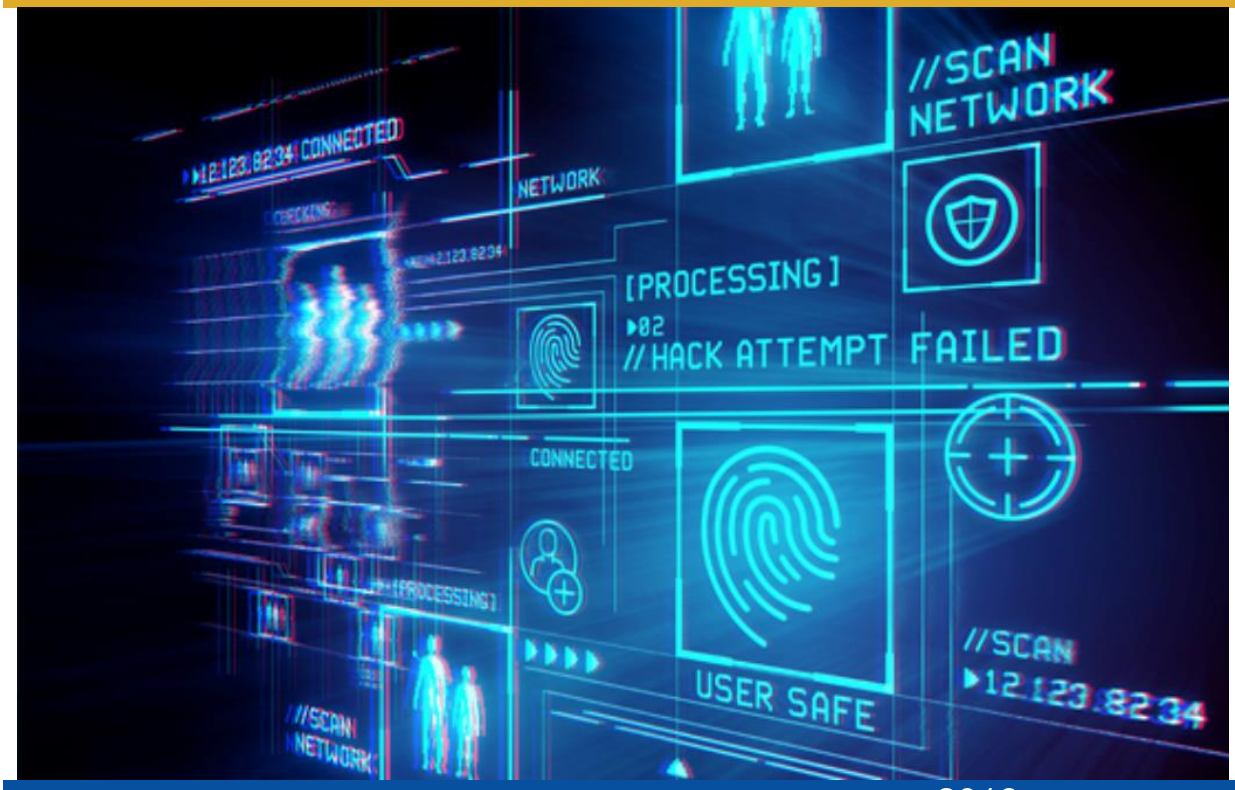
EUIPO
СЛУЖБА НА ЕВРОПЕЙСКИЯ СЪЮЗ ЗА ИНТЕЛЕКТУАЛНА СОБСТВЕНОСТ

ОТКРИВАНЕ И АНАЛИЗИРАНЕ НА ЗЛОВРЕДЕН СОФТУЕР В ИЗБРАНИ УЕБСАЙТОВЕ, ЗА КОИТО ИМА ПОДОЗРЕНИЯ, ЧЕ НАРУШАВАТ АВТОРСКОТО ПРАВО

КРАТКО ИЗЛОЖЕНИЕ



септември 2018 г.

Резюме

Съдържанието, за което има подозрения, че нарушава авторското право, представлява сериозно нарушение на правата върху интелектуалната собственост. Има уебсайтове, които споделят такова съдържание публично, понякога дори безплатно, без регистрация. Наред с това съдържание уебсайтовете обичайно разпространяват различни видове зловреден софтуер и потенциално нежелани програми (англ.: PUPs), като подвеждат потребителите да изтеглят и зареждат тези файлове. Проучването съдържа преглед на най-актуалните примери за зловреден софтуер и потенциално нежелани програми, които се намират в уебсайтове, за които има подозрения, че нарушават авторското право. Тези програми използват измамни техники и социално инженерство, като например празни инсталационни файлове на игри и привидно „полезен“ софтуер, за да подвеждат крайните потребители да разкриват чувствителна информация за себе си. По време на проучването бяха открити различни потенциално нежелани програми, като например „полезен“ софтуер, фалшиви инсталационни файлове за игри и клиенти за платформи за видеострийминг. Не е задължително този софтуер да крие пряка опасност за софтуера или хардуера на потребителя. Чрез трикове на социалното инженерство, обаче, потребител може да бъде убеден да разкрие чувствителна лична информация или информация от платежни карти. Освен това е възможно към други страни да изтече информация за самия компютър без изричното съгласие на потребителя.

Изследователски екип

Изследователският екип включваше Франческа Боско, програмен служител на Междурегионалния научноизследователски институт на ООН по престъпленията и правосъдието (UNICRI) и д-р Андрий Шалагинов, научен сътрудник по информационна сигурност в Отдела за информационна сигурност и комуникационни технологии (Група за цифрова криминалистика), Факултет за информационни технологии и електроинженерство, Норвежки университет за наука и технологии.

Отказ от отговорност

В този контекст следва да се подчертае, че единствената цел на изследването беше да се определят техническите характеристики на зловредния софтуер и потенциално нежелани програми, открити в рамките на проучването, на които биха могли да попаднат потребителите на интернет, търсещи съдържание, за което има подозрения, че нарушава авторското право. Документираните извадки от зловреден софтуер и потенциално нежелани програми не могат да се считат за изчерпателни, нито целта на проучването (или резултатите от него) е била да се предостави оценка на цялостната вероятност или риск от заразяване със зловреден софтуер и потенциално нежелани програми, на който потребителите на интернет са изложени при търсене на материали, за които има подозрения, че нарушават авторското право.

Предговор

Онлайн дейностите, за които има подозрения, че нарушават авторското право, могат да се финансират по множество начини, включително абонаментни такси, дарения, плащане за допълнителни услуги и приходи от реклама чрез показване онлайн.

Не всички средства за финансиране, обаче, са толкова ефикасни, както посочените примери. От години разпространяването на заразяване със зловреден софтуер и други видове потенциално нежелани програми (англ.: PUPs) е от ключово значение във връзка с финансирането на дейности в интернет, за които има подозрения, че нарушават авторското право.

Обикновените потребители на интернет започват да осъзнават рисковете от заразяване, когато осъществяват достъп до уебсайтове или мобилни приложения, за които има подозрения, че нарушават авторското право.

Докладът на Службата на Европейския съюз за интелектуална собственост (EUIPO) от 2015 г. относно младежта по въпросите на интелектуалната собственост показа, че 52 % от младежите считат, че безопасността в уебсайтовете е важна при осъществяване на достъп до онлайн съдържание. Общо 78 % от младежите са заявили, че биха се замислили сериозно, ако знаят, че има риск компютърът или устройството да е заразено с вируси или зловреден софтуер. Общо 84 % са заявили, че биха се замислили сериозно, ако знаят, че има риск информацията от кредитната им карта да бъде откраднатa.

В изследването на това проучване Службата се зае с много технически сложна задача, а именно да открие и документира примери за зловреден софтуер и потенциално нежелани програми, на които потребителят на интернет би могъл да попадне, осъществявайки достъп до популярни пиратски филми, музика, видеоигри и телевизионни заглавия.

В този контекст следва да се подчертае, че единствената цел на изследването беше да се определят техническите характеристики на зловредния софтуер и потенциално нежеланите програми, открити в рамките на проучването, на които биха могли да попаднат потребителите на интернет, търсещи съдържание, за което има подозрения, че нарушава авторското право. Документираните извадки от зловреден софтуер и потенциално нежелани програми не могат да се считат за изчерпателни, нито целта на проучването (или резултатите от него) е била да се предостави оценка на цялостната вероятност или риск от заразяване със зловреден софтуер и потенциално нежелани програми, на който потребителите на интернет са изложени при търсене на материали, за които има подозрения, че нарушават авторското право.

Изследването беше извършено на няколко етапа в тясно сътрудничество с Европейския център за борба с киберпрестъпността (EC3) в Европол.

Резултатите показват множество заплахи от различни видове зловреден софтуер и потенциално нежелани програми, на които потребителите на интернет могат да попаднат, търсейки съдържание, за което има подозрения, че нарушава авторското право. Повечето от документирания зловреден софтуер и потенциално нежелани програми могат да се определят като „троянски коне“ или друг нежелан софтуер, който може да получи непозволен достъп до личните данни на потребителите на интернет. Тези примери ще бъдат от значение и интерес не само за общността на носителите на права върху ИС, но и за правоприлагащите органи и, не на последно място, за потребителите, които са загрижени за осъществяването на достъп до личните им данни без тяхно разрешение.

Кратко изложение

Проучването съдържа преглед на най-актуалните примери за зловреден софтуер и потенциално нежелани програми (англ.: PUPs), които се намират в уебсайтове, за които има подозрения, че нарушават авторското право. Тези програми използват измамни техники и социално инженерство, като например празни инсталационни файлове на игри и привидно „полезен“ софтуер, за да заблуждават крайните потребители да разкриват чувствителна информация за себе си.

Целта на това проучване е да се открие зловредният или изобщо нежелан софтуер, разпространяван в определени уебсайтове, за които има подозрения, че нарушават авторското право, и да се категоризират откритите извадки в съответствие с различните таксономии на зловреден софтуер. В този контекст следва да се подчертае, че единствената цел на проучването беше да се определят техническите характеристики на зловредния софтуер и потенциално нежелани програми, открити в рамките на изследването, на които биха могли да попаднат потребителите на интернет, търсещи съдържание, за което има подозрения, че нарушава авторското право. Документираните извадки от зловреден софтуер и потенциално нежелани програми не могат да се считат за изчерпателни, нито целта на изследването (или резултата от него) е била да се предостави оценка на цялостната вероятност или риск от заразяване със зловреден софтуер и потенциално нежелани програми, на който потребителите на интернет са изложени, когато търсят материали, за които има подозрения, че нарушават авторското право. За целта на това изследване, телевизионни програми, филми, музика и видеоигри се считат за съдържание, защитено от авторско право.

Резултати от проучването

Съдържанието, за което има подозрения, че нарушава авторското право, представлява сериозно нарушение на правата върху интелектуална собственост. Има уебсайтове, които споделят такова съдържание публично, понякога дори безплатно, без регистрация. Наред с такова съдържание уебсайтовете обичайно разпространяват различни видове зловреден софтуер и потенциално нежелани програми, като подвеждат потребителите да изтеглят и зареждат такива файлове. При идентифицирането на уебсайта, базирано на класацията „Топ 500“ на Alexa, в допълнение към симулацията, при която средностатистически потребител извършва търсене в добре познати търсачки като например Google, Yahoo и Bing, бе установено, че наборът от уебсайтове се е променил между двата цикъла на проучването. Тази промяна вероятно се дължи на усилията на търсачките да премахват връзки към уебсайтове, за които има подозрения, че нарушават авторското право, докато продължават да се създават нови уебсайтове, за които има подозрения, че нарушават авторското право. Във връзка с идентифицирането на уебсайтове една интересна констатация е свързана с факта, че по-голямата част от уебсайтовете се хостват в Съединените щати или имената на домейните им са свързани с хостинг там. Тъкмо обратното, много малко се намират на сървъри в ЕС. Освен това .com и .net са имената на домейни от първо ниво, най-често използвани за уебсайтове, за които има подозрения, че нарушават авторското право. Това може да се дължи на факта, че за разлика от специфичните за държавите домейни, за тези може да не е необходимо потребителят да се идентифицира с паспорт или други идентификационни документи. Средно 20 % от новите уебсайтове са били добавени, а 20 % от старите уебсайтове са били премахнати между двата цикъла на идентифициране. Освен това близо 8 % от идентифицираните при двата цикъла уебсайтове са определени от платформата VirusTotal като зловредни. С помощта на различни системи за управление на съдържанието създаването на уебсайт и предоставянето на съдържание, дори и злонамерени приложения, на потребителите вече е безпроблемно.

Преди събирането на информация за зловреден софтуер, в рамките на проучването беше извършена документна проверка на зловредните заплахи през 2017 г. и категоризация на съвременното технологично равнище. Натрупаните знания бяха използвани също и по време на анализа на зловреден софтуер с цел следване на възприетите от общността принципи за откриване на видове и семейства зловреден софтуер. Бяха събрани общо 106 файла по време на двата цикъла на събиране на данни. Те включват файлове, изтеглени пряко от уебсайтове, за които има подозрения, че нарушават авторското право, както и файлове, създадени при обработването на изтеглените файлове. По време на проучването бяха открити различни потенциално нежелани програми, като например „полезен“ софтуер, фалшиви инсталационни файлове за игри и клиенти за платформи за видеострийминг. Не е задължително такъв софтуер да крие пряка опасност за софтуера или хардуера на потребителя. Чрез трикове на социалното инженерство, обаче, потребител може да бъде убеден да разкрие чувствителна лична информация или информация от платежни карти Освен това е възможно към други страни да изтече информация за самия компютър без изричното съгласие на потребителя.

Събраният зловреден софтуер е анализиран първоначално с инструменти с отворен код, за да бъде разбрана вътрешната логика, да се открият възможни зловредни дейности и да се оцени значението им за настоящото проучване на зловреден софтуер. В допълнение към предварителния анализ с инструменти с отворен код извадките от събран зловреден софтуер бяха анализирани от платформата „Решение на Европол за анализ на зловреден софтуер“ (EMAS). Това доведе до откриване на голям брой различни артефакти и злонамерени дейности. Докладите на EMAS включват всеобхватен анализ на файлове посредством четири версии на MS Windows, при което се извършва щателно регистриране на трафик по мрежите, извиквания на функции и действия по диска с цел допълнителен анализ. Освен това платформата разкрива подозрителни действия, засечени по време на рутинно изпълнение на файла. След анализиране на всички доклади EMAS е открила 35 вида злонамерени дейности, разпределени в 17 класа злонамерени събития. Те варират от общи аномалии (като например стартиране на системни процеси или търсене на процеси в памети) до несъмнено злонамерени действия (като например следящ клавиатурата софтуер, руткит и подправяне на трафик в мрежата).

Като цяло двоичните извадки, събрани от зловреден софтуер и потенциално нежелани програми, разкриха няколко различни общи бизнес модела: „полезни“ програми, за които се счита, че почистват старите файлове на компютъра на потребителя при платен абонамент; симулатори на инсталационни файлове на игри, които изискват личните данни на потребителя и безплатни програми, предлагащи достъп до платформи, които разпространяват съдържание, което е обект на пиратство, например чрез тракера BitTorrent. Двата цикъла на идентифициране на уебсайтове и събиране на зловреден софтуер завършиха с обещаващи резултати от гледна точка на разбиране на методите на разпространение на зловреден софтуер и социално инженерство за подвеждане на потребителите да споделят чувствителна лична и идентифицираща информация. Освен това засилващата се популярност на мобилните устройства през последните години е очевидна в светлината на откриването на множество налични потенциално нежелани програми за операционната система Android в платформи за разпространение на съдържание, за които има подозрения, че нарушават авторското право. В резултат на съпоставяне на анализите беше достигнато до заключението, че картината на заплахите от зловреден софтуер, разпространяван чрез уебсайтове, които нарушават авторското право, е по-сложна, отколкото изглежда на пръв поглед. Част от открития софтуер може допълнително да се класифицира като „троянски коне“, рекламен софтуер, „бекдор“ и агент. Това се подкрепя от факта, че са открити също и много специфични семейства зловреден софтуер, като например WisdomEyes, DealPly и FileRepMalware. Освен това такава всеобхватна категоризация напълно важи и за платформата Android, а не само за Microsoft Windows. Има широк набор от заплахи за активите на потребителите, включително, но не само кражба на чувствителни идентификационни данни, лични данни, информация за конфигурация на хардуер и изменение на трафика в мрежата. Следователно, макар че

откритият софтуер са потенциално нежелани програми, те все пак могат да оказват въздействие върху потребителите, особено в случаи, в които средностатистическият потребител не познава достатъчно добре основните практики и мерки за сигурност онлайн.

По-долу е показан пример за констатациите от проучването.

Уебсайт 03	Уебсайт 09	Уебсайт 08
Уебсайтът заблуждава потребителите да използват фалшив инсталационен файл за игра; целият процес по придобиване на чувствителната информация на потребителя е променен между първия и втория цикъл на събиране на зловреден софтуер. Потребителят на тази услуга изтегля архив, чието съдържание е прикрито като файлове, свързани с играта, а не като изрично двоичен изпълним файл, който може да бъде засечен от всяка антивирусна програма като зловреден. Криптираният архив дава достъп само до имената на файловете, но не и до реалното им съдържание.	Уебсайтът дава достъп до всеки вид видеосъдържание, достъпно чрез торент тракери с помощта на софтуерен инструмент. За този инструмент са необходими по-малко взаимодействия с потребителя в сравнение с BitTorrent тракерите. Съдържание от неизвестни източници може да се изтегли само с няколко щраквания, а потребителят нито е защитен, нито има контрол над това, което се изтегля.	(Android) Уебсайтът предоставя достъп до редица безплатни мобилни приложения без регистрация. Едно приложение предоставя неограничен достъп до стрийминг на телевизионни програми и филми. Няма изрично искане за предоставяне на чувствителна информация или информация за плащане с цел купуване на достъп до защитени с авторско право видеоклипове. Необходимо е обаче потребителят да деактивира настройките за сигурност, с което ще позволи инсталирането на приложения с произход, различен от този от официалния пазар на приложения.

Методология

За извършване на изследването беше необходимо да се приеме стабилна методология, предназначена за провеждане на подбор на заглавия и уебсайтове, както и да се предприеме технически сложната задача по откриване и документиране на примерите за открит зловреден софтуер и потенциално нежелани програми. По-долу е описан кратък преглед на методологията:

1. На етап 1 от изследването на UNICRI в сътрудничество с Европейска обсерватория за нарушенията на правата на интелектуална собственост (Обсерваторията) беше създадена експертна помощна група, която да предоставя съвети относно методологията на изследването, подбора на използваните за анализ уебсайтове, и за оценяване на извършваното изследване на всеки етап от изпълнението на проекта. Експертната помощна група беше съставена от представители на заинтересованите страни от Обсерваторията, организации на носители на права, академичните среди, правоприлагащи органи и агенции на ЕС.

2. Успоредно с това беше избран изследователски екип. В рамките на настоящия доклад нямаше техническа възможност[1] да се изследват всички държави — членки на ЕС;

[1] Броят на избраните държави ще има пряко въздействие (в посока увеличение) върху броя на избраните уебсайтове, за които има подозрения, че нарушават авторското право, и съответните двоични файлове, които ще се анализират. Следователно беше решено да се акцентира единствено върху извадка от държави, които да могат успешно да извършват практическата част на проучването в рамките на определен период.

следователно на произволен принцип бяха избрани 10 примерни държави от 28-те държави — членки на ЕС на етап II.

3. На етап III бяха определени популярни филми, телевизионни програми, песни и видеоигри. Популярността включваше световна популярност, както и популярност само в една или повече от 10-те примерни държави към началото на периода на събиране на данни, 23 юни 2017 г. В последващите етапи от проучването тези примерни заглавия бяха използвани систематично в търсения онлайн в мрежата с цел да се открият уебсайтове и приложения, които нарушават авторското право. Всяко заглавие отговаряше на два или повече критерия:

   - популярно в момента на събиране на данни в държавите-членки на ЕС;
   - популярно в момента на събиране на данни в световен мащаб;
   - популярно в исторически план в световен мащаб; и
   - категоризирано като филм, телевизионна програма, песен или видеоигра.

   Бяха избрани пет филмови заглавия, пет телевизионни заглавия, пет музикални заглавия и пет заглавия на видеоигри, в резултат на което бяха подготвени общо 20 примерни заглавия. Бяха внимателно подбрани източниците, използвани за идентифициране на популярността на дадено заглавие, за което беше използван процес на систематичен подбор за гарантиране, че за всички или повечето държави членки ще бъдат налични данни от източника.

4. По време на етап IV бяха определени уебсайтове, за които има подозрения, че предоставят незаконен достъп до защитени с авторско право материали, популярни в целия свят и/или сред 10-те примерни държави, към 26 юни 2017 г. (първи цикъл на събиране на зловреден софтуер). На по-късен етап от проучването тези уебсайтове бяха анализирани за наличие на зловреден софтуер и потенциално нежелани програми.

   Методологията за идентифициране на уебсайтове, за които има подозрения, че нарушават авторското право, беше разработена с помощта на експертната помощна група, определена на етап I, както и въз основа на преглед на съществуващата литература, извършен от UNICRI. Тя беше специално изготвена, за да се генерира извадка от уебсайтове, които:

   - са популярни в различните държави-членки на ЕС, гарантирайки широко географско покритие;
   - представляват различни видове уебсайтове, за които има подозрения, че нарушават авторското право, включително уебсайтове за стрийминг, свързващи уебсайтове, уебсайтове за хостинг услуги, уебсайтове, предлагащи „файл хостинг“ и уебсайтове за торенти;
   - представляват широк набор от съдържание, за което има подозрения, че нарушава авторското право, включително филми, телевизионни заглавия, музика и видеоигри; и
   - представляват уебсайтове, на които би попаднал средностатистическият потребител на интернет при опита да осъществи достъп до материал, за който има подозрения, че нарушава авторското право.

   Бяха използвани пет стъпки за избор на уебсайтове, за които има подозрения, че нарушават авторското право. Първите три стъпки имаха за цел определяне на най-популярните уебсайтове, за които има подозрения, че нарушават авторското право, в държавите-членки на ЕС. Методът наподобяваше сценариите, при които средностатистически потребител може да търси уебсайтове, за които има подозрения, че нарушават авторското право, без да посочва например заглавие на филм или песен. Последните две стъпки имаха за цел да се установят уебсайтовете, за които има подозрения, че нарушават авторското право, на които средностатистическият

потребител може да попадне, когато търси начини за изтегляне на дадено популярно заглавие, без да посочва уебсайт. Тази стъпка беше от особено голямо значение предвид наличието на уебсайтове, за които има подозрения, че нарушават авторското право чрез „заразяване“ на резултатите от търсенето като експлоатират популярни теми посредством оптимизиране на търсачките. Двата подхода заедно обхващаха различните начини, по които средният потребител на интернет би се опитал да намери онлайн материал, за който има подозрения, че нарушава авторското право.

Беше поставен акцент върху паралелния анализ на зловреден софтуер и потенциално нежелани програми, специфични за мобилни приложения на устройства като смартфони и таблети, като една от ключовите възникващи заплахи от престъпления в киберпространството. Анализът беше ограничен до Android устройства, тъй като в съществуващата литература фигурират данни за по-голямо наличие на зловреден софтуер в магазините за Android приложения (т.е. Google Play), отколкото в магазина на Apple iTunes. Методологията беше изготвена, за да се генерира извадка от мобилни приложения, които:

- са популярни в момента на събиране на данни в световен мащаб;
- представляват различен вид приложения (с цел включване на приложения за стрийминг, приложения за торенти и приложения за хостинг услуги);
- съдържат или предоставят достъп до широк набор от съдържание, за което има подозрения, че нарушава авторското право (с цел включване на филми, телевизионни предавания, музика и мобилни игри); и
- представляват това, на което средностатистическият потребител на мобилно устройство ще попадне в опита си да изтегли или използва приложение, улесняващо достъпа до съдържание, за което има подозрения, че нарушава авторското право.

5. Етап V включваше събиране на зловреден софтуер и потенциално нежелани програми в допълнение към мобилни приложения в определените уебсайтове, за които на по-късен етап да бъде извършена проверка с цел да бъдат правилно категоризирани. Етапът на събиране на данни включваше два цикъла от събиране и анализ на зловреден софтуер, които бяха проведени през лятото на 2017 г. Първият цикъл от събиране на зловреден софтуер завърши с 1054 самостоятелни имена на домейни, а вторият - с 1057 самостоятелни имена на домейни в 10 избрани държави-членки на ЕС. Зловреден софтуер беше събиран и ръчно, и автоматизирано, с цел симулиране на опита на средностатистическия потребител.

Ръчно събиране. Този метод включваше ръчно преглеждане на домейните, определени на предишния етап. Посредством ръчно събиране, експертът имаше възможността да симулира опита на средностатистическия интернет потребител, щраквайки върху реклами и реагирайки на уебсайтове, изискващи въвеждане на данни.

Автоматично събиране. Този метод включваше автоматизирана програма за уеб обхождане, проектирана от експерт, която да проследява всички налични връзки на определен уебсайт, за който има подозрения, че нарушава авторското право. Първо, на който и да е уебсайт, програмата за уеб обхождане събираше информация от връзките в началната страница. Второ, програмата за уеб обхождане проследяваше всяка от тези връзки към вторични уебсайтове. Трето, програмата за уеб обхождане проследяваше всяка от тези връзки към третични уебсайтове. На всяка стъпка програмата за уеб обхождане извличаше двоични файлове, които биха били от интерес за последващ ръчен анализ, включително потенциален или предполагаем зловреден софтуер или потенциално нежелани програми. Този процес продължи за до 1000 връзки на уебсайт.

6. След събиране на двоичните файлове те бяха анализирани в безопасна изчислителна среда, за да се установи вътрешната им функционалност и за да се категоризират правилно. Беше извършен предварителен анализ посредством инструменти с отворен

код, за да се осигури възможност за свързване на констатациите с доклади за киберзаплахи. След това събраните извадки от софтуер бяха предоставени за анализ на EMAS, след което анализът на EMAS беше сравнен с предварителните резултати.

Преглед на методологията

Извадки от засечен зловреден софтуер и потенциално нежелани програми

Към 28 юли 2017 г. 5240 уебсайта (1054 самостоятелни) бяха автоматично проверени по време на първия цикъл от събирането, като от общо 47 GB бяха извлечени 617 съответни файлове (музикални, видео, торент файлове и софтуер). Беше необходим допълнителен анализ на този несортиран набор от файлове, за да се определи кои от събраните файлове са от значение за проучването. Извадките от уебсайтове, нарушаващи авторското право, бяха сходни между всички 10 примерни държави по отношение на всеки от видовете носители (телевизионни програми, филми, музика и видеоигри). В резултат на това от примерните държави на случаен принцип беше избрана Белгия и всички уебсайтове, определени като нарушаващи авторското право за Белгия, бяха ръчно проверени за наличие на зловреден или нежелан, поради друга причина, софтуер. На 10 август 2017 г. след втория цикъл на събиране от уебсайтове от всички държави автоматично бяха извлечени общо 3665 файла с общ размер 167 GB. Общият брой самостоятелни URL адреси, извлечени за всички държави, беше 1057 от 5606 уебсайта, което направи невъзможна ръчната проверка на всички тях.

След предварителен анализ на събраните файлове бяха извлечени 106 самостоятелни двоични файла за MS Windows, операционна система Android и Mac OS в резултат на двата цикъла от събиране на зловреден софтуер. По-специално, по време на първия цикъл бяха избрани 41 файла, а по време на втория - 65 файла, и по-специално: 2 за Mac OS, 15 за Android и 89 за MS Windows. 21 от тези файлове могат да се считат за добре известни зловредни програми, определени от множество търговци на антивирусни продукти като

обобщени от платформата VirusTotal. Те включват файлове, изтеглени пряко от избрани уебсайтове, за които има подозрения, че нарушават авторското право, както и файлове, създадени при обработването на изтеглените файлове. След това събраните извадки от софтуер бяха анализирани в изолирана среда и предоставени на EMAS за по-подробен анализ за възможни злонамерени действия. Като цяло в рамките на четири доклада на EMAS бяха открити 821 самостоятелни злонамерени събития (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3) за всички двоични файлове. В някои от докладите не бяха посочени подозрителни действия, а в други — до 10 вече познати злонамерени действия. По време на последния етап от изследването резултатите от предварителния анализ и тези от докладите на EMAS бяха съпоставени. Количественото резюме на резултатите е посочено в таблицата по-долу.

	Цикъл 1	**Цикъл 2**
Дата	28 юли 2017 г.	10 август 2017 г.
Открити уебсайтове в 10 държави от ЕС	5240	5606
Самостоятелни уебсайтове	1054	1057
Съответни файлове	617	3665[2]
Размер на съответните файлове, GB	47	167
Предоставени на EMAS		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Общ размер, байтове	175 600 117	522 991 095

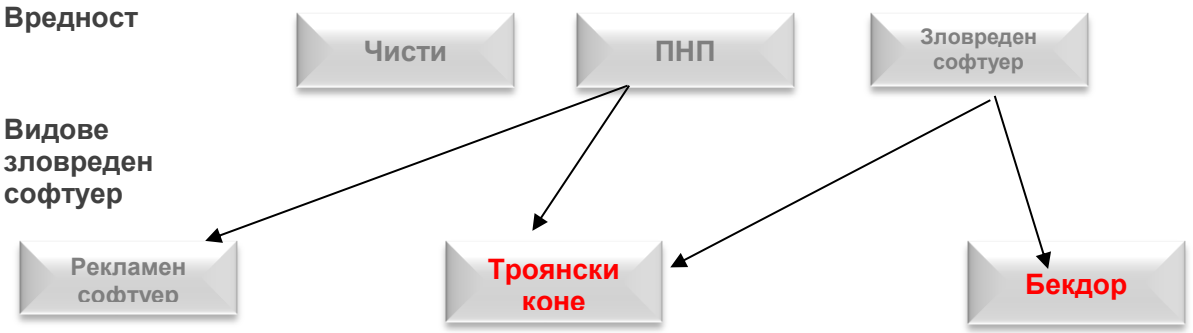
Решение на Европол за анализ на зловреден софтуер (EMAS)

Решението на Европол за анализ на зловреден софтуер (EMAS) е динамично автоматизирано решение за анализ на зловреден софтуер, предоставяно от Европол на държавите-членки на ЕС. EMAS дава възможност за създаване на доклади от анализи, но най-революционната му характеристика е създаване на разузнавателни данни за разследващи полицаи. Чрез автоматични кръстосани проверки могат да бъдат показани връзките между атаки, извършвани в различни държави с един и същ зловреден софтуер, или с една и съща престъпна организация, стояща зад същото семейство зловреден софтуер. През 2015 г. EMAS се автоматизира изцяло, за да се даде възможност за пряк достъп до правоприлагащи страни, с които Европол има оперативни споразумения. През 2015 г.: в EMAS бяха анализирани 525 108 файла, 356 863 от които бяха определени като зловредни.

Както е показано на фигурата по-долу, събраните двоични файлове като цяло могат да се категоризират по своята вредност като безвредни (файлове, които не нанасят вреди), потенциално нежелани програми и опасен зловреден софтуер. Освен това потенциално нежелани програми бяха открити не само за Microsoft Windows, а и за операционните системи Android и Mac OS, което предполага, че разработчиците на зловреден софтуер се опитват за засегнат възможно най-много потребители, като използват различни платформи.

[2] За да се обясни разликата в цифрите между цикъл 1 и цикъл 2, по време на цикъл 2 на автоматично събиране имаше уебсайтове, които публикуваха множество набори от файлове на всяка от своите страници.

Потенциално нежеланите програми и зловредният софтуер могат да се диференцират още и въз основа на главните видове зловреден софтуер, тоест, „троянски коне“, рекламен софтуер и „бекдор“. По-голямата част от установения софтуер попадаше в категорията на потенциално нежелани програми. Функционирането на потенциално нежеланите програми може да бъде свързано с един от следните бизнес модели: фалшив инсталационен файл за игра, който изисква лична информация и информация от банкова сметка, изтегляне на „полезни“ програми, които принуждават потребителите да закупят абонамент за платена версия, или инсталиране на безплатни програми за достъп до нарушаващи авторското право платформи. Тези приложения може да компрометират личните данни и конфигурацията на компютъра на потребителя. Чрез трикове на социалното инженерство, могат да бъдат разкрити различни видове лични данни, като например информация от платежни карти, информация, която позволява установяване на самоличността, и идентификационни данни за профил в социалните мрежи. По подобен начин в изследването бяха открити 15 Android приложения от пазари за приложения на трети страни, а след предварителния анализ беше заключено, че е възможно тези приложения да се използват за разпространение на нарушаващо авторското право съдържание и разкриване на лични данни.



Заплахи за крайните потребители

По време на два цикъла на идентифициране на уебсайтове и анализ на зловреден софтуер не бяха открити двойни спомагателни вируси. Като цяло по-голямата част от събрания зловреден софтуер може да се характеризира като „троянски коне“, което означава, че те могат да бъдат представени на уебсайтовете като безвреден често използван или популярен софтуер, докато реално могат да крадат или разкриват лична информация. Неопитният потребител може да има висока степен на доверие в софтуера и може да не забележи нещо необичайно. Освен това чрез статичен анализ и динамични поведенчески наблюдения на такъв софтуер може да не се разкрие пълната функционалност без наличие на изходен код. След предварителния анализ на зловредния софтуер анализът на EMAS показа по-специфични злонамерени действия. Последиците от наличието на такъв инсталиран софтуер на компютъра на краен потребител могат да бъдат значителни и да нанесат не само финансови загуби, но и кражба на лични данни и други рискове, свързани с неразрешен достъп и контрол. Може да се очаква, че такива действия водят до събиране и предаване на лична информация на трети страни в криптиран или отворен текстови формат. Такива данни могат да включват например, идентификационни данни на банкова сметка от браузъра, информация за конфигурацията на хардуера/софтуера или като цяло всичко, въведено с клавиатурата.

ОТКРИВАНЕ И АНАЛИЗИРАНЕ НА ЗЛОВРЕДЕН СОФТУЕР В ИЗБРАНИ УЕБСАЙТОВЕ, ЗА КОИТО ИМА ПОДОЗРЕНИЯ, ЧЕ НАРУШАВАТ АВТОРСКОТО ПРАВО

КРАТКО ИЗЛОЖЕНИЕ

септември 2018 г.