EUIPO
EUROOPA LIIDU
INTELLEKTUAALOMANDI AMET

KAHJURVARA TUVASTAMINE JA ANALÜÜSIMINE VALITUD VEEBIKOHTADES, MIDA KAHTLUSTATAKSE AUTORIÕIGUSE RIKKUMISES

KOMMENTEERITUD KOKKUVÕTE

September 2018

Kokkuvõte

Autoriõiguse rikkumise kahtlusega sisu on oluline intellektuaalomandiõiguste rikkumine. On veebikohti, mis jagavad sellist sisu avalikult, mõnikord isegi tasuta, ilma mis tahes registreerimiseta. Koos sellise sisuga levitavad need veebikohad tavaliselt mitmesugust kahjurvara ja nugivara, meelitades kasutajaid nende faile alla laadima ja käivitama. Uuringus antakse autoriõiguse rikkumise kahtlusega veebikohtadest leitud kahjurvara ja nugivara uusimate näidete ülevaade. Need programmid kasutavad eksitavaid tehnikaid ja manipuleerimisvõtteid – näiteks mängude tühje installatsioone ja näiliselt „kasulikku“ tarkvara –, millega petavad lõppkasutajailt välja tundlikku teavet. Uuringus avastati mitmesugust nugivara, näiteks „kasulikku“ tarkvara, valemänguinstallereid ja videovoogedastuse platvormide kliente. Selline tarkvara ei ole kasutaja tark- või riistvarale tingimata otseselt ohtlik. Manipuleerivate pettustega võidakse aga veenda kasutajat avalikustama tundlikke isikuandmeid või maksekaardi andmeid. Lisaks võidakse ilma kasutaja selgesõnalise nõusolekuta lekitada kolmandatele isikutele teavet arvuti enda kohta.

Uurimisrühm

Uurimisrühm koosnes ÜRO Regioonidevahelise Kuritegevuse ja Õigusküsimuste Uurimise Instituudi (UNICRI) programmiametnikust Francesca Boscost ning Norra teadus- ja tehnikaülikooli infotehnoloogia ja elektrotehnika teaduskonna infoturbe ja sidetehnika osakonna (digitaalkriminalistika rühma) infoturbe PhD-teadurist Andrii Shalaginovist.

Lahtiütlus

Praeguses kontekstis tuleb rõhutada, et uuringu ainus eesmärk oli tuvastada sellise kahjurvara ja nugivara tehnilised omadused, mis uuringu käigus tuvastati ja millega autoriõiguse rikkumise kahtlusega sisu otsivad internetikasutajad võivad kokku puutuda. Dokumenteeritud kahjurvara ja nugivara näiteid ei saa pidada ammendavaks, samuti ei olnud uuringu (või selle tulemuste) eesmärk hinnata kahjurvaraga ja nugivaraga nakatumise üldist tõenäosust või riski, millega internetikasutaja võib autoriõiguse rikkumise kahtlusega materjali otsimisel kokku puutuda.

EUIPO
EUROOPA LIIDU
INTELLEKTUAALOMANDI AMET

Eessõna

Autoriõiguse rikkumise kahtlusega tegevust internetis võib rahastada mitmeti, näiteks abonenttasudega, annetustega, lisateenuste tasudega ja internetis reklaami kuvamise tuluga.

Kõik rahastusvahendid ei ole siiski sama süütud kui need näited. Kahjurvaraga nakatamine ja nugivara levitamine on olnud aastaid internetis autoriõiguse rikkumise kahtlusega tegevuse rahastamise seisukohast väga tähtis.

Tavalised internetikasutajad hakkavad teadvustama nakatumise ohte, mis kaasnevad autoriõiguse rikkumise kahtlusega veebikohtadele või mobiilirakendustele juurdepääsuga.

EUIPO 2015. aasta uuringus „IP Youth Scoreboard“ selgus, et 52% noori leiab, et veebikoha turvalisus on veebisisule juurdepääsul oluline. Kokku 78% noori märkis, et nad mõtleksid järele, kui teadvustaksid riski, et arvuti või seade võib nakatuda viiruste või kahjurvaraga. 84% märkis, et nad mõtleksid järele, kui teadvustaksid riski, et krediitkaardi andmed võidakse varastada.

Käesoleva uuringu jaoks tehtud uurimistöös püstitas amet tehniliselt väga keeruka ülesande: leida ja dokumenteerida näiteid kahjurvarast ja nugivarast, millega internetikasutajad võivad kokku puutuda, kui nad proovivad saada juurdepääsu populaarsele sisule: piraatfilmidele, -muusikale, -videomängudele ja -telesaadetele.

Praeguses kontekstis tuleb rõhutada, et uuringu ainus eesmärk oli tuvastada uuringus tuvastatud sellise kahjurvara ja nugivara tehnilised omadused, millega autoriõiguse rikkumise kahtlusega sisu otsivad internetikasutajad võivad kokku puutuda. Dokumenteeritud kahjurvara ja nugivara näiteid ei saa pidada ammendavaks, samuti ei olnud uuringu (või selle tulemuste) eesmärk hinnata kahjurvaraga ja nugivaraga nakatumise üldist tõenäosust või riski, millega internetikasutaja võib autoriõiguse rikkumise kahtlusega materjali otsimisel kokku puutuda.

Uuring toimus mitmes etapis ja tihedas koostöös Europoli juures tegutseva küberkuritegevuse vastase võitluse Euroopa keskusega (EC3).

Tulemused osutavad arvukatele mitmesugustele kahjurvara- ja nugivaraohtudele, millega internetikasutaja võib autoriõiguse rikkumise kahtlusega sisu otsimisel kokku puutuda. Enamikku dokumenteeritud kahjurvara ja nugivara võib kirjeldada troojanitena või muu soovimatu tarkvarana, mis suudab saada internetikasutajate isikuandmetele volitamata juurdepääsu. Need näited on olulised ja huvipakkuvad peale intellektuaalomandiõiguste omanike ka õiguskaitseasutustele ja tarbijatele, kes kardavad, et nende isikuandmetele võidakse saada volitamata juurdepääs.

Kommenteeritud kokkuvõte

Uuringus antakse ülevaade autoriõiguse rikkumise kahtlusega veebikohtadest leitud kahjurvara ja nugivara kõige uuematest näidetest. Need programmid kasutavad eksitavaid tehnikaid ja manipuleerimisvõtteid – näiteks mängude tühje installatsioone ja näiliselt „kasulikku“ tarkvara –, millega petavad lõppkasutajailt välja tundlikku teavet.

Käesoleva uuringu eesmärk on leida ja dokumenteerida kahjurvara või muu soovimatu tarkvara, mida levitatakse autoriõiguse rikkumise kahtlusega valitud veebikohtades, ning liigitada leitud näited kahjurvara liikide järgi. Praeguses kontekstis tuleb rõhutada, et uuringu ainus eesmärk oli tuvastada sellise uuringu käigus tuvastatud kahjurvara ja nugivara tehnilised omadused, millega autoriõiguse rikkumise kahtlusega sisu otsivad internetikasutajad võivad kokku puutuda. Dokumenteeritud kahjurvara ja nugivara näiteid ei saa pidada ammendavaks, samuti ei olnud uuringu (või selle tulemuse) eesmärk hinnata kahjurvara ja nugivaraga nakatumise üldist tõenäosust või riski, millega internetikasutaja võib autoriõiguse rikkumise kahtlusega materjali otsimisel kokku puutuda. Käesolevas uuringus peetakse autoriõigusega kaitstud sisuks telesaateid, muusikat ja videomänge.

Uuringu tulemused

Autoriõiguse rikkumise kahtlusega sisu on intellektuaalomandiõiguste oluline rikkumine. On veebikohti, mis jagavad sellist sisu avalikult, mõnikord isegi tasuta, ilma mis tahes registreerimiseta. Koos sellise sisuga levitavad veebikohad tavaliselt mitmesugust kahjur- ja nugivara, mis meelitavad kasutajaid selliseid faile alla laadima ja avama. Veebikohtade tuvastamine põhines veebikohtade edetabelil Alexa Top 500 ja tuntud otsingumootoreid (nt Google, Yahoo ja Bing) kasutava keskmise kasutaja otsingute imiteerimisel ning sellel leiti, et veebikohtade kogum muutus uuringu kahe vooru vahel. Selline muutus tuleneb ilmselt sellest, et otsingumootorid kustutavad linke autoriõiguse rikkumise kahtlusega veebikohtadele, kuid pidevalt ilmuvad uued kahtlased veebikohad. Veebikohtade tuvastamisel oli üks huvitav leid seotud asjaoluga, et valdavat enamikku veebikohti hostitakse USAs või neil on seal hostimisega seotud domeeninimed. Seevastu Euroopa Liidu serverites oli selliseid veebikohti vähe. Kõige sagedamad edetabeli tipus olevad domeeninimed, mida kasutavad autoriõiguse rikkumise kahtlusega veebikohad, on .com ja .net. Põhjus võib olla, et teisiti kui riigidomeenide korral, saab neid võib-olla asutada ilma kasutajat passi või muude isikudokumentide abil tuvastamata. Keskmiselt lisandus veebikohtade tuvastamise mõlema vooru vahelisel ajal 20% uusi veebikohti ja kadus 20% vanu. Lisaks iseloomustas platvorm VirusTotal peaaegu 8% mõlemas voorus tuvastatud veebikohti kahjulikuna. Sisuhaldussüsteemide abil on uue veebikoha loomine ja sisu, isegi kahjurvararakenduste kasutajatele edastamine praegu väga lihtne.

Enne kahjurvara kogumist hõlmas käesolev uuring 2017. aastal kahjurvara ohtude dokumentaalset ülevaadet ja tehnika taseme liigitamist. Seda teadmiste kogumit kasutati hiljem kahjurvara analüüsis, et järgida ühenduses kahjurvara liikide ja perede tuvastamise kokkulepitud põhimõtteid. Andmete kogumise mõlema vooru ajal koguti kokku 106 faili. Nende hulgas on autoriõiguse rikkumise kahtlusega veebikohtadest otse alla laaditud failid ja failid, mis tekkisid allalaaditud failide käivitamisel. Uuringus avastati mitu nugivaraprogrammi, näiteks „kasulik“ tarkvara, vale-mänguinstallerid ja videovoogedastuse platvormide kliendid. Selline tarkvara ei pruugi olla kasutaja tarkvarale või riistvarale otseselt ohtlik. Manipuleerivate pettustega võidakse aga veenda kasutajat avalikustama tundlikke isikuandmeid või maksekaardi andmeid. Lisaks võidakse ilma kasutaja selgesõnalise nõusolekuta lekitada kolmandatele isikutele teavet arvuti enda kohta.

Kogutud kahjurvara analüüsiti kõigepealt avatud lähtekoodiga töövahendite abil, et mõista siseloogikat, tuvastada võimalik pahatahtlik tegevus ja hinnata selle olulisust käesoleva kahjurvarauuringu jaoks. Lisaks avatud lähtekoodiga töövahendeid kasutades tehtud esialgsele

analüüsile analüüsis kogutud kahjurvaranäiteid Europoli kahjurvara analüüsi vahendi platvorm Malware Analysis Solution (EMAS). Selle tulemusena tuvastati arvukalt mitmesuguseid artefakte ja pahatahtlikke tegevusi. EMASi aruanded sisaldavad igakülgset analüüsi failide kohta, mis kasutavad nelja MS Windowsi versiooni, kus võrguliiklus, funktsioonikäsud ja kettatoimingud edasiseks analüüsiks põhjalikult logitakse. Lisaks juhib platvorm tähelepanu kõigile kahtlastele toimingutele, mis tuvastatakse faili kasutamisel. Pärast kõigi aruannete analüüsi märkis EMAS 35 liiki pahatahtlikku tegevust, mis koondati kahjulike juhtumite 17 klassi. Need ulatuvad üldanomaaliatest (nt süsteemiprotsesside käivitamine või mälust protsesside otsimine) ilmselgelt pahatahtlike toiminguteni (nt klahvinuhk, juurkratt ja võrguliikluse häirimine).

Üldiselt ilmnevad kogutud kahjurvara ja nugivara kahendkoodi näidetest mitu üldist tegevusmudelit: „kasulikud“ programmid, mis väidetavalt puhastavad tasulise tellimise korral kasutaja arvuti vanadest failidest; mängu installimise imitaatorid, mis nõuavad kasutaja isikuandmeid; ning tasuta programmid, mis pakuvad juurdepääsu piraatsisu levitavatele platvormidele, näiteks BitTorrenti jälgurite kaudu. Veebikohtade tuvastamise ja kahjurvara kogumise kaks vooru andsid paljulubavaid tulemusi kahjurvara levitamise ja selliste manipuleerimisvõtete mõistmisel, millega meelitatakse välja tundlikku isiklikku ja tuvastatavat teavet. Lisaks on paljude operatsioonisüsteemi Android kasutavate nugivaraprogrammide (mis on kättesaadavad autoriõiguse rikkumise kahtlusega sisu levitavate platvormide kaudu) tuvastamist arvestades ilmne, et viimastel aastatel on suurenenud mobiilseadmete populaarsus. Analüüside seostamise tulemusel järeldati, et autoriõigusi rikkuvate veebikohtade kaudu leviva kahjurvaraga ohtude kogum on esmamuljest keerukam. Avastatud tarkvarast mõne võib liigitada ka troojaniks, reklaamvaraks, tagaukseks ja agendiks. Sellele lisandub asjaolu, et leiti ka palju spetsiifilisi kahjurvaraperesid, nt WisdomEyes, DealPly ja FileRepMalware. Veelgi enam, selline ulatuslik liigitus kehtib peale Microsoft Windowsi ka platvormi Android kohta. Kasutajate vara ähvardavad arvukad ohud, näiteks tundlike kasutajaandmete, isikuandmete ja riistvara konfiguratsiooniteabe varastamine ja võrguliikluse moonutamine. Seega, kuigi tuvastatud tarkvara võib olla nugivara, võib see siiski mõjutada kasutajaid, eriti kui tegu on keskmise kasutajaga, kes ei pruugi täielikult teadvustada veebiturvalisuse lihtsaimaid tavasid ja meetmeid.

Allpool on näide uuringu leidudest.

Veebikoht 03	Veebikoht 09	
Veebikoht meelitab kasutajaid installima valemänge; kasutaja tundlike andmete hankimise kogu protsess on kahjurvara kogumise esimese ja teise etapi vahelisel ajal muutunud. Teenuse kasutaja laadib alla arhiivi, mis sisaldab mänguga seotud failideks maskeeritud sisu, mitte selgelt käivitatavat kahendfaili, mille tuvastaks kahjurvarana iga viirusetõrje. Krüptitud arhiiv annab juurdepääsu ainult failinimedele, kuid mitte failide põhisisule.	Veebikoht pakub tarkvaravahendi abil juurdepääsu igat liiki videosisule, mis on kättesaadav torrentijälgurite kaudu. Võrreldes teiste BitTorrenti jälguritega vajab see vähem kasutaja sekkumist. Tundmatutest allikatest sisu allalaadimiseks on vaja ainult mõnda klõpsu, kuid kasutaja ei ole allalaaditava sisu eest ei kaitstud ja see ei ole tema võimuses.	(Android) Veebikoht annab registreerimata juurdepääsu paljudele tasuta mobiilirakendustele. Sama rakendus pakub piiramatut juurdepääsu telesaadete ja filmide voogedastusele. Autoriõigusega kaitstud videotele juurdepääsu saamiseks ei nõuta selge sõnaga kasutaja tundliku teabe või makseandmete esitamist. Kasutaja peab aga välja lülitama turvaseaded, et ta saaks paigaldada rakendusi, mis ei pärine rakenduste ametlikust müügikohast.

Metoodika

Uuringu tegemiseks tuli koostada töökindel metoodika, et käsitleda pealkirjade ja veebikohtade valikut ning täita tehniliselt nõudlik ülesanne tuvastada ja dokumenteerida leitud kahjurvara ja nugivara näited. Metoodika lühiülevaade on järgmine.

1. UNICRI uuringu esimeses etapis moodustati koostöös intellektuaalomandiga seotud õigusrikkumiste Euroopa vaatluskeskusega (edaspidi „vaatluskeskus“) ekspertide tugirühm, kes annab nõu uurimismetoodika ja analüüsis kasutatavate veebikohtade valiku kohta ning hindab projekti rakendamise igas etapis tehtud uurimistööd. Ekspertide tugirühma kuulusid vaatluskeskuse sidusrühmade, õiguste omanike organisatsioonide, teadusringkondade, õiguskaitseasutuste ja Euroopa Liidu asutuste esindajad.

2. Samal ajal valiti uurimisrühm. Selles aruandes ei olnud tehniliselt võimalik[1] uurida kõiki Euroopa Liidu liikmesriike, mispärast koostati teises etapis 28 liikmesriigist juhuvalikuga 10 riigi valim.

3. Kolmandas etapis tuvastati populaarsed filmid, telesaated, laulud ja videomängud. Populaarsus hõlmas ülemaailmset populaarsust ja populaarsust ühes või mitmes valimisse kuuluvas 10 riigis andmete kogumise ajavahemiku alguskuupäeval 23. juunil 2017. Uuringu järgmistes etappides kasutati neid näidispealkirju süstemaatiliselt veebiotsingutes, et leida autoriõigusi rikkuvaid veebikohti ja mobiilirakendusi. Iga pealkiri vastas ühele või mitmele järgmisele kriteeriumile:

   - andmete kogumise ajal populaarne Euroopa Liidu liikmesriikides,
   - andmete kogumise ajal populaarne kogu maailmas,
   - on olnud üle maailma populaarne ja
   - on film, telesaade, laul või videomäng.

   Välja valiti viis filmipealkirja, viis telesaate pealkirja, viis laulupealkirja ja viis videomängu pealkirja, kokku 20 näidispealkirja. Iga pealkirja populaarsuse määramise allikaid kaaluti hoolikalt, see hõlmas süstemaatilist valikuprotsessi, et olla kindel, et allikandmed on kättesaadavad kõigis või enamikus liimesriikides.

4. Neljandas etapis tuvastati veebikohad, mida kahtlustati ebaseadusliku juurdepääsu pakkumises autoriõigusega kaitstud materjalile, mis oli 26. juuni 2017. aasta seisuga populaarne kogu maailmas ja/või valimisse kuuluvas 10 liikmesriigis (kahjurvara kogumise esimene voor). Uuringu hilisemas etapis uuriti kahjurvara ja nugivara olemasolu nendes veebikohtades.

   Autoriõiguse rikkumise kahtlusega veebikohtade tuvastamise metoodika töötati välja esimeses etapis loodud ekspertide tugirühma esitatud andmete ja UNICRI olemasoleva kirjandusülevaate alusel. See töötati spetsiaalselt välja selliste veebikohtade valimi koostamiseks, mis

   - on populaarsed Euroopa Liidu eri liikmesriikides, tagades sellega laia geograafilise ulatuse;
   - esindavad autoriõiguse rikkumise kahtlusega veebikohtade liike, sealhulgas voogedastuse, linkivaid, hostivaid veebikohti, failivahetuskohti ja torrent-veebikohti;
   - esindavad mitmesugust autoriõiguse rikkumise kahtlusega sisu, näiteks filme, telesaateid, muusikat ja videomänge, ning
   - esindavad veebikohti, millele satuks keskmine internetikasutaja, kui ta üritab juurdepääsu autoriõiguse rikkumise kahtlusega materjalile.

   Autoriõiguse rikkumise kahtlusega veebikohad valiti viies etapis. Esimesed kolm etappi olid kavandatud kõigis Euroopa Liidu liikmesriikides kõige populaarsemate autoriõiguse rikkumise

[1] Valitud riikide arv mõjutab otseselt valitud autoriõiguse rikkumise kahtlusega veebikohtade ja vastavate analüüsitavate kahendfailide arvu (mida rohkem on riike, seda rohkem on faile). Seega otsustati keskenduda ainult sellisele riikide valimile, et uuringu praktiline osa valmiks ettenähtud aja jooksul.

kahtlusega veebikohtade tuvastamiseks. Meetod jäljendas stsenaariume, kus keskmine kasutaja võib otsida autoriõiguse rikkumise kahtlusega veebikohti, täpsustamata näiteks filmi või laulu pealkirja. Kaks viimast etappi püüdsid tuvastada neid autoriõiguse rikkumise kahtlusega veebikohti, millele keskmine kasutaja võib sattuda, kui ta otsib, kuidas saab teatud populaarse teose alla laadida, kuid ei nimeta veebikohta. See etapp oli eriti tähtis, arvestades selliste kahjurvara kahtlusega veebikohtade olemasolu, mis osalevad otsingutulemuste moonutamises, millega nad kasutavad ära populaarseid teemasid, optimeerides otsimootoreid. Koos hõlmasid mõlemad meetodid eri viise, kuidas keskmine internetikasutaja üritaks internetis leida autoriõiguse rikkumise kahtlusega materjali.

Rõhuasetus oli seadmete (nt nutitelefonide ja tahvelarvutite) mobiilirakendustele omase kahjurvara ja nugivara kui küberkuritegevuse ühe olulise tekkiva ohu üheaegsel analüüsil. Tuginedes olemasolevas kirjanduses esitatud viidetele, et kahjurvara leidub rohkem Androidi rakenduste poodides (st Google Play) kui Apple iTunes'i poes, piirduti analüüsis Androidi seadmetega. Metoodika töötati spetsiaalselt välja selliste mobiilirakenduste valimi koostamiseks, mis

- on andmete kogumise ajal populaarsed kogu maailmas;
- esindavad eri liiki rakendusi (et hõlmata voogedastuse rakendused, torrentrakendused ja hostimisrakendused);
- esindavad mitmesugust autoriõiguse rikkumise kahtlusega sisu (et hõlmata filmid, telesaated, muusika ja videomängud) või pakuvad sellele juurdepääsu; ning
- esindavad seda, millega keskmine mobiilseadme kasutaja kokku puutub, kui ta üritab alla laadida või kasutada rakendust, mis hõlbustab juurdepääsu autoriõiguse rikkumise kahtlusega sisule.

5. Viiendas etapis koguti lisaks mobiilirakendustele kahjurvara ja nugivara tuvastatud veebikohtades, et uurida neid liigitamiseks hilisemas etapis. Andmete kogumise etapp hõlmas kahjurvara kogumise ja analüüsimise kaht vooru, mis toimusid 2017. aasta suvel. Kahjurvara kogumise esimese vooru tulemusena saadi 10 valitud Euroopa Liidu liikmesriigis 1054 kordumatut domeeninime ja teises voorus 1057. Kahjurvara koguti käsitsi ja automaatselt, jäljendades keskmise kasutaja kogemust.

Kogumine käsitsi. Selle meetodiga vaadati eelmises etapis tuvastatud domeenid käsitsi läbi. Käsitsi kogumise abil sai ekspert jäljendada keskmise internetikasutaja kogemust, klõpsates reklaame ja suheldes veebikohtadega, mis nõudsid kasutaja reageerimist.

Automaatkogumine. Selle meetodi korral kasutati automaatset veebiämblikku, mis kontrollis läbi kõik autoriõiguse rikkumise kahtlusega määratud veebikohas olevad lingid. Esiteks kogus veebiämblik igas veebikohas teavet esilehel olevatest linkidest. Teiseks avas veebiämblik iga lingi, mis viis sekundaarsetesse veebikohtadesse. Kolmandaks avas veebiämblik iga lingi, mis viis tertsiaarsetesse veebikohtadesse. Igas etapis leidis veebiämblik kahendfaile, mis võisid järgneva käsitsi analüüsi jaoks huvi pakkuda, sealhulgas võimaliku või kahtlustatava kahjurvara ja nugivara. See protsess jätkus kuni 1000 lingini veebikoha kohta.

6. Kui kahendfailid olid kogutud, analüüsiti neid turvalises arvutikeskkonnas, et mõista nende sisefunktsioone ja need õigesti liigitada. Esialgses analüüsis kasutati avatud lähtekoodiga töövahendeid, et tulemusi oleks võimalik seostada teatatud küberohtudega. Seejärel saadeti kogutud tarkvara näited EMASile analüüsimiseks; pärast võrreldi EMASi analüüsi esialgsete tulemustega.

Metoodika ülevaade

Tuvastatud kahjurvara ja nugivara näited

28. juuli 2017. aasta seisuga oli kogumise esimeses voorus automaatselt kontrollitud 5240 veebikohta (1054 kordumatut), seejuures leiti 617 asjakohast faili (muusika, video, torrentfailid ja tarkvara), kogusuurusega 47 GB. Seda sortimata failikogumit tuli edasi analüüsida, et otsustada, mis kogutud failid on uuringu seisukohast asjakohased. Autoriõigusi rikkuvate veebikohtade näited olid sarnased kõigis 10 valimisse kuuluvas riigis igas meedialiigis (telesaated, filmid, muusika ja videomängud). Selle tulemusena valiti valimisse kuuluvatest riikidest juhuvalikuga välja Belgia ning kõiki veebikohti, mis tuvastati Belgias autoriõigusi rikkuvana, kontrolliti käsitsi, kas neis on kahjurvara või nugivara. Pärast kogumise teist vooru laaditi 10. augustil 2017 kõigi riikide veebikohtadest automaatselt alla 3665 faili kogusuurusega 167 GB. Kõigi riikide jaoks välja võetud URLe oli 5606 veebikoha kohta kokku 1057, mis välistas nende kõigi käsitsi kontrollimise.

Pärast kogutud failide esialgset analüüsi eraldati kahjurvara kogumise mõlema vooru tulemusena 106 MS Windowsi, Androidi ja Mac Osi kordumatut kahendfaili. Täpsemalt valiti esimeses voorus 41 faili ja teises 65, mis jagunesid konkreetselt järgmiselt: 2 Maci, 15 Androidi ja 89 MS Windowsi faili. Neist failidest 21 võib pidada tuntud kahjurvaraprogrammideks, mida on nimetanud paljud viirusetõrje müüjad, keda koondab platvorm VirusTotal. Nende hulgas on autoriõiguse rikkumise kahtlusega valitud veebikohtadest otse alla laaditud failid ja failid, mis tekkisid allalaaditud failide käitamisel. Seejärel analüüsiti kogutud näiteid turvalises aedikukeskkonnas ja saadeti võimaliku pahatahtliku tegevuse täpsemaks analüüsiks EMASile. EMASi neljas aruandes (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3) avastati kõigis kahendfailides kokku 821 kahjurvara üksikjuhtumit. Mõnes aruandes ühtki kahtlast tegevust ei leidunud ja mõnes oli kuni 10 varasemast teatud pahatahtlikku tegevust. Uuringu viimases etapis uuriti esialgse analüüsi ja EMASi aruannete tulemuste vastastikseoseid. Tulemuste kvantitatiivne kokkuvõte on järgmises tabelis.

	1. voor	2. voor
Kuupäev	28. juuli 2017	10. august 2017
Euroopa Liidu 10 liikmesriigis avastatud veebikohti	5240	5606
Kordumatuid veebikohti	1054	1057
Asjakohaseid faile	617	3665[2]
Asjakohaste failide suurus (GB)	47	167
Edastatud EMASile		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Suurus kokku (baiti)	175 600 117	522 991 095

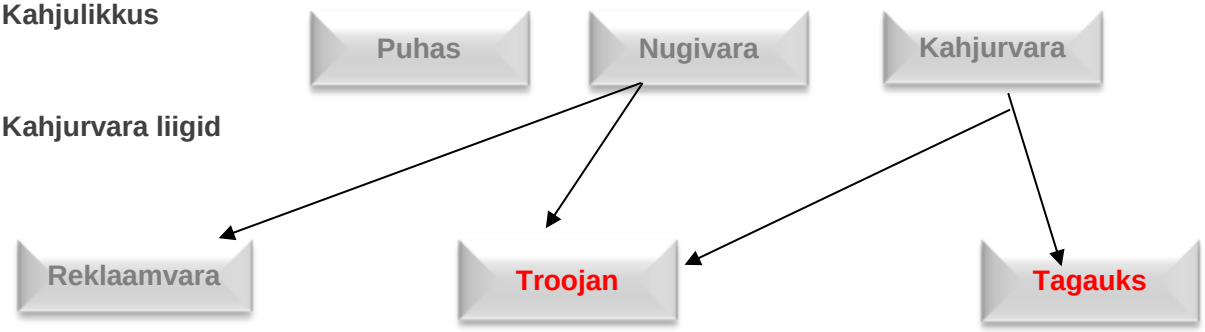
Europoli kahjurvara analüüsi vahend (EMAS)

Europoli kahjurvara analüüsi vahend (EMAS) on kahjurvara automaatanalüüsi dünaamiline vahend, mida pakub Europol ELi liikmesriikidele. EMAS pakub analüüsiaruannete koostamise võimalust, kuid selle kõige pöördelisem omadus on politseiuurijatele luureandmete väljastamine. Automaatsed ristkontrollid näitavad seoseid eri riikides sama kahjurvaraga sooritatud rünnakute vahel või sama kahjurvarapere taga oleva sama kuritegeliku organisatsiooniga, võttes ühendust samade domeenidega, ja on seotud eri uurimistega Euroopa Liidus või mujal. 2015. aastal muutus EMAS täisautomaatseks, et võimaldada otsejuurdepääsu õiguskaitseasutustest osalistele, kellega Europolil on koostöölepingud. 2015. aastal: analüüsiti EMASis 525 108 faili, millest kahjurvarana tuvastati 356 863.

Nagu on näha alljärgneval joonisel, võib kogutud kahendfailid üldiselt liigitada kahjulikkuse alusel kahjututeks (failideks, mis ei tekita kahju), nugivaraks ja kahjurvaraks. Nugivara tuvastati peale Microsoft Windowsi ka operatsioonisüsteemide Android ja Mac Os korral, mis tähendab, et kahjurvara arendajad üritavad mõjutada võimalikult paljusid kasutajaid, kasutades eri platvorme. Nugivara ja kahjurvara võib täpsemalt eristada peamiste kahjurvara liikide alusel (troojan, reklaamvara ja tagauks). Enamik leitud tarkvarast kuulub nugivara kategooriasse. Nugivara toimimist võib seostada ühega järgmistest tegevusmudelitest: vale-mänguinstallerid, mis nõuavad isikuandmeid ja pangakonto andmeid; allalaaditavad „kasulikud“ programmid, mis sunnivad kasutajaid tellima tasulise versiooni; või tasuta programmide installimine autoriõigusi rikkuvatele platvormidele pääsemiseks. Need rakendused võivad kahjustada kasutajate isikuandmeid ja arvuti konfiguratsiooni. Manipuleerivate pettustega võidakse avalikustada ka mitmesugust privaatset teavet, näiteks maksekaardi andmeid, isikut tuvastavaid andmeid ja suhtlusmeedia konto andmeid. Samuti tuvastati uuringus kolmandate isikute rakenduste turgudel 15 Androidi rakendust, pärast esialgset analüüsi järeldati, et need rakendused võivad olla seotud autoriõigusi rikkuva sisu levitamise ja isikuandmete avalikustamisega.

[2] 1. ja 2. vooru arvude erinevust selgitab, et 2. vooru automaatsel kogumisel oli veebikohti, mis avaldasid igal oma veebilehel mitu failikomplekti.

Kahjulikkus



Ohud lõppkasutajatele

Veebikoha tuvastamise ja kahjurvara analüüsi kahes voorus ei leitud ühtki lunavara kahendfaili. Üldiselt võib enamikku kogutud kahjurvara kirjeldada troojanitena, mis tähendab, et need võivad veebikohtades matkida üldkasutatavat või populaarset tarkvara, kuid tegelikult võivad varastada või avalikustada privaatset teavet. Kogenematu kasutaja võib pidada tarkvara väga usaldusväärseks ega pruugi märgata erinevusi tavalisest. Lisaks sellele ei pruugi sellise tarkvara staatiline analüüs ja dünaamilised käitumisvaatlused ilma lähtekoodi analüüsimata paljastada selle kõiki funktsioone. EMASi analüüs näitas pärast kahjurvara esialgset analüüsi täpsemaid pahatahtlikke tegevusi. Selle tarkvara lõppkasutaja arvutisse paigaldamise mõju võib olla oluline, põhjustades peale rahalise kahju ka isikuandmete vargust ning muid soovimatu juurdepääsu ja kontrolliga seotud ohte. Sellise tegevuse eeldatav tagajärg võib olla isikuandmete kogumine ja edastamine kolmandatele isikutele krüptituna või avatud tekstivormingus. Sellised andmed võivad olla näiteks brauserist saadud pangakonto andmed, arvuti riistvara/tarkvara konfiguratsiooni andmed või põhimõtteliselt kõik, mis tipitakse klaviatuuril.

KAHJURVARA TUVASTAMINE JA ANALÜÜSIMINE VALITUD VEEBIKOHTADES, MIDA KAHTLUSTATAKSE AUTORIÕIGUSE RIKKUMISES

KOMMENTEERITUD KOKKUVÕTE

September 2018