EUIPO
EIROPAS SAVIENĪBAS
INTELEKTUĀLĀ ĪPAŠUMA BIROJS

KONKRĒTU TĀDU TĪMEKĻA VIETŅU ĻAUNPROGRAMMATŪRU IDENTIFICĒŠANA UN ANALĪZE, PAR KURĀM IR AIZDOMAS, KA AR TĀM TIEK PĀRKĀPTAS AUTORTIESĪBAS

KOPSAVILKUMS

2018. gada septembris

Rezumējums

Saturs, par ko ir aizdomas, ka ar to pārkāpj autortiesības, ir būtisks intelektuālā īpašuma tiesību pārkāpums. Ir dažas tīmekļa vietnes, kurās publiski kopīgo šādu saturu, dažkārt pat bez maksas un bez jebkādas reģistrācijas. Kopā ar šo saturu tīmekļa vietnēs parasti izplata arī dažāda veida ļaunprogrammatūras un potenciāli nevēlamas programmas (PNP), kas vilina lietotājus lejupielādēt un atvērt šos failus. Šajā pētījumā sniegts pārskats par visjaunākajiem ļaunprogrammatūru un PNP piemēriem, kas atrasti tīmekļa vietnēs, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības. Šajās programmās izmanto maldinošus paņēmienus un sociālo inženieriju, piemēram, tukšu spēļu instalēšanu un šķietami "lietderīgas" programmatūras, lai izmānītu no lietotājiem konfidenciālu informāciju. Pētījuma laikā tika atklātas dažādas PNP, piemēram, kā "lietderīgas" programmatūras, neīsti spēļu instalētāji un klienti video straumēšanas platformām. Ne vienmēr šādas programmatūras tiešā veidā apdraud lietotāja programmatūras vai iekārtas. Tomēr, izmantojot inženierijas trikus, lietotāju var pārliecināt atklāt konfidenciālu personas informāciju vai maksājumu karšu datus. Turklāt var tikt citām personām nopludināta informācija par pašu datoru bez nepārprotamas lietotāja piekrišanas.

Pētniecības grupa

Pētniecības grupas dalībnieki: Apvienoto Nāciju Organizācijas Starpreģionālā noziedzības un tieslietu pētniecības institūta (*UNICRI*) programmas vadītāja *Francesca Bosco* un Norvēģijas Zinātnes un tehnoloģiju universitātes Informācijas tehnoloģiju un elektrotehnikas fakultātes Informācijas drošības un sakaru tehnoloģiju katedras (Digitālās tiesu ekspertīzes grupas) informācijas drošības doktorants *Andrii Shalaginov*.

Saistību atruna

Šajā kontekstā ir jāuzsver, ka šī pētījuma vienīgais mērķis bija noteikt tādu pētījuma laikā konstatēto ļaunprogrammatūru un PNP tehnisko raksturojumu, ar kādām varētu saskarties interneta lietotāji, kuri meklē saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības. Dokumentētie ļaunprogrammatūru un PNP paraugi nav uzskatāmi par pilnīgiem, kā arī šī pētījuma (vai tā rezultātu) mērķis nebija novērtēt vispārīgās iespējas vai draudus inficēties ar ļaunprogrammatūrām un PNP, ar ko saskartos interneta lietotājs, kurš meklē materiālus, par ko ir aizdomas, ka ar tiem pārkāpj autortiesības.

Priekšvārds

Dažādos veidos var finansēt darbības internetā, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, tostarp ar abonēšanas maksām, ziedojumiem, maksājumiem par papildpakalpojumiem un ienākumiem no tiešsaistes reklāmām internetā.

Tomēr ne visi finansēšanas veidi ir tik nekaitīgi kā iepriekšminētie piemēri. Jau daudzus gadus ļaunprogrammatūru infekciju un cita veida potenciāli nevēlamu programmu (PNP) izplatīšanai ir bijusi būtiska nozīme saistībā ar tādu darbību internetā finansēšanu, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības.

Parastie interneta lietotāji sāk apzināties inficēšanās riskus, kas rodas, piekļūstot tīmekļa vietnēm vai mobilajām lietotnēm, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības.

EUIPO 2015. gada IĪ Jauniešu rezultātu pārskatā bija redzams, ka 52 % jauniešu uzskata, ka, piekļūstot tiešsaistes saturam, drošība internetā ir svarīga. Kopumā 78 % jauniešu apgalvoja, ka viņi būtu padomājuši divreiz, ja būtu zinājuši par risku, ka datoru vai iekārtu var inficēt vīrusi vai ļaunprogrammatūras. Kopumā 84 % apgalvoja, ka viņi būtu padomājuši divreiz, ja būtu zinājuši par risku, ka var tikt nozagti viņu kredītkaršu dati.

Šajā pētījumā birojs bija noteicis tehniski ļoti sarežģītu uzdevumu, proti, identificēt un dokumentēt ļaunprogrammatūru un PNP paraugus, ar ko varētu sastapties interneta lietotāji, cenšoties piekļūt populārām pirātiskām filmām, mūzikai, videospēlēm un televīzijas raidījumiem.

Šajā kontekstā ir jāuzsver, ka šā pētījuma vienīgais mērķis bija noteikt tādu pētījuma laikā konstatēto ļaunprogrammatūru un PNP tehniskos raksturlielumus, ar kurām varētu saskarties interneta lietotāji, kuri meklē saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības. Dokumentētie ļaunprogrammatūru un PNP paraugi nav uzskatāmi par pilnīgiem, kā arī šī pētījuma (vai tā rezultātu) mērķis nebija novērtēt vispārīgo iespēju vai draudus inficēties ar ļaunprogrammatūrām un PNP, ar ko saskartos interneta lietotājs, kurš meklē materiālus, par ko ir aizdomas, ka ar tiem pārkāpj autortiesības.

Pētījumu veica vairākos posmos ciešā sadarbībā ar Eiropola Eiropas Kibernoziedzības apkarošanas centru (EC3).

Iegūtie rezultāti atklāj dažādus ļaunprogrammatūru un PNP draudus, ar ko interneta lietotājs var sastapties, meklējot saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības. Vairumu dokumentēto ļaunprogrammatūru un PNP var raksturot kā “Trojas zirgus” vai citas nevēlamas programmatūras, kas spēj iegūt nesankcionētu piekļuvi interneta lietotāju personas datiem. Šie piemēri būs svarīgi un interesanti ne tikai tiem, kuriem pieder intelektuālā īpašuma tiesības, bet arī tiesībaizsardzības iestādēm, kā arī patērētājiem, kuri raizējas par to, ka viņu personas datiem var piekļūt bez viņu atļaujas, kas ir ne mazāk svarīgi.

Kopsavilkums

Šajā pētījumā ir sniegts pārskats par visjaunākajiem ļaunprogrammatūru un potenciāli nevēlamu programmu (PNP) piemēriem, kas atrasti tīmekļa vietnēs, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības. Šajās programmās izmanto maldinošus paņēmienus un sociālo inženieriju, piemēram, tukšu spēļu instalēšanu un šķietami "lietderīgas" programmatūras, lai izmānītu no lietotājiem konfidenciālu informāciju.

Šī pētījuma mērķis ir atklāt un dokumentēt ļaunprogrammatūras vai citādi nevēlamas programmatūras, kas izplatās noteiktās tīmekļa vietnēs, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, kā arī sistematizēt atrastos paraugus saskaņā ar dažādu ļaunprogrammatūru taksonomijām. Šajā kontekstā ir jāuzsver, ka šā pētījuma vienīgais mērķis bija noteikt tādu pētījuma laikā konstatēto ļaunprogrammatūru un PNP tehnisko raksturojumu, ar kurām varētu saskarties interneta lietotāji, kuri meklē saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības. Dokumentētie ļaunprogrammatūru un PNP paraugi nav uzskatāmi par pilnīgiem, kā arī šā pētījuma (vai tā rezultātu) mērķis nebija novērtēt vispārīgo iespēju vai draudus inficēties ar ļaunprogrammatūrām un PNP, ar ko saskartos interneta lietotājs, kurš meklē materiālus, par ko ir aizdomas, ka ar tiem pārkāpj autortiesības. Šī pētījuma izpratnē TV raidījumi, filmas, mūzika un videospēles ir uzskatāmas par saturu, kas aizsargāts ar autortiesībām.

Pētījuma rezultāti

Saturs, par ko ir aizdomas, ka ar to pārkāpj autortiesības, ir būtisks intelektuālā īpašuma tiesību pārkāpums. Ir dažas tīmekļa vietnes, kurās publiski kopīgo šādu saturu, dažkārt pat bez maksas un bez jebkādas reģistrācijas. Kopā ar šādu saturu tīmekļa vietnes parasti izplata arī dažāda veida ļaunprogrammatūras un PNP, kas vilina lietotājus lejupielādēt un atvērt šādus failus. Tīmekļa vietņu identificēšanas laikā, balstoties uz *Alexa Top 500* vērtējumu, ne tikai simulēja vidusmēra lietotāja meklēšanu, izmantojot visiem labi zināmās meklētājprogrammas *Google*, *Yahoo* un *Bing*, bet arī atklāja, ka tīmekļa vietņu kopas laikā starp abām pētījuma kārtām bija mainījušās. Šo izmaiņu cēlonis, iespējams, ir tas, ka meklētājprogrammas cenšas izdzēst saites uz tīmekļa vietnēm, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, bet to vietā turpina parādīties jaunas aizdomīgas tīmekļa vietnes. Saistībā ar tīmekļa vietņu identificēšanu tika izdarīts interesants atklājums saistībā ar faktu, ka lielākā daļa tīmekļa vietņu tiek mitinātas ASV vai arī tām ir domēna nosaukumi saistībā ar mitināšanu šajā valstī. Savukārt tikai nedaudz no tām atrodas ES serveros. Turklāt .com un .net ir augstākā līmeņa domēnu nosaukumi, ko visbiežāk izmanto tīmekļa vietnēs, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības. Tā cēlonis var būt fakts, ka atšķirībā no konkrētiem valsts domēniem šiem var nebūt nepieciešama lietotāja identifikācija, izmantojot pasi vai citus identifikācijas dokumentus. Laikā starp abām vietņu identificēšanas kārtām tika vidēji pievienoti 20 % jaunu tīmekļa vietņu un izdzēsti 20 % veco tīmekļa vietņu. Turklāt *VirusTotal* platforma raksturoja kā ļaunprātīgas gandrīz 8 % identificēto tīmekļa vietņu abās kārtās. Izmantojot dažādas satura pārvaldības sistēmas, mūsdienās gandrīz bez pūlēm var izveidot tīmekļa vietni un piegādāt saturu lietotājiem, pat ļaunprātīgas lietotnes.

Pirms ļaunprogrammatūru apkopošanas 2017. gadā šajā pētījumā tika veikta iespējamo ļaunprogrammatūru draudu dokumentāra pārbaude un esošā stāvokļa sistematizācija. Šo zināšanu kopumu pēc tam izmantoja ļaunprogrammatūru analīzes laikā, lai ievērotu pieņemtos principus ļaunprogrammatūru veidu un grupu identificēšanā. Abās datu apkopošanas kārtās kopumā apkopoja 106 failus. Tie ietver failus, kas lejupielādēti tieši no tīmekļa vietnēm, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, kā arī failus, kas izveidoti lejupielādēto failu izpildes laikā. Pētījuma laikā tika atklātas dažādas PNP, piemēram, "lietderīgas" programmatūras, neīsti spēļu instalētāji un klienti video straumēšanas platformām. Ne vienmēr šādas programmatūras tiešā veidā apdraud lietotāja programmatūras vai iekārtas. Tomēr, izmantojot sociālās inženierijas trikus, lietotāju var pārliecināt atklāt konfidenciālu personas informāciju vai maksājumu karšu

datus. Turklāt var tikt citām personām nopludināta informācija par pašu datoru bez nepārprotamas lietotāja piekrišanas.

Apkopotās ļaunprogrammatūras tika analizētas, sākotnēji izmantojot atvērtā koda rīkus, lai izprastu iekšējo loģiku, atklātu iespējamas ļaunprātīgas darbības un izvērtētu to nozīmi šā ļaunprogrammatūru pētījuma aspektā. Papildus sākotnējai analīzei, kurā tika izmantoti atvērtā koda rīki, apkopotos ļaunprogrammatūru paraugus analizēja Eiropola Ļaunprogrammatūru analīzes risinājumu (*EMAS*) platforma. Tā rezultātā atklāja lielu skaitu dažādu artefaktu un ļaunprātīgu darbību. *EMAS* ziņojumi ietver failu, kuros izmanto četras *MS Windows* versijas, visaptverošu analīzi, kurā turpmākas analīzes vajadzībām rūpīgi reģistrēja tīkla trafiku, funkciju izsaukumus un diska darbības. Turklāt šī platforma norāda jebkādas aizdomīgas darbības, kas atklātas failu izpildes rutīnu laikā. Pēc visu ziņojumu analīzes *EMAS* norādīja uz 35 ļaunprātīgām darbībām, kas apkopotas 17 ļaunprātīgu gadījumu klasēs. Tās ir gan vispārējas anomālijas (piemēram, sistēmas procesu palaišana vai procesu meklēšana atmiņās), gan nepārprotami ļaunprātīgas darbības (tādas kā taustiņsitienu reģistrētājs, sistēmlauznis un tīkla trafika pārveidošana).

Kopumā apkopotie ļaunprogrammatūru un PNP binārie paraugi atklāja dažus atšķirīgus vispārīgas darbības modeļus: “lietderīgas” programmas, kas šķietami iztīra vecos failus lietotāja datorā pēc maksas abonēšanas, spēļu instalēšanas simulatori, kas pieprasa lietotāja personas datus, kā arī bezmaksas programmas, kurās piedāvā piekļuvi platformām, kas izplata pirātisku saturu, piemēram, izmantojot *BitTorrent* izsekotāju. Abas tīmekļa vietņu identifikācijas un ļaunprogrammatūru apkopošanas kārtas sniedza daudzsološus rezultātus attiecībā uz ļaunprogrammatūru izplatīšanas paņēmieniem un sociālo inženieriju nolūkā izvilināt konfidenciālu personas informāciju un identificējamu informāciju. Turklāt ir acīmredzama aizvien lielākā mobilo ierīču popularitāte pēdējo gadu laikā, ņemot vērā daudzās atklātās *Android OS* PNP, kas pieejamas platformās, kurās izplata saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības. Analīžu korelācijas rezultātā tika izdarīti secinājumi, ka tīmekļa vietnēs, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, izplatītāko ļaunprogrammatūru draudi ir daudz izsmalcinātāki, nekā varētu šķist sākumā. Starp atklātajām programmatūrām dažas var papildu klasificēt kā Trojas zirgus, reklāmprogrammatūras, slepenas programmatūras un aģentus. To vēl vairāk apgrūtina fakts, ka tika atklātas arī daudzas īpašas ļaunprogrammatūru grupas, piemēram, *WisdomEyes*, *DealPly* un *FileRepMalware*. Turklāt šāda visaptveroša sistematizācija darbojas arī *Android* platformā, ne tikai *Microsoft Windows*. Pastāv plašs draudu klāsts attiecībā uz lietotāju datiem, tostarp, bet ne tikai konfidenciālu akreditācijas datu, personas datu, iekārtu konfigurēšanas informācijas zagšana un tīkla trafika pārveidošana. Tādējādi, lai gan identificētās programmatūras var būt PNP, tās var ietekmēt lietotājus, jo īpaši gadījumos, kad ir iesaistīts vidusmēra lietotājs, kurš, iespējams, pilnībā nepārzina pamata drošības praksi un pasākumus internetā.

Pētījuma rezultātu paraugi ir sniegti turpmāk.

Tīmekļa vietne 03	Tīmekļa vietne 09	Tīmekļa vietne 08
Tīmekļa vietne ievilina lietotājus viltus spēļu instalēšanas izmantošanā. Laikā starp pirmo un otro ļaunprogrammatūru apkopošanu viss lietotāju konfidenciālās informācijas iegūšanas process bija mainījies. Šā pakalpojuma lietotājs lejupielādē arhīvu, kura saturs ir maskēts kā faili, kas saistīti ar spēli, un nav nepārprotami binārs izpildāms fails, ko antivīrusu programma var atklāt kā ļaunprātīgu. Šifrētais arhīvs sniedz pieeju tikai failu nosaukumiem, nevis failu saturam pēc būtības.	Tīmekļa vietne piedāvā piekļuvi jebkura veida video saturam, kas pieejams, ar programmnodrošinājuma palīdzību izmantojot gāzmas izsekotājus. Šim rīkam, salīdzinot ar citiem *BitTorrent* izsekotājiem, ir nepieciešama mazāka lietotāju iesaistīšanās. Lai lejupielādētu saturu no nezināma avota, ir nepieciešami tikai pāris klikšķi, bet lietotājs nav ne aizsargāts, ne spēj kontrolēt to, kas tiek lejupielādēts.	(*Android*) Šī tīmekļa vietne sniedz piekļuvi plašam bezmaksas tālruņa lietotņu klāstam bez reģistrācijas. Viena lietotne sniedz neierobežotu piekļuvi TV raidījumu un filmu straumēšanai. Nav nepārprotamas prasības sniegt konfidenciālu lietotāja informāciju vai maksājumu datus, iegādājoties piekļuvi ar autortiesībām aizsargātiem videomateriāliem. Tomēr lietotājam ir jāatspējo drošības iestatījumi, kas ļauj instalēt arī citas lietotnes, nevis tikai tās, kas pieejamas oficiālajā lietotņu tirdzniecības veikalā.

Metodika

Lai veiktu pētījumu, ir jābūt izstrādātai pamatīgai metodikai, lai tiktu galā ar noteiktiem nosaukumiem un tīmekļa vietnēm, kā arī tehniski sarežģītiem uzdevumiem, piemēram, atrasto ļaunprogrammatūru un PNP piemēru atklāšanu un dokumentēšanu. Turpmāk ir sniegts īss metodikas pārskats.

1. *UNICRI* pētījuma I fāzē sadarbībā ar Eiropas Intelektuālā īpašuma tiesību pārkāpumu novērošanas centru (Novērošanas centru) izveidoja ekspertu atbalsta grupu, lai sniegtu konsultācijas par pētniecības metodiku, tīmekļa vietņu atlasi analīzei un veikto pētījuma izvērtēšanu katrā projekta ieviešanas fāzē. Ekspertu atbalsta grupa sastāvēja no Novērošanas centra, tiesību īpašnieku organizāciju, akadēmisko aprindu, tiesībaizsardzības iestāžu un ES iestāžu pārstāvjiem.

2. Vienlaikus izveidoja pētniecības darba grupu. Saistībā ar šo ziņojumu nebija tehniski iespējams[1] izpētīt visas ES valstis, tāpēc II fāzē no ES 28 dalībvalstīm tika nejaušā veidā izvēlētas 10 parauga valstis.

3. III fāzes gaitā tika identificētas populāras filmas, televīzijas programmas, dziesmas un videospēles. Popularitāte ietvēra gan pasaules popularitāti, gan popularitāti tikai vienā no 10 parauga valstīm, kāda tā bija datu apkopošanas posma sākumā 2017. gada 23. jūnijā. Turpmākajās pētījuma fāzēs šos parauga nosaukumus sistemātiski izmantoja tiešsaistes tīmekļa meklējumos, lai atrastu tīmekļa vietnes un mobilās lietotnes, ar kurām pārkāpj autortiesības. Katrs nosaukums atbilda diviem vai vairākiem šādiem kritērijiem:

   - populārs datu apkopošanas laikā ES dalībvalstīs,
   - populārs datu apkopošanas laikā visā pasaulē,
   - vēsturiski populārs visā pasaulē un

[1] Izvēlēto valstu skaitam ir tieša ietekme (palielinoša) uz analizējamo tīmekļa vietņu, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, un atbilstošo bināro failu skaitu. Tāpēc nolēma koncentrēties tikai uz parauga valstīm, lai varētu veiksmīgi veikt pētījuma praktisko daļu noteiktajā laika posmā.

- piederība filmu, televīzijas programmu, dziesmu vai videospēļu kategorijai.

Tika atlasīti pieci filmu nosaukumi, pieci televīzijas nosaukumi, pieci mūzikas nosaukumi un pieci videospēļu nosaukumi, kopumā iegūstot 20 parauga nosaukumus. Tika rūpīgi pārdomāti avoti, ko izmantoja konkrētu nosaukumu popularitātes noteikšanai. Tā ietvēra sistemātisku atlases procesu, lai nodrošinātu, ka datu avots ir pieejams visām dalībvalstīm vai vairumam dalībvalstu.

4. IV fāzes laikā tika identificētas tīmekļa vietnes, ko turēja aizdomās par nelegālas piekļuves nodrošināšanu ar autortiesībām aizsargātiem materiāliem, kas bija populāri visā pasaulē un/vai šajās 10 parauga valstīs 2017. gada 26. jūnijā (ļaunprogrammatūru apkopošanas pirmajā kārtā). Vēlākā pētījuma fāzē analizēja šīs tīmekļa vietnes, lai pārbaudītu ļaunprogrammatūru un potenciāli nevēlamu programmu esamību.

   Metodika tīmekļa vietņu, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, identificēšanai tika izstrādāta ar I fāzē izveidotās ekspertu atbalsta grupas palīdzību, kā arī pēc tam, kad *UNICRI* bija izvērtējis esošo literatūru. Tā tika īpaši izstrādāta, lai izveidotu tādu tīmekļa vietu sarakstu, kas:

   - ietver vietnes, kuras ir populāras dažādās ES dalībvalstīs, nodrošinot plašu ģeogrāfisko pārklājumu;
   - norāda dažāda veida tīmekļa vietnes, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, tostarp straumēšanas tīmekļa vietnes, saistīšanas tīmekļa vietnes, mitināšanas tīmekļa vietnes, datņu glabātājus un gāzmas tīmekļa vietnes;
   - norāda plašu par autortiesību pārkāpumiem aizdomās turēta satura klāstu, tostarp filmas, televīzijas raidījumus, mūziku un videospēles, un
   - norāda tīmekļa vietnes, ar kurām vidusmēra interneta lietotājs sastaptos, cenšoties piekļūt materiāliem, par kuriem ir aizdomas, ka ar tiem pārkāpj autortiesības.

   Izmantoja piecus posmus, lai atlasītu tīmekļa vietnes, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības. Pirmie trīs posmi bija paredzēti vispopulārāko tīmekļa vietņu, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, identificēšanai visās ES dalībvalstīs. Šis paņēmiens atdarināja to, kā vidusmēra lietotājs varētu meklēt tīmekļa vietnes, par kurām ir aizdomas, ka ar tām pārkāpj autortiesības, nenorādot, piemēram, filmas vai dziesmas nosaukumu. Pēdējie divi posmi bija paredzēti tādu tīmekļa vietņu identificēšanai, par ko ir aizdomas, ka ar tām pārkāpj autortiesības, un ar ko vidusmēra interneta lietotājs varētu sastapties, meklējot iespējas lejupielādēt kādu konkrētu populāru nosaukumu, nenorādot tīmekļa vietni. Šis posms bija īpaši svarīgs, ņemot vērā tādu aizdomīgu ļaunprātīgu tīmekļa vietņu esamību, kas piesārņo meklēšanas rezultātus, tādējādi izmantojot populārus tematus, veicot meklētājprogrammu optimizēšanu. Abas pieejas kopā aptvēra dažādus veidus, kā vidusmēra interneta lietotājs varētu mēģināt atrast internetā saturu, par ko ir aizdomas, ka ar to pārkāpj autortiesības.

   Īpašu uzmanību pievērsa tādu ļaunprogrammatūru un PNP vienlaicīgai analīzei, kas raksturīgas mobilajām lietotnēm ierīcēs, piemēram, viedtālruņos un planšetdatoros, jo tas ir viens no jaunākajiem kibernoziegumu draudiem. Analizētas tika vienīgi *Android* ierīces, jo esošajā literatūrā ir norādes, ka *Android* lietojumprogrammu veikalos (piemēram, *Google Play*) ir vairāk ļaunprogrammatūru nekā *Apple iTunes* veikalā. Tika izstrādāta metodika, lai izveidotu tādu mobilo lietotņu paraugu, kas:

   - ir populāras datu apkopošanas laikā visā pasaulē,
   - norāda dažāda veida lietotnes (tostarp straumēšanas lietotnes, gāzmas lietotnes un mitināšanas lietotnes);
   - satur vai nodrošina piekļuvi plašam par autortiesību pārkāpumiem aizdomās turēta satura klāstam (tostarp filmām, televīzijas raidījumiem, mūzikai un mobilajām spēlēm) un

- parāda to, ar ko vidusmēra mobilās ierīces lietotājs sastaptos, mēģinot lejupielādēt vai izmantot lietotni, kura veicina piekļuvi saturam, par ko ir aizdomas, ka ar to pārkāpj autortiesības.

5. V fāzē veica mobilo lietotņu, kā arī ļaunprogrammatūru un PNP apkopošanu identificētajās tīmekļa vietnēs, kas vēlākā posmā jāpārbauda, lai veiktu pienācīgu sistematizāciju. Datu ieguves fāze sastāvēja no divām ļaunprogrammatūru apkopošanas un analīzes kārtām, kas notika 2017. gada vasarā. Pirmajā ļaunprogrammatūru apkopošanas kārtā ieguva 1054 unikālus domēnu nosaukumus, bet otrajā kārtā — 1057 unikālus domēnu nosaukumus visās 10 atlasītajās ES dalībvalstīs. Ļaunprogrammatūras tika apkopotas gan manuāli, gan automātiski, lai simulētu vidusmēra lietotāja pieredzi.

Manuāla apkopošana. Šis paņēmiens ietvēra iepriekšējā fāzē identificēto domēnu manuālu izskatīšanu. Izmantojot manuālu apkopošanu, eksperti varēja simulēt vidusmēra interneta lietotāja pieredzi, klikšķinot uz reklāmām un sazinoties ar tīmekļa vietnēm, uz kurām norādīja uzvednes.

Automātiska apkopošana. Šajā paņēmienā izmantoja automātisku tīmekļa rāpuļprogrammu, ko bija izstrādājuši eksperti, lai sekotu visām pieejamajām saitēm konkrētā tīmekļa vietnē, kas tiek turēta aizdomās par to, ka ar to pārkāpj autortiesības. Vispirms konkrētā tīmekļa vietnē rāpuļprogramma apkopoja informāciju par tīmekļa vietnē esošajām saitēm. Pēc tam rāpuļprogramma atvēra visas šīs saites uz sekundārajām tīmekļa vietnēm. Tad rāpuļprogramma atvēra visas šīs saites uz terciārajām tīmekļa vietnēm. Katrā posmā rāpuļprogramma izguva binārus failus, kas varētu būt noderīgi sekojošai manuālai analīzei, ieskaitot potenciālas vai aizdomās turētas ļaunprogrammatūras un potenciāli nevēlamas programmas. Šo procesu turpināja līdz pat 1000 saitēm vienā tīmekļa vietnē.

6. Kad binārie faili bija iegūti, tos analizēja drošā datorvidē, lai izprastu to iekšējo funkcionalitāti un tos pienācīgi sistematizētu. Tika veikta sākotnēja analīze, izmantojot atvērtā koda rīkus, lai rezultātus varētu korelēt ar kiberdraudu ziņojumiem. Pēc tam apkopotos programmatūru paraugus nosūtīja analīzei uz *EMAS*, savukārt *EMAS* analīzi salīdzināja ar sākotnējiem rezultātiem.

Metodikas pārskats

Atklātie ļaunprogrammatūru un PNP paraugi

Pirmās apkopošanas kārtas laikā 2017. gada 28. jūlijā tika automātiski pārbaudītas 5240 tīmekļa vietnes (1054 unikālas), iegūstot 617 saistītus failus (mūzikas, video, gāzmas failus un programmatūras), kuru kopējais izmērs bija 47 GB. Šo nešķiroto failu kopumam bija nepieciešama turpmāka analīze, lai izlemtu, kuri no apkopotajiem failiem ir piemēroti pētījumam. Paraugi no tīmekļa vietnēm, ar ko pārkāpj autortiesības, bija līdzīgi visās 10 parauga valstīs katrā no mediju veidiem (televīzijas programmas, filmas, mūzika un videospēles). Rezultātā no parauga valstīm nejaušā veidā tika izvēlēta Beļģija un tika pārbaudītas visas tīmekļa vietnes, kuras bija identificētas kā tādas, ar ko pārkāpj autortiesības, lai pārbaudītu ļaunprogrammatūru vai citādi nevēlamu programmu esamību. Pēc otrās apkopošanas kārtas 2017. gada 10. augustā kopumā automātiski izguva 3665 failus no tīmekļa vietnēm visās valstīs, kuru kopējais izmērs bija 167 GB. Kopumā visās valstīs no 5606 tīmekļa vietnēm izguva 1057 unikālus vietrāžus URL, kas padarīja neiespējamu to manuālu pārbaudi pilnībā.

Pēc apkopoto failu sākotnējās analīzes abās ļaunprogrammatūru apkopošanas kārtās izguva 106 unikālus *MS Windows*, *Android* un *MAC OS* binārus failus. Konkrētāk, pirmās kārtas laikā atlasīja 41 failu un 65 failus atlasīja otrās kārtas laikā, proti: 2 *Mac*, 15 *Android* un 89 *MS Windows* operētājsistēmas failus. No šiem failiem 21 failu var uzskatīt par labi zināmām ļaunprātīgām programmām, ko *VirusTotal* platformā atzīmējuši daudzi antivīrusu programmu pārdevēji. Tie ietver failus, kuri lejupielādēti tieši no noteiktām tīmekļa vietnēm, par ko ir aizdomas, ka ar tām pārkāpj autortiesības, kā arī failus, kas izveidoti lejupielādēto failu izpildes laikā. Pēc tam apkopotos failus analizēja smilšu kastes vidē un nosūtīja *EMAS* iespējamu ļaunprātīgu darbību padziļinātai analīzei. Kopumā *EMAS* ziņojumos visiem binārajiem failiem atklāja 821 atšķirīgu ļaunprātīgu notikumu *(Windows 7 SP1*, *Windows7 SP1 64-bit*, *Windows 10 64-bit*, *Windows XP SP3*). Dažos ziņojumos nebija nevienas aizdomīgas darbības, savukārt citos ziņojumos bija pat 10 iepriekš zināmas ļaunprātīgas darbības. Pētījuma pēdējā posmā korelēja sākotnējās analīzes

un *EMAS* ziņojumu rezultātus. Rezultātu kvantitatīvais kopsavilkums attēlots turpmāk sniegtajā tabulā.

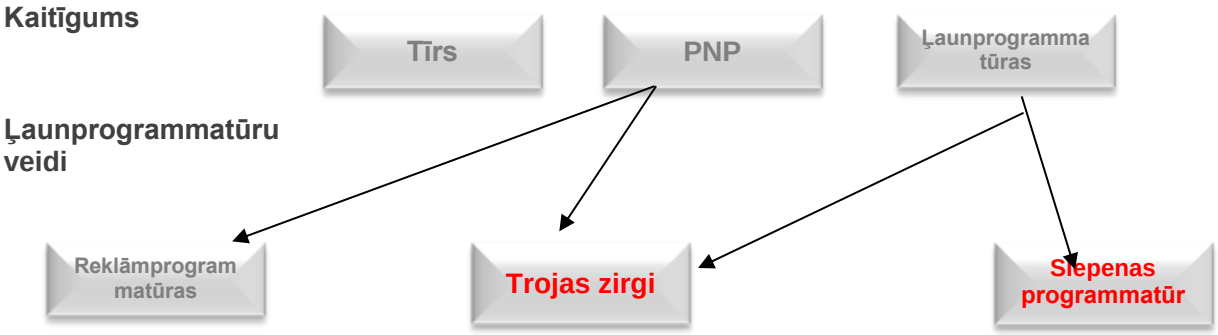
	1. kārta	**2. kārta**
Datums	2017. gada 28. jūlijs	2017. gada 10. augusts
Atklātās tīmekļa vietnes ES 10 valstīs	5240	5606
Unikālas tīmekļa vietnes	1054	1057
Saistītie faili	617	3665[2]
Saistīto failu izmērs, GB	47	167
Iesniegts *EMAS*		
Android	3	12
Mac OS	2	–
MS Windows	36	53
Kopējais izmērs, baiti	175 600 117	522 991 095

Eiropola Ļaunprogrammatūru analīzes risinājums (*EMAS*)

Eiropola Ļaunprogrammatūru analīzes risinājums (*EMAS*) ir dinamisks, automatizēts ļaunprogrammatūru analīzes risinājums, ko Eiropols nodrošina ES dalībvalstīm. *EMAS* piedāvā iespēju sagatavot analīzes ziņojumus, taču visrevolucionārākā iespēja ir nodrošināt policijas izmeklētājiem informācijas iegūšanu. Automātiskās kontrolpārbaudēs var atklāt saikni starp uzbrukumiem, kas izdarīti dažādās valstīs, izmantojot vienas un tās pašas ļaunprogrammatūras, vai arī to, ka tos ar vienas ļaunprogrammatūru grupas palīdzību ir veikusi viena un tā pati noziedzīgā organizācija, pieslēdzoties vieniem un tiem pašiem domēniem, kā arī to saistību ar dažādiem izmeklēšanas procesiem gan ES, gan ārpus tās. *EMAS* 2015. gadā tika pilnībā automatizēta, nodrošinot tiešu pieeju tām tiesībaizsardzības iestādēm, kas ar Eiropolu ir noslēgušas darbības nolīgumus. 2015. gadā: *EMAS* izanalizēja 525108 failus, no kuriem 356863 failus identificēja kā ļaunprātīgus.

Kā parādīts turpmāk sniegtajā attēlā, apkopotos bināros failus atkarībā no to kaitīguma var vispārīgi sistematizēt kā nekaitīgus failus, kas nenodara nekādu ļaunumu), PNP un kaitīgas ļaunprogrammatūras. Turklāt PNP tika atklātas ne tikai *Microsoft Windows*, bet arī *Android* un *Mac OS*, kas liecina, ka ļaunprogrammatūru izstrādātāji cenšas ietekmēt pēc iespējas vairāk lietotāju, izmantojot dažādas platformas. PNP un ļaunprogrammatūras var turpmāk tikt iedalītas, pamatojoties uz galvenajiem ļaunprogrammatūru veidiem, t. i., Trojas zirgiem, reklāmprogrammatūrām un slepenām programmatūrām. Vairums atklāto programmatūru piederēja PNP kategorijai. PNP funkcionēšanu var saistīt ar vienu no šādiem darbības veidiem: neīstu spēļu instalēšana, kam nepieciešami personas un bankas konta dati, "lietderīgu" programmu lejupielādēšana, piespiežot lietotāju iegādāties maksas versijas abonementu, vai bezmaksas programmu instalēšana, lai piekļūtu platformām, ar ko pārkāpj autortiesības. Šīs lietotnes var apdraudēt lietotāja personas datus un datora konfigurāciju. Izmantojot sociālās inženierijas trikus, var tikt izpausti dažāda veida privāti dati, piemēram, maksājumu karšu dati, personu identificējoša informācija, kā arī sociālo tīklu kontu dati. Pētījumā arī identificēja 15 *Android* lietotnes no trešo personu lietojumprogrammu veikaliem, kā arī pēc sākotnējās analīzes secināja, ka šādas lietotnes var izplatīt saturu, ar ko pārkāpj autortiesības, un izpaust personas datus.

[2] Atšķirību starp 1. un 2. kārtas rezultātiem var izskaidrot ar to, ka automatizētās apkopošanas 2. kārtā bija tīmekļa vietnes, kas katrā savā tīmekļa lapā publicēja vairākas failu kopas.



Draudi lietotājiem

Abu tīmekļa vietņu identificēšanas un ļaunprogrammatūru analīzes kārtu laikā netika atklāts neviens izspiedējprogrammatūras binārais fails. Kopumā vairumu apkopoto ļaunprogrammatūru var raksturot kā Trojas zirgus, kas nozīmē, ka tīmekļa vietnēs tās var izlikties par nekaitīgām bieži izmantotām vai populārām programmatūrām, bet patiesībā tās var nozagt vai izpaust privātu informāciju. Nepieredzējis lietotājs var ļoti uzticēties šādai programmatūrai un var nespēt pamanīt nekādas anomālijas. Turklāt šādu programmatūru statiskā analīze un dinamiskā uzvedības novērošana bez avota koda var neatklāt to darbību pilnībā. Pēc sākotnējās ļaunprogrammatūru analīzes *EMAS* analīzē tika atklātas daudz konkrētākas kaitīgas darbības. Šādas programmatūras instalēšana lietotāja datorā var izraisīt nopietnas sekas, ne tikai radot finansiālus zaudējumus, bet arī personas datu zādzību un citus nevēlamas piekļuves un kontroles riskus. Šādu darbību rezultātā var tikt apkopota un trešām personām šifrētā vai atklātā teksta formātā pārsūtīta personas informācija. Šādi dati var ietvert, piemēram, bankas konta datus no pārlūkprogrammas, datora aparatūras/programmatūras konfigurācijas informāciju vai jebko, kas tiek rakstīts ar tastatūru.

KONKRĒTU TĀDU TĪMEKĻA VIETŅU ĻAUNPROGRAMMATŪRU IDENTIFICĒŠANA UN ANALĪZE, PAR KURĀM IR AIZDOMAS, KA AR TĀM TIEK PĀRKĀPTAS AUTORTIESĪBAS

KOPSAVILKUMS

2018. gada septembris