EUIPO
DEN EUROPÆISKE UNIONS
KONTOR FOR INTELLEKTUEL EJENDOMSRET

IDENTIFIKATION OG ANALYSE AF MALWARE PÅ UDVALGTE WEBSTEDER, SOM MISTÆNKES FOR AT KRÆNKE OPHAVSRETTIGHEDER

RESUMÉ

September 2018

Sammendrag

Indhold, der mistænkes for at krænke ophavsrettigheder, udgør en betydelig krænkelse af intellektuelle ejendomsrettigheder. Der er nogle websteder, der deler dette indhold offentligt, i visse tilfælde endog gratis, uden registrering. Sammen med dette indhold lokker websteder, der sædvanligvis distribuerer forskellige former for malware og potentielt uønskede programmer (PUP'er), ofte brugere til at downloade og åbne disse filer. Undersøgelsen giver et overblik over de seneste eksempler på malware og PUP'er, der findes på websteder, der mistænkes for at krænke ophavsretten. Disse programmer anvender vildledende metoder og social engineering - såsom tomme spilinstallationer og tilsyneladende "nyttigt" software - til at narre slutbrugere til at videregive deres følsomme oplysninger. I løbet af undersøgelsen blev der fundet en bred vifte af PUP'er såsom enten "nyttigt" software, falske spilinstallationsprogrammer og klienter til videostreamingplatforme. Denne software udgør ikke nødvendigvis direkte farer for brugerens software eller hardware. Imidlertid kan en bruger ved hjælp af social engineering blive narret til at offentliggøre følsomme personoplysninger eller betalingskortoplysninger. Desuden kan oplysninger om selve computeren blive lækket til andre parter uden udtrykkeligt samtykke fra brugeren.

Forskerhold

Forskerholdet bestod af Francesca Bosco, UNICRI-programmedarbejder, og Andrii Shalaginov, ph.d.--forskningsstipendiat i informationssikkerhed ved afdelingen for informationssikkerhed og kommunikationsteknik (digitale kriminaltekniske gruppe) ved fakultetet for informationsteknologi og elektroteknik på Norges universitet for videnskab og teknik.

Ansvarsfraskrivelse

I denne forbindelse skal det understreges, at forskningen udelukkende havde til formål at fastlægge de tekniske karakteristika for malware og PUP'er, som man var stødt på i løbet af undersøgelsen, og som internetbrugerne kunne komme ud for, når de søgte efter indhold, der mistænkes for at krænke ophavsretten. Listen over malware og PUP'er, der er dokumenteret, kan ikke betragtes som udtømmende. Det var heller ikke formålet med undersøgelsen (eller resultaterne heraf) at foretage en vurdering af den samlede sandsynlighed eller risiko for malware og PUP-infektion hos en internetbruger, når der søges efter materiale, der mistænkes for at krænke ophavsretten.

Forord

Aktiviteter på internettet, der mistænkes for at krænke ophavsretten, kan finansieres på en række forskellige måder, herunder abonnementsafgifter, bidrag, betaling for hjælpetjenester og indtægter fra onlinereklamer.

Det er dog ikke alle midler til finansiering, der er lige så harmløse som de anførte eksempler. I årevis har spredningen af malware og andre former for potentielt uønskede programmer været af central betydning i forbindelse med finansiering af aktiviteter på internettet, der mistænkes for at krænke ophavsretten.

Almindelige internetbrugere er begyndt at blive opmærksomme på risikoen for infektion, når de tilgår websteder eller mobilapplikationer, der mistænkes for at krænke ophavsretten.

EUIPO's ungdomsresultattavle for 2015 viste, at 52 % af de unge mener, at sikkerheden på et websted er vigtig for adgangen til onlineindhold. I alt erklærede 78 % af de unge, at de ville tænke sig om en ekstra gang, hvis de vidste, at der var risiko for, at computeren eller enheden kunne blive inficeret med virus eller malware. I alt erklærede 84 % af de unge, at de ville tænke sig om en ekstra gang, hvis de vidste, at der var risiko for, at kreditkortoplysninger kunne blive stjålet.

Under researchen til denne undersøgelse redegjorde kontoret for en meget teknisk udfordrende opgave, nemlig at afsløre og dokumentere eksempler på malware og PUP'er, som en internetbruger kunne støde på, når denne forsøgte at få adgang til populære piratkopierede film, musik, videospil og tv-serier.

I denne forbindelse skal det understreges, at forskningen udelukkende havde til formål at fastlægge de tekniske karakteristika for malware og PUP'er, som man var stødt på i løbet af undersøgelsen, og som internetbrugerne kunne støde på, når de søgte efter indhold, der mistænkes for at krænke ophavsretten. Listen over malware og PUP'er, der er dokumenteret, kan ikke betragtes som udtømmende, og det var heller ikke formålet med undersøgelsen (eller resultaterne heraf) at foretage en vurdering af den samlede sandsynlighed eller risiko for malware og PUP-infektion hos en internetbruger på jagt efter materiale, der mistænkes for at krænke ophavsretten.

Forskningen blev gennemført i flere faser i tæt samarbejde med Det Europæiske Center til Bekæmpelse af It-Kriminalitet (EC3) under Europol.

Resultaterne viser en række forskellige malware- og PUP-trusler, som internetbrugere kan støde på, når de søger efter indhold, der mistænkes for at krænke ophavsretten. Størstedelen af den dokumenterede malware og PUP'er kan betegnes som trojanske heste eller anden uønsket software, der kan få uberettiget adgang til internetbrugernes personoplysninger. Disse eksempler vil være relevante og af interesse ikke kun for rettighedsindehavere af intellektuelle ejendomsrettigheder, men også for de retshåndhævende myndigheder og sidst, men ikke mindst for forbrugere, der er bekymrede for, at nogen får adgang til deres personlige oplysninger uden deres tilladelse.

Sammendrag

Undersøgelsen giver et overblik over de seneste eksempler på malware og potentielle uønskede programmer (PUP'er), der findes på websteder, som mistænkes for at krænke ophavsretten. Disse programmer anvender vildledende teknikker og social manipulation (social engineering) - såsom tomme spilinstallationer og tilsyneladende "nyttigt" software - til at narre slutbrugere til at oplyse deres følsomme oplysninger.

Målet med denne undersøgelse er at opdage og dokumentere skadelig eller på anden måde uønsket software, der spredes på udvalgte websteder, som mistænkes for at krænke ophavsretten, og at kategorisere de prøver, der er fundet i overensstemmelse med forskellige malwareklassifikationer. I denne forbindelse skal det understreges, at forskningen udelukkende havde til formål at fastlægge de tekniske karakteristika for malware og PUP'er, som man var stødt på under undersøgelsen, og som internetbrugerne kunne støde på, når de søgte efter indhold, der mistænkes for at krænke ophavsretten. Listen over malware- og PUP'er, der er dokumenteret, kan ikke betragtes som udtømmende. Det var heller ikke formålet med undersøgelsen (eller resultatet heraf) at foretage en vurdering af den samlede sandsynlighed eller risiko for malware og PUP-infektion hos en internetbruger på jagt efter efter materiale, der mistænkes for at krænke ophavsretten. I forbindelse med denne undersøgelse anses tv-shows, film, musik og videospil som ophavsretligt beskyttet indhold.

Undersøgelsens resultater

Indhold, der mistænkes for at krænke ophavsretten, udgør en betydelig krænkelse af intellektuelle ejendomsrettigheder. Der er nogle websteder, der deler dette indhold offentligt, i visse tilfælde endog gratis, uden registrering. Sammen med sådant indhold distribuerer webstederne sædvanligvis forskellige former for malware og PUP'er, der lokker brugerne til at downloade og åbne sådanne filer. Det viste sig under identificeringen af websteder, jf. Alexas 500 mest anvendte websteder, samt ved hjælp af gennemsnitlige brugersøgninger på velkendte søgemaskiner som Google, Yahoo og Bing, at disse websteder ændrede sig i løbet af undersøgelsens to faser. Denne ændring skyldes sandsynligvis en indsats fra søgemaskiner til at fjerne links til websteder, der mistænkes for at krænke ophavsretten, mens der fortsat dukker nye websteder op, som mistænkes for at krænke ophavsretten. Et interessant resultat i forbindelse med identifikation af websteder er, at langt størstedelen af webstederne ligger i USA eller har domænenavne, der er hostet i USA. Tværtimod er kun få placeret på servere i EU. Dertil kommer, at .com og .net er de mest hyppige domænenavne på topniveau, der anvendes på websteder, der mistænkes for at krænke ophavsretten. Dette kan skyldes, at de i modsætning til landespecifikke domæner ikke nødvendigvis kræver identifikation af brugeren med pas eller andre identifikationsdokumenter. Gennemsnitligt blev 20 % af de nye websteder tilføjet og 20 % af de gamle websteder blev fjernet mellem de to identifikationsrunder. Desuden blev næsten 8 % af de websteder, der blev identificeret i begge runder, karakteriseret som skadelige af platformen VirusTotal. Med hjælp fra forskellige indholdsstyringssystemer er det nu næsten så let som ingenting at oprette et websted og levere indhold til brugere, endda skadelige programmer.

Inden indsamlingen af malware gennemførtes der i denne undersøgelse en skrivebordsgennemgang af malwaretrusler i 2017 og en kategorisering af de mest avancerede. Denne viden blev yderligere anvendt i forbindelse med analysen af malware for alment accepterede principper inden for identificering af malware og grupper. I alt blev der indsamlet 106 filer under begge dataindsamlingsrunder. Disse omfatter filer, der downloades direkte fra udvalgte websteder, der mistænkes for at krænke ophavsretten, samt filer, der blev oprettet under kørslen af de downloadede filer. I løbet af undersøgelsen blev der fundet en bred vifte af PUP'er såsom "nyttigt" software, falske spilinstallationsprogrammer og klienter til videostreamingplatforme. Sådan software udgør ikke nødvendigvis direkte farer for brugerens software eller hardware. Imidlertid

kan en bruger ved hjælp af social engineering blive lokket til at offentliggøre følsomme personoplysninger eller betalingskortoplysninger. Desuden kan oplysninger om selve computeren lækkes til andre parter uden udtrykkeligt samtykke fra brugeren.

Den indsamlede malware blev oprindeligt analyseret med anvendelse af open source-værktøjer for at forstå den interne logik, afsløre eventuelle skadelige aktiviteter og evaluere deres relevans for den nuværende undersøgelse. Ud over den foreløbige analyse ved hjælp af open source-værktøjer blev det indsamlede malware analyseret af Europols Malware Analysis Solution (EMAS)-platform. Dette resulterede i opdagelsen af en lang række forskellige artefakter og skadelige aktiviteter. EMAS-rapporterne indeholder en omfattende analyse af filer, som anvender fire versioner af MS Windows, hvor netværkstrafik, funktionskald og diskaktiviteter er grundigt logført med henblik på yderligere analyse. Derudover fremhæver platformen eventuelle mistænkelige aktiviteter, der blev afsløret under kørslen af filer. Efter at have analyseret alle rapporterne blev 35 typer skadelige aktiviteter registreret af EMAS, der kategoriseres i 17 klasser af skadelige hændelser. Disse spænder fra generelle afvigelser (f.eks. kørsel af systemprocesser eller undersøgelse af processer i datalagre) til umiskendeligt skadelige tiltag (f.eks. keylogger, rootkit og manipulering af netværkstrafik).

De binære stikprøver af malware og PUP'er, der blev indsamlet, afslørede nogle få generelle forretningsmodeller: "nyttige" programmer, der hævder at rydde op i gamle filer på en brugers computer efter betaling af abonnement, spilinstallationssimulatorer, der kræver brugerens personoplysninger, og gratis programmer, der giver adgang til platforme, der distribuerer piratkopieret indhold, f.eks. gennem BitTorrent-tracker. De to runder med identifikation af websteder og indsamling af malware har givet lovende resultater med hensyn til forståelsen af de metoder, der anvendes til spredning af malware, og de former for social engineering, der anvendes til indsamling af følsomme personoplysninger og identificerbare oplysninger. Desuden er mobilenheders øgede popularitet i de seneste år åbenbar, eftersom mange PUP'er til Android OS er tilgængelige via distributionsplatforme, der mistænkes for at indeholde ophavsretsbeskyttet indhold. Som følge af korrelerede analyser blev der draget den konklusion, at trusselsbilledet for malware, som distribueres via websteder, der krænker ophavsretten, er mere avanceret, end man umiddelbart skulle tro. Nogle af programmerne kan også klassificeres som trojanske heste, adware, backdoor og agent. Dette forværres yderligere af, at der også blev fundet mange specifikke malwarefamilier, f.eks. WisdomEyes, DealPly og FileRepMalware. Desuden gælder en sådan samlet kategorisering også for Android-platformen og ikke kun for Microsoft Windows. Der er en lang række trusler mod brugernes aktiver, herunder, men ikke begrænset til, tyveri af følsomme oplysninger, personoplysninger, konfigurationsoplysninger om hardware og ændring af nettrafik. Selv om den identificerede software kan være en PUP, kan den ikke desto mindre have en indvirkning på brugerne, navnlig i tilfælde, der involverer en gennemsnitlig bruger, som måske ikke fuldt ud har kendskab til grundlæggende sikkerhedspraksis og -foranstaltninger på internettet.

Et eksempel på undersøgelsens resultater er vist nedenfor.

Websted 03	Websted 09	Websted 08
Webstedet narrer brugere til at anvende et falsk spilinstallationsprogram, hvor hele processen med at indhente en brugers følsomme oplysninger er ændret mellem første og anden runde af indsamlingen af malware. Brugeren af denne tjeneste downloader et arkiv med indhold, der er maskeret som spilrelaterede filer og ikke en eksplicit, binær eksekverbar fil, der kan registres af enhver form for antivirus som skadelig. De krypterede arkiver giver kun adgang til filnavne, men ikke filernes materielle indhold.	På webstedet kan du få adgang til alle former for videoindhold, der er tilgængelig gennem torrent trackers ved hjælp af et softwareværktøj. Dette værktøj kræver færre brugerinteraktioner i forhold til andre BitTorrent trackers. Det kræver kun nogle få klik at downloade indhold fra ukendte kilder, mens brugeren hverken er beskyttet eller har kontrol over, hvad der downloades.	(Android) Webstedet giver adgang til en række gratis mobilapplikationer uden registrering. En af de to applikationer giver ubegrænset adgang til streaming af tv-shows og film. Der er ingen udtrykkelig anmodning om at oplyse brugerfølsomme oplysninger eller betalingsoplysninger for at kunne købe adgang til ophavsretligt beskyttede videoer. Brugeren skal imidlertid deaktivere de sikkerhedsindstillinger, der vil gøre det muligt at installere andre applikationer end dem, der kommer fra et officielt applikationsmarked.

Metode

For at kunne udføre undersøgelsen var det nødvendigt at anvende en god metode til at håndtere udvælgelsen af titler og websteder samt den teknisk udfordrende opgave at afsløre og dokumentere eksemplerne på den malware og de PUP'er, der blev fundet. En kort oversigt over metoden er beskrevet nedenfor:

1. Under fase I i UNICRI-undsøgelsen blev der i samarbejde med Det Europæiske Observationscenter for Krænkelser af Intellektuelle Ejendomsrettigheder (observationscenter) nedsat en ekspertgruppe med henblik på rådgivning om forskningsmetoden, udvælgelse af de websteder, der anvendes til analyse, og vurdering af den forskning, der er foretaget i hver af projektgennemførelsens faser. Ekspertgruppen bestod af repræsentanter fra observationscentrets interessenter, organisationer af rettighedsindehavere, akademiske kredse, retshåndhævende myndigheder og EU-agenturer.

2. Sideløbende hermed blev forskerholdet udvalgt. Inden for rammerne af denne rapport var det ikke teknisk muligt[1] at undersøge alle EU's medlemsstater. Derfor blev 10 lande tilfældigt udvalgt blandt de 28 EU-medlemsstater i fase II.

3. I fase III blev der identificeret populære film, tv-programmer, sange og videospil. Popularitet omfattede verdensomspændende popularitet samt popularitet i kun et eller flere af de 10 medlemsstater ved starten af dataindsamlingsperioden, den 23. juni 2017. I de efterfølgende faser af undersøgelsen blev disse udvalgte titler systematisk anvendt i internetsøgninger til at finde websteder og mobile applikationer, der krænker ophavsretten. Hver titel opfyldte to eller flere af følgende kriterier:

[1] Antallet af udvalgte lande vil få en direkte indvirkning (stigning) på antallet af de udvalgte websteder, der mistænkes for at krænke ophavsretten, og tilhørende binære filer, der skal analyseres. Det blev derfor besluttet kun at koncentrere sig om et udsnit af landene for at kunne gennemføre den praktiske del af undersøgelsen inden for en bestemt tidsramme.

- populære på det tidspunkt, hvor dataindsamlingen finder sted i EU-medlemsstater
- populære på det tidspunkt, hvor dataindsamlingen finder sted på globalt plan
- populære historisk set på globalt plan, og
- kategoriserede som film, tv-programmer, sang eller videospil.

Der blev udvalgt fem filmtitler, fem tv-titler, fem musiktitler og fem videospiltitler, hvilket resulterede i 20 prøvetitler i alt. Der blev taget nøje hensyn til de kilder, der anvendes til at identificere en bestemt titels popularitet, hvilket indebar en systematisk udvælgelsesproces for at sikre, at kildedata ville være tilgængelige for alle eller de fleste medlemsstater.

4. Fase IV identificerede websteder, der var mistænkt for at give ulovlig adgang til ophavsretligt beskyttet materiale, der var populært på verdensplan og/eller blandt de 10 prøvelande pr. 26. juni 2017 (første runde af indsamlingen af malware). I en senere fase af undersøgelsen blev disse websteder analyseret for forekomsten af malware og potentielt uønskede programmer.

   Metoden til identifikation af websteder, der mistænkes for at krænke ophavsretten, blev udviklet med input fra den ekspertstøttegruppe, der blev identificeret i fase I, samt efter en gennemgang af UNICRI af den eksisterende litteratur. Den var specielt udformet med henblik på at generere en stikprøve af websteder, som:

   - er populære i forskellige EU-medlemsstater og sikrer bred geografisk dækning
   - repræsenterer forskellige typer websteder, der mistænkes for at krænke ophavsretten, herunder streamingwebsteder, links til websteder, værtswebsteder, cyberlockers og torrent-websteder
   - repræsenterer en bred vifte af indhold, der mistænkes for at krænke ophavsretten, herunder film, tv-titler, musik og videospil, og
   - repræsenterer websteder, som den gennemsnitlige bruger på internettet kan støde på, når denne forsøger at få adgang til materiale, der mistænkes for at krænke ophavsretten.

   Der blev gjort brug af fem trin til at udvælge websteder, der mistænkes for at krænke ophavsretten. De første tre trin var udformet med henblik på at identificere de mest populære websteder, der mistænkes for at krænke ophavsretten, på tværs af EU's medlemsstater. Denne metode efterligner de scenarier, hvor en gennemsnitlig bruger kan søge efter websteder, der mistænkes for at krænke ophavsretten, uden f.eks. at angive titlen på en film eller en sang. De sidste to trin er udformet med henblik på at identificere websteder, der mistænkes for at krænke ophavsretten, som en gennemsnitlig bruger kan støde på under søgning efter forskellige måder at downloade en bestemt populær titel på uden at angive et websted. Dette trin var særligt vigtigt set i lyset af forekomsten af formodede skadelige websteder, der manipulerer søgeresultater, hvorved de udnytter tendenser inden for emner ved hjælp af søgemaskineoptimering. Tilsammen dækkede de to fremgangsmåder de forskellige måder, en gennemsnitlig bruger på internettet kan anvende for at forsøge at finde materiale på internettet, der mistænkes for at krænke ophavsretten.

   Der blev lagt særlig vægt på en sideløbende analyse af malware og PUP'er, der er specifikke for mobile applikationer på enheder såsom smartphones og tablets, som en af de vigtigste nye trusler inden for it-kriminalitet Analysen var begrænset til Android-enheder som følge af indikationer i den eksisterende litteratur om en større tilstedeværelse af malware i Android-applikationsbutikker (f.eks. Google Play) end i Apple iTunes store. Metoden blev udformet med henblik på at generere en stikprøve af mobile applikationer, som:

   - er populære på det tidspunkt, hvor dataindsamlingen finder sted på globalt plan
   - repræsenterer forskellige typer applikationer (for at inkludere streamingapplikationer, torrent-applikationer og hostingapplikationer)
   - indeholder eller giver adgang til et stort udvalg af indhold, der mistænkes for at krænke ophavsretten (for at inkludere film, tv-titler, musik og mobilspil), og

- repræsenterer, hvad en gennemsnitlig bruger af en mobil enhed vil støde på ved forsøg på at downloade eller bruge en applikation, der letter adgangen til mistænkeligt ophavsretligt beskyttet indhold.

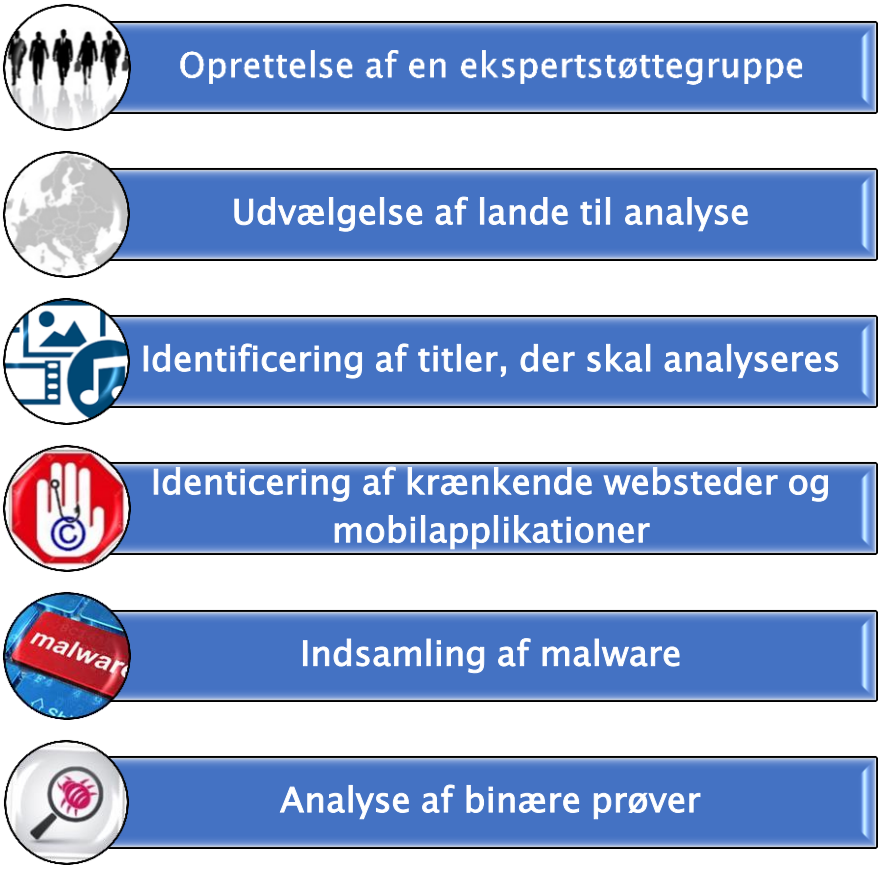
5. Fase V bestod i indsamling af malware og PUP'er i tillæg til mobile applikationer på de identificerede websteder, som senere skulle undersøges med henblik på en korrekt kategorisering. Dataindsamlingsfasen omfattede to runder af indsamling og analyse af malware i løbet af sommeren 2017. Den første runde af indsamling af malware resulterede i 1 054 unikke domænenavne, og den anden runde gav 1 057 unikke domænenavne i de 10 udvalgte EU-medlemsstater. Malware blev indsamlet både manuelt og automatisk for at simulere en gennemsnitlig brugers oplevelse.

Manuel indsamling. Denne metode omfattede manuel gennemgang af de domæner, der blev identificeret i den foregående fase. Ved hjælp af manuel indsamling var eksperten i stand til at simulere den gennemsnitlige internetbrugers oplevelse ved at klikke på reklamer og interagere med de websteder, der krævede instrukser.

Automatiseret indsamling. Denne metode anvendte en automatiseret webcrawler, der var udformet af en ekspert til af følge alle tilgængelige links på et givet websted, der mistænkes for at krænke ophavsretten. Først vil crawleren på et givet websted indsamle oplysninger fra linkene på webstedet. Derefter vil crawleren følge hver af disse links til sekundære websteder. Dernæst vil crawleren følge hver af disse links til tertiære websteder. På hvert trin indhentede crawleren binære filer, som kunne være af interesse for efterfølgende manuel analyse, herunder potentiel eller mistænkelig malware og potentielt uønskede programmer. Denne proces fortsatte med op til 1 000 links pr. websted.

6. Efter indsamlingen af de binære filer blev de analyseret i et sikkert computermiljø for at forstå deres interne funktion og for korrekt kategorisering. En foreløbig analyse blev foretaget ved hjælp af open source-værktøjer for at kunne sammenholde resultaterne med rapporter om it-trusler. Indsamlede softwareprøver blev derefter leveret til EMAS til analyse. EMAS-analysen blev derefter sammenholdt med de foreløbige resultater.

Overblik over metoden



Detekterede malware og PUP'er

Pr. 28. juli 2017 var 5 240 websteder (1 054 unikke) automatisk blevet kontrolleret i den første indsamlingsrunde. Disse indeholdt 617 relevante filer (musik, video, torrent-filer og -software) med en samlet størrelse på 47 GB. Denne usorterede serie af filer krævede yderligere analyser for at afgøre, hvilke indsamlede filer der var relevante for undersøgelsen. Webstederne, der krænkede ophavsretten, var ens i alle 10 prøvelande, når det gælder hver af de forskellige medietyper (tv-programmer, film, musik og videospil). Som følge heraf blev Belgien udvalgt tilfældigt fra prøvelandene, og alle websteder udpeget som websteder, der krænker ophavsretten i Belgien, blev manuelt kontrolleret for skadelig eller anden vis uønsket software. Efter den anden indsamlingsrunde blev i alt 3 665 filer automatisk hentet fra webstederne for alle lande med en samlet størrelse på 167 GB. Det samlede antal unikke webadresser for alle lande var 1 057 ud af 5 606 websteder, hvilket gjorde det umuligt at kontrollere dem alle manuelt.

Efter en foreløbig analyse af de indsamlede filer blev der udtrukket 106 unikke binære filer for MS Windows, Android og Mac OS som et resultat af begge runder med indsamling af malware. Mere specifikt blev der udvalgt 41 filer i den første runde, og 65 blev udvalgt i den anden runde, navnlig: 2 for Mac, 15 for Android og 89 for MS Windows. 21 af disse filer kan betragtes som velkendte skadelige programmer som angivet af flere antivirusforhandlere, der er aggregeret af platformen VirusTotal. De omfatter filer, der downloades direkte fra udvalgte websteder, som mistænkes for at krænke ophavsretten, samt filer, der blev oprettet under kørslen af de downloadede filer. Efterfølgende blev indsamlede softwareprøver analyseret i et sandkassemiljø og leveret til EMAS med henblik på en mere avanceret analyse af mulige skadelige aktiviteter. I alt blev der opdaget 821 forskellige skadelige hændelser i fire EMAS-rapporter (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3) for alle binære filer. Nogle af rapporterne havde ingen mistænkelige aktiviteter, og nogle af dem havde op til 10 kendte skadelige aktiviteter. I undersøgelsens sidste fase var der en indbyrdes sammenhæng mellem resultaterne af den

foreløbige analyse og EMAS-rapporterne. Det kvantitative sammendrag af resultaterne fremgår af nedenstående tabel.

	Runde 1	Runde 2
Dato	28. juli 2017	10. august 2017
Fundne websteder i 10 EU-lande	5 240	5 606
Unikke websteder	1 054	1 057
Relevante filer	617	3 665[2]
Størrelsen af de relevante filer, GB	47	167
Leveret til EMAS		
Android	3	12
MAC OS	2	–
MS Windows	36	53
Størrelse i alt (byte)	175 600 117	522 991 095

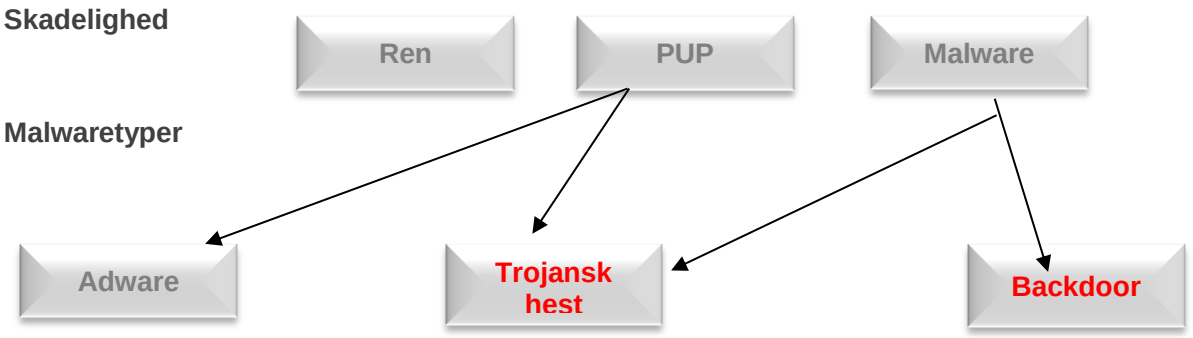
Europol Malware Analysis Solution (EMAS)

Europol Malware Analysis Solution (EMAS) er en dynamisk, automatiseret analyse af malware, som Europol stiller til rådighed for EU's medlemsstater. EMAS giver mulighed for at udarbejde analyserapporter, men dets mest revolutionerende funktion er at fremskaffe efterretninger til politiefterforskninger. Automatiseret krydskontrol kan vise forbindelser mellem angreb, der udføres i forskellige lande med den samme malware, eller med den samme kriminelle organisation bag den samme malewaregruppe, som forbinder de samme domæner og er relateret til forskellige efterforskninger i eller uden for EU. I 2015 blev EMAS automatiseret fuldt ud for at give direkte adgang til de retshåndhævende myndigheder, som Europol har operationelle aftaler med. I 2015 blev 525 108 filer analyseret i EMAS, hvoraf 356 863 blev identificeret som skadelige.

Som det fremgår af figuren nedenfor, kan indsamlede binære filer generelt kategoriseres efter skadelighed, som harmløse (filer, der ikke medfører skader), PUP'er og skadelig malware. Desuden blev PUP'er ikke kun fundet for Microsoft Windows, de blev også fundet for Android og Mac OS, hvilket tyder på, at udviklere af malware forsøger at påvirke så mange brugere som muligt ved hjælp af forskellige platforme. PUP'er og malware kan differentieres yderligere på grundlag af de vigtigste malwaretyper, dvs. trojanske heste, adware og backdoor. Størstedelen af den software, der blev fundet, faldt ind under kategorien PUP. PUP'ers funktion kan knyttes til en af følgende forretningsmodeller: falske spilinstallationsprogrammer, der kræver personlige oplysninger og bankkontooplysninger, download af "nyttige" programmer, som tvinger brugerne til at købe et abonnement til en udbetalt version eller installation af gratis programmer for adgang til platforme, der krænker ophavsretten. Disse applikationer kan bringe brugernes personlige oplysninger og computerkonfiguration i fare. Gennem social engineering kan forskellige former for private oplysninger, f.eks. oplysninger om betalingskort, personlige identificerbare oplysninger og sociale mediers kontooplysninger ligeledes videregives. På samme måde blev der i undersøgelsen identificeret 15 Android-applikationer fra markedet for tredjepartsapplikationer, og efter den

[2] For at forklare forskellen i antal mellem runde 1 og runde 2 var der i runde 2 af den automatiserede indsamling websteder, hvor der blev offentliggjort flere sæt filer på hver af deres websider.

indledende analyse blev det konkluderet, at sådanne applikationer kan være involveret i distributionen af indhold, der krænker ophavsretten, og i videregivelse af personoplysninger.



Trusler mod slutbrugerne

I løbet af to runder med identifikation af websteder og malwareanalyse blev der ikke fundet ransomware binære filer. Generelt kan det meste af den indsamlede malware karakteriseres som trojanske heste, hvilket betyder, at den kan være repræsenteret på websteder som harmløst, almindeligt anvendt eller populær software, mens det i virkeligheden kan stjæle eller videregive personoplysninger. En uerfaren bruger kan have en høj grad af tillid til softwaren og har måske ikke mulighed for at bemærke abnormiteter. Desuden kan statiske analyser og dynamiske observationer af denne softwares adfærd ikke afsløre den komplette funktionalitet uden adgang til en kildekode. Efter den indledende analyse af malware viste EMAS-analysen mere specifikke skadelige aktiviteter. Indvirkningen af, at denne software er installeret på en slutbrugers computer, kan være betydelig og medføre ikke blot økonomiske tab, men også tyveri af personoplysninger og andre risici forbundet med uønsket adgang og kontrol. Disse aktiviteter kan forventes at føre til indsamling og videregivelse af personoplysninger til tredjeparter i krypteret format eller offentligt format. Disse oplysninger kan f.eks. bestå af bankkontooplysninger fra browseren, oplysninger om computerens hardware-/softwarekonfiguration eller praktisk talt alt, hvad der bliver skrevet på tastaturet.

IDENTIFIKATION OG ANALYSE AF MALWARE PÅ UDVALGTE WEBSTEDER, SOM MISTÆNKES FOR AT KRÆNKE OPHAVSRETTIGHEDER

RESUMÉ

September 2018