EUIPO
OFICIUL UNIUNII EUROPENE
PENTRU PROPRIETATE INTELECTUALĂ

# IDENTIFICAREA ȘI ANALIZA PROGRAMELOR MALWARE DE PE SITE-URI SELECTATE, SUSPECTATE DE ÎNCĂLCAREA DREPTURILOR DE AUTOR

## REZUMAT


Septembrie 2018

# Sinteză

Conținutul suspectat de încălcarea drepturilor de autor reprezintă o nerespectare gravă a drepturilor de proprietate intelectuală. Există site-uri care partajează public astfel de conținut, uneori chiar gratuit, fără nicio înregistrare. Odată cu acest conținut, site-urile distribuie, de obicei, diferite tipuri de programe malware și programe potențial nedorite (PUP-uri), care atrag utilizatorii să descarce și să lanseze aceste fișiere. Studiul oferă o prezentare generală a celor mai recente exemple de programe malware și PUP-uri de pe site-uri suspectate de încălcarea drepturilor de autor. Aceste programe utilizează tehnici înșelătoare și inginerie socială — precum instalări de jocuri goale și de software în aparență „util” — pentru a păcăli utilizatorii finali să divulge informații sensibile. În timpul studiului au fost descoperite diferite PUP-uri, precum software „util”, aplicații false de instalare de jocuri și clienți pentru platforme de transmisie video în flux continuu. Acest software nu prezintă în mod obligatoriu un pericol direct pentru software-ul sau hardware-ul utilizatorului. Cu toate acestea, prin trucuri de inginerie socială, un utilizator poate fi convins să divulge informații sensibile cu caracter personal sau datele cardului de plată. În plus, informații despre calculatorul în sine pot fi divulgate altor părți fără consimțământul explicit al utilizatorului.

**Echipa de cercetare**

Din echipa de cercetare au făcut parte Francesca Bosco, responsabil de program la UNICRI, și Andrii Shalaginov, cercetător științific doctorand în domeniul securității informaționale în cadrul Departamentului de Securitate Informațională și Tehnologia Comunicațiilor (Grupul de Criminalistică Digitală), Facultatea de Tehnologia Informației și Inginerie Electrică, Universitatea Norvegiană de Știință și Tehnologie.

**Declinarea responsabilității**

În acest context, ar trebui subliniat faptul că unicul obiectiv al studiului a fost acela de a determina caracteristicile tehnice ale programelor malware și ale PUP-urilor care au fost întâlnite în timpul studiului și care ar putea fi întâlnite de utilizatorii de internet în momentul căutării de conținut suspectat de încălcarea drepturilor de autor. Eșantioanele de programe malware și PUP-uri documentate nu pot fi considerate exhaustive, iar obiectivul studiului (sau rezultatele acestuia) nu a fost de a furniza o evaluare generală a probabilității sau a riscului de infectare a utilizatorilor cu un malware și PUP în momentul căutării de materiale suspectate de încălcarea drepturilor de autor.

# Cuvânt înainte

Activitățile online suspectate de încălcarea drepturilor de autor pot fi finanțate în diverse moduri, inclusiv prin taxe de abonare, donații, plata pentru servicii suplimentare și venituri din publicitatea online.

Cu toate acestea, nu toate mijloacele de finanțare sunt la fel de inofensive ca exemplele oferite. Timp de ani de zile, diseminarea infectării cu programe malware și cu alte tipuri de programe potențial nedorite (PUP-uri) a avut o importanță majoră în ceea ce privește finanțarea activităților suspectate de încălcarea drepturilor de autor pe internet.

Utilizatorii de internet obișnuiți încep să devină conștienți de riscurile de infectare atunci când accesează site-uri sau aplicații mobile suspectate de încălcarea drepturilor de autor.

IP Youth Scoreboard [Tabloul de bord pe probleme de proprietate intelectuală pentru tineret] din 2015 a EUIPO a arătat că 52% dintre tineri consideră că siguranța pe un site este importantă atunci când accesează conținut online. În total, 78% dintre tineri au afirmat că s-ar gândi de două ori dacă ar ști că există un risc de infectare a calculatorului sau a dispozitivului cu viruși ori cu programe malware. În total, 84% au afirmat că s-ar gândi de două ori dacă ar ști că există un risc de furt al datelor cardului de credit.

În cercetarea pentru acest studiu, Oficiul și-a asumat o sarcină foarte dificilă din punct de vedere tehnic, și anume de a detecta și de a documenta exemple de programe malware și de PUP-uri pe care un utilizator de internet le-ar putea întâlni atunci când încearcă să acceseze filme, muzică, jocuri video și emisiuni de televiziune piratate populare.

În acest context, ar trebui subliniat faptul că unicul obiectiv al studiului a fost acela de a determina caracteristicile tehnice ale programelor malware și ale PUP-urilor care au fost întâlnite în timpul studiului și care ar putea fi întâlnite de utilizatorii de internet în momentul căutării de conținut suspectat de încălcarea drepturilor de autor. Eșantioanele de programe malware și PUP-uri documentate nu pot fi considerate exhaustive, iar obiectivul studiului (sau rezultatele acestuia) nu a fost de a furniza o evaluare generală a probabilității sau a riscului de infectare a utilizatorilor cu programe malware și PUP-uri în momentul căutării de materiale suspectate de încălcarea drepturilor de autor.

Studiul s-a desfășurat în mai multe etape, în strânsă colaborare cu Centrul european de combatere a criminalității informatice (EC3) din cadrul Europol.

Rezultatele indică o varietate de amenințări cu programe malware și PUP-uri diferite pe care un utilizator de internet le poate întâlni în momentul căutării de conținut suspectat de încălcarea drepturilor de autor. Cele mai multe programe malware și PUP-uri documentate pot fi descrise ca troieni sau alt software nedorit care poate dobândi acces neautorizat la datele cu caracter personal ale utilizatorilor de internet. Aceste exemple vor fi relevante și de interes nu doar pentru comunitatea titularilor de drepturi de proprietate intelectuală, ci și pentru autoritățile de aplicare a legii și nu în cele din urmă, pentru consumatorii îngrijorați de accesarea datelor lor cu caracter personal fără permisiunea lor.

# Rezumat

Studiul oferă o prezentare generală a celor mai recente exemple de programe malware și programe potențial nedorite (PUP-uri) de pe site-uri suspectate de încălcarea drepturilor de autor. Aceste programe utilizează tehnici înșelătoare și inginerie socială — precum instalări de jocuri goale și software în aparență „util” — pentru a păcăli utilizatorii finali să furnizeze informații sensibile.

Scopul acestui studiu este de a descoperi și de a documenta software-ul dăunător sau alt tip de software nedorit diseminat pe site-urile selectate suspectate de încălcarea drepturilor de autor și de a clasifica eșantioanele găsite în baza diverselor taxonomii ale programelor malware. În acest context, ar trebui subliniat faptul că unicul obiectiv al studiului a fost acela de a determina caracteristicile tehnice ale programelor malware și ale PUP-urilor care au fost întâlnite în timpul studiului și care ar putea fi întâlnite de utilizatorii de internet în momentul căutării de conținut suspectat de încălcarea drepturilor de autor. Probele de programe malware și PUP-uri documentate nu pot fi considerate exhaustive, iar obiectivul cercetării (sau rezultatul acesteia) nu a fost acela de a furniza o evaluare a probabilității sau a riscului general de infectare de către malware și PUP cu care un utilizator s-ar putea confrunta la momentul căutării de materiale suspectate de încălcarea drepturilor de autor. În scopul acestui studiu, emisiunile TV, filmele, muzica și jocurile video sunt considerate conținut protejat de drepturi de autor.

**Rezultatele studiului**

Conținutul suspectat de încălcarea drepturilor de autor reprezintă o violare gravă a drepturilor de proprietate intelectuală. Există site-uri care partajează public astfel de conținut, uneori chiar gratuit, fără nicio înregistrare. Odată cu un astfel de conținut, site-urile distribuie, de obicei, diferite tipuri de programe malware și PUP-uri, care atrag utilizatorii să descarce și să lanseze astfel de fișiere. În timpul identificării site-urilor pe baza clasamentului Alexa Top 500, în plus față de o simulare de căutări ale utilizatorului mediu cu ajutorul unor motoare de căutare bine-cunoscute, precum Google, Yahoo și Bing, s-a descoperit faptul că setul de site-uri s-a schimbat între cele două sesiuni ale studiului. Această schimbare este probabil rezultatul eforturilor motoarelor de căutare de a elimina linkurile către site-uri suspectate de încălcarea drepturilor de autor, în timp ce noi site-uri suspectate continuă să apară. În ceea ce privește identificarea site-urilor, o constatare interesantă este legată de faptul că majoritatea copleșitoare a site-urilor sunt găzduite în Statele Unite ale Americii sau au nume de domeniu legate de găzduirea acestora tot acolo. În schimb, doar câteva sunt localizate pe servere din UE. Mai mult decât atât, .com și .net sunt cele mai frecvente nume de domeniu de nivel superior utilizate pe site-uri suspectate de încălcarea drepturilor de autor. Acest lucru poate fi datorat faptului că, spre deosebire de domeniile specifice țărilor, acestea nu necesită stabilirea identității utilizatorului cu un pașaport sau cu alte documente de identificare. În medie, între cele două sesiuni de identificare au fost adăugate 20% de site-uri noi și eliminate 20% din site-urile vechi. Mai mult decât atât, aproape 8% din site-urile identificate în ambele sesiuni au fost caracterizate de către platforma VirusTotal drept dăunătoare. Cu ajutorul diverselor sisteme de gestionare a conținutului, crearea unui site și livrarea conținutului către utilizatori, inclusiv a aplicațiilor dăunătoare, se pot realiza acum aproape fără niciun efort.

Înainte de colectarea programelor malware, acest studiu a presupus o examinare documentară a amenințărilor cu programe malware în 2017 și o clasificare a stadiului actual al tehnologiei. Acest corpus de date a fost utilizat mai departe în timpul analizei programelor malware pentru a urmări principiile acceptate de comunitate în ceea ce privește identificarea tipurilor și familiilor de programe malware. În total au fost strânse 106 fișiere în timpul ambelor sesiuni de colectare a datelor. Acestea includ fișiere descărcate direct de pe site-uri suspectate de încălcarea drepturilor de autor, precum și fișiere care au fost create în timpul rulării fișierelor descărcate. În timpul studiului au fost descoperite diferite PUP-uri, precum software „util”, false programe de instalare de jocuri și clienți pentru platforme de transmisie video în flux continuu. Un astfel de program nu prezintă în mod obligatoriu un pericol direct pentru software-ul sau hardware-ul utilizatorului. Cu toate acestea, prin trucuri de inginerie socială, un utilizator poate fi convins să divulge informații sensibile cu caracter personal sau datele cardului de plată. În plus, informații despre calculatorul în sine pot fi divulgate altor părți fără consimțământul explicit al utilizatorului.

Programele malware colectate au fost analizate inițial utilizând instrumente cu sursă deschisă pentru a înțelege logica internă, a detecta activități posibil dăunătoare și a evalua relevanța acestora pentru studiul de față. În plus față de analiza preliminară cu ajutorul instrumentelor cu sursă deschisă, eșantioanele de programe malware colectate au fost analizate de platforma Europol pentru soluții de analiză malware (Europol Malware Analysis Solution – EMAS). Drept rezultat s-a detectat un număr mare de artefacte diferite și de activități dăunătoare. Rapoartele EMAS includ o analiză completă a fișierelor, în cadrul căreia s-au utilizat patru versiuni de MS Windows și unde traficul de rețea, apelurile de funcție și activitățile discului sunt amănunțit înregistrate pentru o ulterioară analiză. În plus, platforma evidențiază orice activitate suspicioasă detectată în timpul rutinelor de rulare a fișierelor. În urma analizei tuturor rapoartelor, EMAS a observat 35 de tipuri de activități dăunătoare, care sunt reunite în 17 clase de evenimente dăunătoare. Acestea cuprind de la anomalii generale (precum lansarea proceselor de sistem sau căutarea proceselor în memorii) până la acțiuni evident dăunătoare (precum keylogger, rootkit și manipularea traficului de rețea).

În general, probele binare de programe malware și PUP-uri colectate au scos la iveală câteva modele generale diferite de a acționa: programe „utile” care pretind că vor curăța fișierele vechi de pe calculatorul unui utilizator pe baza unui abonament cu plată; simulatoare de instalare a jocurilor care necesită datele cu caracter personal ale utilizatorului; și programe gratuite care oferă acces la platforme care distribuie conținut piratat, de exemplu prin intermediul tracker-ului BitTorrent. Cele două sesiuni de identificare a site-urilor și de colectare a programelor malware au generat rezultate promițătoare în ceea ce privește înțelegerea metodelor de diseminare a programelor malware și a ingineriei sociale pentru obținerea informațiilor cu caracter personal și a informațiilor identificabile sensibile. Mai mult decât atât, popularitatea sporită a dispozitivelor mobile din ultimii ani este evidentă în lumina detectării numeroaselor PUP-uri pentru Android OS, disponibile prin intermediul platformelor de distribuire a conținutului suspectat de încălcarea drepturilor de autor. Drept rezultat al corelării analizelor, concluzia trasă a fost că peisajul amenințărilor pentru programe malware distribuite prin intermediul site-urilor care încalcă drepturile de autor este mai sofisticat decât ar putea să pară la prima vedere. Printre software-urile descoperite, unele pot fi clasificate suplimentar ca troian, adware, backdoor și agent. Acest lucru este amplificat de faptul că s-au găsit, de asemenea, numeroase familii de programe malware specifice, precum WisdomEyes, DealPly, și FileRepMalware. În plus, o astfel de clasificare completă este valabilă atât pentru platforma Android, cât și pentru Microsoft Windows. Există o gamă largă de amenințări la adresa bunurilor utilizatorilor, inclusiv, dar fără a se limita la, furtul de date de autentificare sensibile, date cu caracter personal, informații despre configurația hardware-ului și modificarea traficului de rețea. Drept urmare, cu toate că software-urile identificate pot fi PUP-uri, acestea pot oricum avea un impact asupra utilizatorilor, în special în cazurile în care sunt implicați utilizatori obișnuiți care s-ar putea să nu fie pe deplin conștienți de practicile și măsurile de bază pentru securitatea online.

Un exemplu de constatare în cadrul studiului este prezentat mai jos.

| Site-ul 03 | Site-ul 09 | Site-ul 08 |
|---|---|---|
| Site-ul păcălește utilizatorii să utilizeze o instalare falsă a unui joc; întregul proces de obținere a informațiilor sensibile ale utilizatorului s-a schimbat între prima și a doua sesiune de colectare a programelor malware. Utilizatorul acestui serviciu descarcă o arhivă care cuprinde conținut deghizat sub forma unor fișiere legate de joc, fără să fie un fișier executabil binar explicit care poate fi detectat de orice anti-virus ca fiind dăunător. Arhiva criptată acordă acces doar la | Site-ul oferă acces la orice tip de conținut video disponibil prin intermediul trackerelor de fișiere de tip „torrent” cu ajutorul unui instrument software. Acest instrument necesită mai puține interacțiuni cu utilizatorul față de alte trackere BitTorrent.<br>Sunt necesare doar câteva clicuri pentru a descărca conținut din surse necunoscute, utilizatorul nefiind protejat și neavând control asupra a ceea ce se descarcă. | (Android) Site-ul oferă acces la o gamă de aplicații mobile gratuite fără înregistrare. O aplicație oferă acces nelimitat la transmisia de emisiuni TV și filme în flux continuu. Nu există nicio solicitare explicită de furnizare a informațiilor sensibile ale unui utilizator sau a datelor de plată pentru cumpărarea accesului la materiale video protejate de drepturi de autor. Cu toate acestea, utilizatorul trebuie să dezactiveze setări de securitate care vor permite instalarea unor |

| | | |
|---|---|---|
| numele de fișiere, nu și la conținutul efectiv al fișierelor. | | aplicații, altele decât cele de pe o piață oficială de aplicații. |

**Metodologie**

Pentru a realiza studiul, a fost necesară adoptarea unei metodologii solide pentru a face față selecției de titluri și site-uri, precum și a sarcinii solicitante din punct de vedere tehnic de detectare și documentare a exemplelor de programe malware și PUP-uri găsite. O scurtă prezentare generală a metodologiei este descrisă mai jos:

1. În Faza I a cercetării UNICRI, în colaborare cu Observatorul European al Încălcării Drepturilor de Proprietate Intelectuală (Observator) a fost constituit un grup de suport format din experți, pentru a oferi sfaturi cu privire la metodologia de cercetare, la selectarea site-urilor utilizate pentru analiză și la evaluarea studiului desfășurat în fiecare fază a implementării proiectului. Grupul de suport format din experți a cuprins reprezentanți ai părților interesate ale Observatorului, organizații titulare de drepturi de autor, academicieni, autorități de aplicare a legii și agenții UE.

2. În paralel a fost selectată echipa de cercetare. În cadrul acestui raport nu a fost posibil din punct de vedere tehnic[1] ca toate statele membre ale UE să fie analizate; drept urmare, în Faza II au fost selectate aleatoriu 10 țări-eșantion din cele 28 de state membre ale UE.

3. În Faza III au fost identificate filme, programe de televiziune, cântece și jocuri video populare. S-a ținut cont atât de popularitatea la nivel mondial, cât și de popularitatea la nivelul uneia sau a mai multor țări din cele 10 țări-eșantion la data de 23 iunie 2017, care a marcat începutul perioadei de colectare a datelor. În fazele ulterioare ale studiului, aceste titluri-eșantion au fost utilizate sistematic în căutări online pentru a găsi site-uri și aplicații mobile care încalcă drepturile de autor. Fiecare titlu a îndeplinit cel puțin două dintre următoarele criterii:

   - popular la momentul colectării datelor în cadrul statelor membre ale UE,
   - popular la momentul colectării datelor la scară globală,
   - popular din punct de vedere istoric la scară globală și
   - clasificat drept film, program de televiziune, cântec sau joc video.

   Au fost selectate cinci titluri de film, cinci titluri de programe de televiziune, cinci titluri de muzică și cinci titluri de joc video, rezultatul fiind un total de 20 de titluri-eșantion. S-a acordat o atenție deosebită surselor utilizate pentru identificarea popularității unui titlu anume, ceea ce a necesitat un proces de selecție sistematic pentru a se asigura că datele vor fi disponibile pentru toate sau majoritatea statelor membre.

4. În Faza IV au fost identificate site-uri suspectate de oferirea accesului ilegal la material protejat de drepturi de autor care era popular la nivel mondial și/sau în cele 10 țări-eșantion la data de 26 iunie 2017 (prima sesiune de colectare a programelor malware). Într-o fază ulterioară a studiului, aceste site-uri au fost analizate cu privire la prezența programelor malware și a programelor potențial nedorite.

   Metodologia pentru identificarea site-urilor suspectate de încălcarea drepturilor de autor a fost dezvoltată cu aportul grupului de suport format din experți identificat în Faza I, precum și pe baza unei revizuiri de către UNICRI a literaturii de specialitate existente. Aceasta a fost concepută în mod specific pentru a genera un eșantion de site-uri care:

   - sunt populare în diferite state membre ale UE, asigurând o acoperire geografică largă;
   - reprezintă diferite tipuri de site-uri suspectate de încălcarea drepturilor de autor, inclusiv site-uri cu redare în flux continuu, site-uri cu linkuri, site-uri de găzduire, servicii de găzduire de tip „cyberlocker” și site-uri cu tehnologie de tip „torrent”;
   - reprezintă o gamă largă de conținut suspectat de încălcarea drepturilor de autor, inclusiv filme, titluri de televiziune, muzică și jocuri video; și

[1] Numărul de țări selectate va avea un impact direct (va crește) asupra numărului de site-uri selectate, suspectate de încălcarea drepturilor de autor, și asupra fișierelor binare corespunzătoare de analizat. Drept urmare, s-a luat decizia de a pune accentul doar pe un eșantion de țări pentru a putea efectua cu succes partea practică a studiului în intervalul de timp dat.

- reprezintă site-uri pe care utilizatorul obișnuit de internet le-ar întâlni atunci când încearcă să acceseze material suspectat de încălcarea drepturilor de autor.

În selectarea site-urilor suspectate de încălcarea drepturilor de autor au fost utilizați cinci pași. Primii trei pași au fost concepuți pentru a identifica cele mai populare site-uri suspectate de încălcarea drepturilor de autor din statele membre ale UE. Această metodă a simulat scenariile în care un utilizator obișnuit ar căuta site-uri suspectate de încălcarea drepturilor de autor fără a specifica, de exemplu, titlul unui film sau al unui cântec. Ultimii doi pași au fost concepuți pentru a identifica site-uri suspectate de încălcarea drepturilor de autor pe care un utilizator obișnuit le-ar întâlni atunci când caută modalități de a descărca un anume titlu popular fără a specifica un site. Acest pas a fost deosebit de important, dată fiind prezența site-urilor suspectate a fi dăunătoare, care presupun denaturarea rezultatelor căutării prin care exploatează subiecte de actualitate prin optimizarea motoarelor de căutare. Împreună, cele două abordări au acoperit diferitele moduri prin care un utilizator obișnuit de internet ar încerca să găsească online material suspectat de încălcarea drepturilor de autor.

S-a pus accent pe analiza concomitentă a programelor malware și a PUP-urilor specifice aplicațiilor mobile de pe dispozitive, precum telefoanele inteligente și tabletele, fiind una dintre noile amenințări majore de criminalitate informatică. Analiza a fost limitată la dispozitive Android, în urma indicațiilor din literatura de specialitate existentă cu privire la o prezență mai mare a programelor malware în magazine de aplicații Android (adică Google Play) decât în magazinul iTunes al Apple. Metodologia a fost concepută pentru a genera un eșantion de aplicații mobile care:

- sunt populare la momentul colectării datelor la o scară globală;
- reprezintă diferite tipuri de aplicații (incluzând aplicații de redare în flux continuu, aplicații de tip „torrent” și aplicații de găzduire);
- conțin sau oferă acces la o gamă largă de conținut suspectat de încălcarea drepturilor de autor (incluzând filme, titluri de televiziune, muzică și jocuri mobile); și
- reprezintă ceea ce un utilizator obișnuit al unui dispozitiv mobil va întâlni atunci când încearcă să descarce sau să utilizeze o aplicație care facilitează accesul la conținut protejat de drepturi de autor suspectat.

5. Faza V a constat în colectarea de programe malware și PUP-uri, în plus față de aplicațiile mobile de pe site-urile identificate, pentru a fi examinate într-o etapă ulterioară în vederea unei clasificări corecte. Faza de obținere a datelor a cuprins două sesiuni de colectare și analiză a programelor malware efectuate în vara anului 2017. Prima sesiune de colectare de programe malware a avut drept rezultat 1 054 de nume de domeniu unice, iar a doua sesiune a avut drept rezultat 1 057 de nume de domeniu unice din 10 state membre ale UE selectate. Programele malware au fost colectate atât manual, cât și automat, pentru a simula experiența unui utilizator obișnuit.

**Colectarea manuală**. Această metodă a presupus examinarea manuală a domeniilor identificate în faza precedentă. Utilizând colectarea manuală, expertul a putut să simuleze experiența unui utilizator de internet obișnuit făcând clic pe reclame și interacționând cu site-uri care necesită prompt-uri.

**Colectarea automată**. Această metodă a utilizat un web-crawler automat conceput de un expert pentru a urmări toate linkurile disponibile pe un site ales suspectat de încălcarea drepturilor de autor. În primul rând, pe orice site, crawler-ul urma întâi să colecteze informații din linkurile de pe pagina principală. În al doilea rând, crawler-ul urmărea fiecare din acele linkuri către site-uri secundare. În al treilea rând, crawler-ul urmărea fiecare din acele linkuri către site-uri de nivel trei. La fiecare pas, crawler-ul a recuperat fișiere binare care ar putea prezenta interes pentru o analiză manuală ulterioară, inclusiv programe malware potențiale sau suspectate și programe potențial nedorite. Acest proces a continuat pentru până la 1 000 de linkuri pentru fiecare site.

6. Odată ce fișierele binare au fost colectate, acestea au fost analizate într-un mediu informatic sigur în vederea înțelegerii funcționalității interne a acestora și a clasificării corecte. S-a efectuat o

analiză preliminară, utilizând instrumente cu sursă deschisă pentru a putea corela constatările cu rapoartele de amenințări informatice. Probele de software colectate au fost apoi livrate către EMAS pentru a fi analizate; analiza EMAS a fost apoi comparată cu rezultatele preliminare.

**Prezentare generală a metodologiei**


**Eșantioane de programe malware și PUP detectate**

La data de 28 iulie 2017, 5 240 de site-uri (1 054 unice) au fost verificate automat în timpul primei sesiuni de colectare, fiind găsite 617 fișiere relevante (muzică, video, fișiere de tip „torrent” și software) cu o dimensiune totală de 47 GB. Acest lot de fișiere nesortate a necesitat analiză suplimentară pentru a decide care dintre fișierele colectate erau relevante pentru studiu. Eșantioanele de site-uri care încalcă drepturile de autor au fost similare în toate cele 10 țări-eșantion pentru fiecare dintre aceste tipuri de media (programe de televiziune, filme, muzică și jocuri video). Drept rezultat, Belgia a fost selectată aleatoriu din rândul țărilor-eșantion și toate site-urile identificate încălcând drepturile de autor pentru Belgia au fost examinate manual pentru a verifica prezența software-urilor dăunătoare sau nedorite. La data de 10 august 2017, după a doua sesiune de colectare, a fost recuperat în mod automat un număr total de 3 665 de fișiere de pe site-uri din toate țările, cu o dimensiune totală de 167 GB. Numărul total de URL-uri unice extrase pentru toate țările a fost de 1 057 din cele 5 606 site-uri, ceea ce a făcut ca verificarea manuală a tuturor să fie imposibilă.

După o analiză preliminară a fișierelor colectate, 106 fișiere binare unice pentru MS Windows, Android și MAC OS au fost extrase ca rezultat al ambelor sesiuni de colectare de programe malware. Mai exact, 41 de fișiere au fost selectate în timpul primei sesiuni și 65 au fost selectate în timpul celei de-a doua sesiuni — în special: 2 pentru Mac, 15 pentru Android și 89 pentru MS Windows. Dintre aceste fișiere, 21 pot fi considerate programe dăunătoare binecunoscute, așa cum au fost etichetate de numeroși distribuitori de programe anti-virus, conform clasificării făcute de către platforma VirusTotal. Acestea includ fișiere descărcate direct de pe site-uri selectate, suspectate de încălcarea drepturilor de autor, precum și fișiere care au fost create în timpul rulării fișierelor descărcate. Ulterior, eșantioanele de software colectate au fost analizate într-un mediu de tip „sandbox” și transmise către EMAS pentru o

analiză mai profundă a posibilelor activități dăunătoare. Pentru toate fișierele binare au fost descoperite în total 821 de evenimente distincte dăunătoare în cadrul a patru rapoarte EMAS (Windows 7 SP1, Windows7 SP1 64-bit, Windows 10 64-bit, Windows XP SP3). Unele rapoarte nu au prezentat activități suspicioase, iar unele au prezentat până la 10 activități dăunătoare cunoscute anterior. În timpul etapei finale a studiului, rezultatele analizei preliminare și cele din rapoartele EMAS au fost corelate. Rezumatul cantitativ al rezultatelor este oferit în tabelul de mai jos.

| | **Sesiunea 1** | **Sesiunea 2** |
|---|---|---|
| **Data** | 28 iulie 2017 | 10 august 2017 |
| **Site-uri descoperite în 10 țări din UE** | 5 240 | 5 606 |
| **Site-uri unice** | 1 054 | 1 057 |
| **Fișiere relevante** | 617 | 3 665[2] |
| **Dimensiunea fișierelor relevante, GB** | 47 | 167 |
| **Livrate către EMAS** | | |
| **Android** | 3 | 12 |
| **Mac OS** | 2 | – |
| **MS Windows** | 36 | 53 |
| **Dimensiune totală, biți** | 175 600 117 | 522 991 095 |

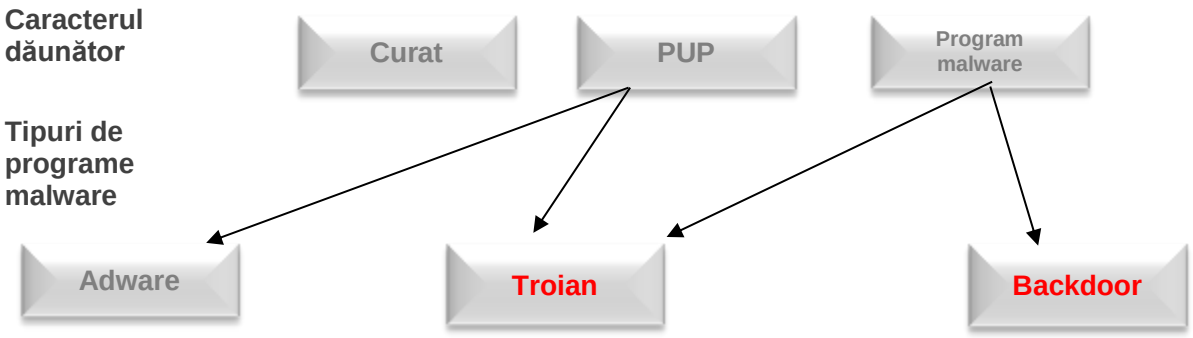
**Europol Malware Analysis Solution (EMAS)**

Europol Malware Analysis Solution (EMAS) este o soluție de analiză dynamică automată a programelor malware, furnizată de Europol statelor membre ale UE. EMAS oferă posibilitatea creării de rapoarte de analiză, însă caracteristica sa cea mai revoluționară este de a genera date active pentru anchetatorii din cadrul poliției. Verificările încrucișate automate pot indica legături între atacuri desfășurate în țări diferite cu același program malware sau cu aceeași organizație criminală, care se află în spatele aceleiași familii de programe malware, ducând la aceleași domenii și legate de anchete diferite în interiorul sau în afara UE. În 2015, EMAS a devenit complet automatizată, pentru a permite accesul direct al autorităților de aplicare a legii cu care Europol are acorduri operaționale. În 2015: au fost analizate 525 108 fișiere în EMAS, dintre care 356 863 au fost identificate drept dăunătoare.

După cum reiese din figura de mai jos, în general, fișierele binare colectate pot fi clasificate în funcție de caracterul lor dăunător drept inofensive (fișiere care nu dăunează), PUP-uri și programe malware dăunătoare. Mai mult decât atât, au fost descoperite PUP-uri nu doar pentru Microsoft Windows, ci și pentru Android și Mac OS, ceea ce sugerează faptul că dezvoltatorii de programe malware încearcă să afecteze cât mai mulți utilizatori posibil folosind diferite platforme. PUP-urile și programele malware pot fi mai departe diferențiate în baza categoriilor principale de programe malware, și anume troian, adware și backdoor. Cele mai multe software-uri găsite fac parte din categoria PUP. Funcționarea PUP-urilor poate fi asociată cu unul dintre următoarele modele de acționare: instalări false de jocuri care necesită date cu caracter personal și despre contul bancar, descărcare de programe „utile” care obligă utilizatorii să cumpere un abonament la o versiune plătită sau instalare de programe gratuite pentru a accesa platforme care încalcă drepturile de autor. Aceste aplicații pot compromite datele cu caracter personal ale utilizatorilor și configurația calculatorului. Prin trucuri de inginerie socială, diverse tipuri de date personale, precum datele cardului de plată, informațiile identificabile personal și datele de autentificare pe rețelele de socializare pot fi, de asemenea, divulgate. De asemenea, studiul a identificat 15 aplicații Android de pe piața aplicațiilor de la terți, iar după o analiză preliminară, s-a ajuns la concluzia că astfel

[2] Pentru a explica diferența în rezultatele numerice dintre Sesiunea 1 și Sesiunea 2: în timpul Sesiunii 2 de colectare automată au existat site-uri care au publicat seturi multiple de fișiere pe fiecare dintre paginile web ale acestora.

de aplicații pot fi implicate în distribuirea de conținut care încalcă drepturile de autor și în divulgarea datelor cu caracter personal.




**Amenințări la adresa utilizatorilor finali**

În timpul a două sesiuni de identificare a site-urilor și de analiză a programelor malware, nu au fost găsite programe binare de tip ransomware. În general, cele mai multe programe malware colectate pot fi caracterizate drept troieni, ceea ce înseamnă că pot fi reprezentate pe site-uri ca software inofensiv des utilizat sau popular în timp ce, în realitate, acestea pot fura sau divulga informații private. S-ar putea ca un utilizator fără experiență să aibă un grad ridicat de încredere în software și să nu poată observa nicio anomalie. În plus, s-ar putea ca analiza statică și observațiile dinamice de comportament ale unui astfel de software să nu scoată la iveală funcționalitatea completă fără a avea un cod sursă. În urma analizei preliminare a programelor malware, analiza EMAS a indicat mai multe activități specifice dăunătoare. Prezența unui astfel de software instalat pe calculatorul unui utilizator final poate avea un impact considerabil, provocând nu doar pierderi financiare, ci și furtul datelor cu caracter personal și alte riscuri legate de accesul și controlul nedorit. Se poate ca aceste activități să aibă drept rezultat colectarea și transmiterea de informații cu caracter personal către terțe părți, în format de text criptat sau deschis. De exemplu, astfel de date pot fi datele de autentificare ale contului bancar din browser, detalii ale configurației hardware/software ale calculatorului sau pur și simplu orice se tastează la calculator.


# IDENTIFICAREA ȘI ANALIZA PROGRAMELOR MALWARE DE PE SITE-URI SELECTATE, SUSPECTATE DE ÎNCĂLCAREA DREPTURILOR DE AUTOR

REZUMAT

Septembrie 2018