Lucrare de diplomă – Raport nr. 1

Analiza comportamentală a fișierelor potențial malițioase în cadrul unui mediu izolat utilizând o arhitectură modulară

Student: **Ștefan Paraschiv**
Coordonator științific: **Ș.l.dr.ing. Cătălin Mironeanu**

Scopul temei alese

În prezent, prevenirea infectării unui sistem IT este o problemă critică iar mulți utilizatori se bazează pe un antivirus pentru a se proteja împotriva *malware*-urilor – software rău intenționat, se referă la orice software dezvoltat de către infractori cibernetici pentru a fura date și pentru a afecta sau distruge calculatoare și sisteme informatice [1]. Cu toate acestea, antivirusul are dezavantajul de a nu detecta atacurile noi cu precizie. În contrast, *sandboxing*-ul oferă o soluție prin care se pot detecta și analiza amenințările necunoscute prin izolarea lor într-un mediu controlat și sigur [2].

Lucrarea propune crearea un mediu sigur pentru compararea rezultatelor obținute prin intermediul unui *sandbox* specializat pe securitate cu alte rezultate obținute prin algoritmi diferiți sau prin alte instrumente. Toate acestea vor fi centralizate într-o bază de cunoștințe specializată pentru stocarea informațiilor legate de securitatea cibernetică. Scopul acestei lucrări este explorarea domeniului, identificarea potențialelor amenințări și reducerea riscurilor de securitate în industria IT.

Unul dintre avantajele utilizării unui *sandbox* constă în posibilitatea de a adăuga module specializate care să ajute la analiza datelor, un exemplu ar fi integrarea unui antivirus cu un *sandbox* pentru detectarea avansată a amenințărilor.

Pentru implementare, lucrarea propune utilizarea unui *sandbox* cu următoarele module: MISP[1], Gmail, PeePDF și un modul propriu pentru a analiza comportamentul unui fișier și a determina dacă acesta prezintă un comportament suspect sau nu.

Referințe la temă/subiecte similare

Cuckoo

Cuckoo este unul din puținele *sandbox*-uri *open-source* care poate analiza automat orice fișier potențial *malware* sub diferite sisteme de operare, inclusiv Windows, macOS, Linux și Android. Prin simpla trimitere a unui fișier suspect către Cuckoo, software-ul va executa fișierul într-un mediu controlat și izolat și va oferi un raport detaliat asupra comportamentului fișierului [3].

Cuckoo ajută la prevenirea amenințărilor prin automatizarea procesului de analiză, având ca rezultat al acesteia informații cu privire la comportamentul fișierelor potențial *malware*.

Unul dintre avantajele oferite de Cuckoo este faptul că vine cu o interfață web intuitivă, care prezintă în mod clar și accesibil rezultatele obținute în urma analizei fișierelor suspecte. Prin intermediul acestei interfețe, utilizatorii pot accesa toate analizele procesate de Cuckoo, care sunt:

- Rezumatul analizei - care oferă informații generale despre fișierul analizat și rezultatele obținute în urma executării sale în mediu izolat.
- Analiza dinamică - care prezintă informații detaliate despre comportamentul fișierului în timpul execuției în mediul izolat, inclusiv apeluri de sistem, procese, comunicare de rețea și alte activități suspecte.

[1] Malware Information Sharing Platform

- Analiza statică - care examinează fișierul din punct de vedere al semnăturilor și a altor atribute statice pentru a detecta semne de *malware*.
- Capturi de ecran - care prezintă capturi de ecran realizate în timpul execuției fișierului suspect în mediul izolat, pentru a oferi o imagine mai clară a modului în care acesta acționează.
- Raportul de rețea - care oferă informații detaliate despre activitatea de rețea a fișierului suspect, inclusiv adrese IP, porturi, protocoale și alte informații relevante.
- Module opționale suportate de Cuckoo - acestea sunt module pentru care Cuckoo a facilitat integrarea, un exemplu ar fi MISP.

Toate aceste analize pot fi accesate și vizualizate într-un mod intuitiv prin intermediul interfeței Cuckoo , oferind astfel utilizatorilor posibilitatea de a evalua rapid și eficient potențialele amenințări și de a lua măsuri de protecție adecvate.

Cuckoo poate fi accesat printr-un API[2] care poate fi extins, permițând utilizatorilor să integreze *sandbox*-ul în fluxul lor de lucru existent și să extindă funcționalitatea acestuia prin dezvoltarea de module suplimentare.

Pentru o analiză mai amănunțită Cuckoo oferă un raport detaliat în format JSON. Acest raport poate fi folosit pentru a identifica și analiza comportamentul specific al *malware*-ului și poate fi folosit pentru a dezvolta semnături și alte metode de detectare și prevenire a atacurilor similare.

ANY.RUN

ANY.RUN este o platformă care folosește tehnologii *cloud*, permițând utilizatorilor să încarce și să analizeze fișiere și URL-uri suspecte. Furnizează o interfață prietenoasă cu utilizatorul și o gamă largă de instrumente de analiză, inclusiv analiză dinamică, analiză statică și analiză comportamentală [4].

ANY.RUN oferă suport *live* prin intermediul *chat*-ului online, care poate fi accesat prin pagina de contact a site-ului. Utilizatorii pot accesa chat-ul online pentru a obține asistență tehnică sau pentru a solicita ajutor cu problemele legate de utilizarea platformei ANY.RUN.

Un dezavantaj al *sandbox*-ului ANY.RUN este faptul că este suportat doar pe sistemele de operare Windows și că deși există o versiune gratuită, nu toate funcțiile și capacitățile sunt disponibile în această versiune. Pentru utilizatorii care folosesc alte sisteme de operare, cum ar fi macOS sau Linux, acest aspect poate fi un dezavantaj major deoarece nu pot utiliza ANY.RUN pentru analiza fișierelor și a URL-urilor suspecte.

Alegerea dintre ANY.RUN și Cuckoo depinde de nevoile specifice ale utilizatorului. Dacă utilizatorul preferă o soluție bazată pe cloud și suport live ANY.RUN poate fi cea mai bună opțiune. Cu toate acestea, dacă utilizatorul are nevoie de o platformă *sandbox* personalizabilă și extensibilă care poate fi integrată cu diverse instrumente și servicii, Cuckoo este alegerea mai bună.

FortiSandbox

FortiSandbox este o soluție de securitate avansată a companiei Fortinet bazată pe *sandbox*-ing care ajută organizațiile să detecteze și să prevină atacurile cibernetice prin analiza automată a fișierelor *malware* și a amenințărilor necunoscute. Acesta oferă capacități de analiză dinamică și de emulare a sistemului de operare, folosind tehnici de invățare automată prin care sunt identificate și izolate *malware*-uri [5] care pot să pătrundă într-un sistem de securitate.

FortiSandbox poate fi integrat cu soluțiile de securitate existente ale organizației și poate analiza diverse tipuri de amenințări, inclusiv fișiere executabile, fișiere descărcate și atașamente

[2] https://cuckoo.readthedocs.io/en/latest/usage/api/

de e-mail. Soluția utilizează analiză în timp real pentru a identifica și a bloca amenințările noi și necunoscute.

De asemenea, FortiSandbox oferă capacități de analiză a rețelei, permițând identificarea amenințărilor care folosesc tehnici de atac sofisticate pentru a pătrunde într-un sistem. Soluția poate să identifice atacurile de tipul *zero-day* (un atac care profita de o vulnerabilitate necunoscuta a sistemului) și poate să ofere informații detaliate despre sursă.

Una dintre principalele diferențe între cele două soluții este faptul că FortiSandbox este o soluție comercială, în timp ce Cuckoo este o soluție *open-source* gratuită. FortiSandbox este oferit ca un produs hardware sau software, în timp ce Cuckoo necesită ca utilizatorii să configureze și să ruleze *sandbox*-ul pe propriile lor sisteme.

O altă diferență importantă între cele două soluții este nivelul de personalizare și flexibilitate. Cuckoo este o soluție extrem de flexibilă și personalizabilă, permițând utilizatorilor să configureze *sandbox*-ul în funcție de nevoile lor specifice. În schimb, FortiSandbox oferă mai puține opțiuni de personalizare, dar este mai ușor de configurat și de implementat.

De asemenea o altă deosebire este ca FortiSandbox nu dispune de un API deschis și extensibil, ceea ce limitează posibilitățile de integrare cu alte instrumente și servicii. Cu toate acestea, Fortinet oferă un set de interfețe de programare a aplicațiilor (API) pentru a permite integrarea cu produsele proprii Fortinet.

Combined dynamic multi-feature and rule-based behavior for accurate malware detection

Articolul [6] abordează o problemă veche însă importantă din securitate, anume detectarea de *malware*-uri. În general *malware*-ul poate fi detectat prin doua metode principale, prin semnături sau/și prin comportament. Detectarea bazată pe semnătură utilizează semnături de *malware* existente pentru a detecta atacurile cunoscute, iar detectarea bazată pe comportament se concentrează pe analiza comportamentului *malware*-ului.

Articolul propune o abordare nouă pentru detecția bazată pe comportament. Mai exact, abordarea propusă în articol utilizează analiza dinamică pentru a identifica comportamentele suspecte ale *malware*-ului, iar apoi utilizează analiza de comportament bazată pe reguli pentru a confirma dacă comportamentul este malițios sau nu.

Autorii afirmă că există mai multe modalități de a detecta un comportament suspect al *malware*-ului, însă consideră că cele mai importante informații referitoare la modul în care *malware*-ul se desfășoară pot fi extrase din următoarele trei elemente:

- API calls (Apeluri de API) sunt reprezentate de apeluri făcute de sistemul de operare către alte aplicații/programe, și sunt esențiale pentru interacțiunea dintre acestea. Un exemplu concret de astfel de apeluri este funcția "NtOpenFile", care este folosită pentru a deschide fișiere sau directoare în sistemul de operare Windows.

- API sequence (Secvențe API) sunt alcătuite din apelurile de sistem făcute de un proces și reprezintă un șir de instrucțiuni care descriu interacțiunea dintre un program și sistemul de operare. Aceste secvențe sunt importante pentru analiza comportamentului unui proces sau program și pot fi folosite pentru a detecta activități suspecte sau potențial dăunătoare.

- Trafic de internet care reprezintă fluxul de date care circulă între un dispozitiv și serverele conectate la internet, acesta poate fi analizat pentru a observa cererile făcute de către *malware*. Prin monitorizarea traficului de internet, se pot detecta activități suspecte sau potențial dăunătoare ale programelor *malware*, cum ar fi descărcarea altor fișiere *malware* sau comunicarea cu servere de tip C&C (Command and Control).

Astfel, prin elementele enumerate mai sus, se poate determina comportamentul unui fișier executat și pentru extragerea acestor informații autorii propun utilizarea *sandbox*-ului Cuckoo.

Din rezultatele preluate din raportul generat de *sandbox*, se aplica doi algoritimi pentru extragerea de API-uri care ar putea să determine comportamentul fișierului. În urma aplicării lor, se pot genera reguli care determina dacă intențiile fișierului sunt dăunătoare sau nu, acestea vor fi stocate într-o baza de date care conține reguli YARA[3] – o soluție software specializată în detectarea și identificarea amenințărilor *malware*.

Aceasta reprezintă etapa de antrenare pentru a popula baza de date cu reguli. În etapa de testare sunt extrase doar informațiile necesare din raportul generat de *sandbox*, iar apoi aceste date sunt comparate cu reguli YARA, urmând pe baza unui sistem de votare să se decidă dacă fișierul analizat are sau nu intenții dăunătoare. Acest proces de votare ia în considerare toate regulile aplicabile și decide în funcție de numărul de voturi pozitive sau negative pentru fiecare regulă. În acest fel, se poate identifica cu precizie de 97.22% (conform autorilor [6] în situația cea mai favorabilă) dacă fișierul este un program *malware* sau nu.

Pentru a evalua eficacitatea abordării propuse, autorii au efectuat experimente pe un set de date care conținea diverse tipuri de *malware*. În situația în care nu sunt disponibile toate atributele necesare analizei (menționare în enumerarea anterioară), precizia scade până la 66.11%. Rezultatele experimentelor au arătat că abordarea propusă a avut o performanță mai bună decât alte abordări existente.

Resurse hardware/software utilizate

Resurse hardware

Resursele hardware necesare pentru acest proiect nu sunt foarte restrictive, însă pentru o rulare decentă ar trebui să existe minim 16 GB RAM și un procesor cu minim 6 nuclee.

Resurse software

Pentru a implementa aplicația, este necesar să se creeze un mediu virtual Linux separat în care să se instaleze *sandbox*-ul. În acest mediu, modulele suplimentare sunt dezvoltate în Python pentru a facilita prelucrarea datelor și comunicarea între module. De asemenea, proiectul[4] Cuckoo este scris în Python, iar adăugarea de noi funcționalități este mai ușoară dacă se utilizează același limbaj. Am decis să folosesc PyCharm ca mediu de dezvoltare, deoarece acesta oferă un set de funcționalități și instrumente care facilitează procesul de dezvoltare în Python.

Algoritmi sau metode alese

Modulul suplimentar pentru clasificarea unui fișier în categoria de software rău intenționat sau nu, necesită prelucrarea unor date. Pentru a determina din ce clasă fac parte datele, propunem utilizarea algoritmilor:

- LCS (Longest Common Subsequence) - este un algoritm de calculare a celei mai lungi secvențe comune dintre două șiruri de caractere. Această secvență comună nu trebuie să fie continuă, ci poate fi o secvență de caractere care apare în ambele șiruri, în orice ordine, dar fără a fi nevoie să apară consecutiv în ambele șiruri . Acest algoritm va fi utilizat pentru determinarea celor mai importante apeluri de sistem făcute de către mai multe procese.

- TF-IDF (Term Frequency-Inverse Document Frequency) - este un algoritm de prelucrare a textului care se bazează pe frecvența termenilor într-un set de date pentru a evalua importanța unui cuvânt dintr-un document, în aceasta lucrare datele sunt reprezentate de API calls. Algoritmul constă în două părți principale: TF (Term Frequency) și IDF (Inverse Document Frequency). TF reprezintă frecvența termenului într-un document, iar IDF reprezintă inversa

[3] **Y**et **A**nother **R**ecursive/Ridiculous **A**cronym
[4] https://github.com/cuckoosandbox/cuckoo

frecvenței acestui termen în setul de documente. Valorile TF și IDF sunt înmulțite pentru a obține un scor TF-IDF pentru acel termen în documentul respectiv. Cu cât un termen apare mai des într-un document, dar mai rar în setul de documente, cu atât va avea un scor mai mare TF-IDF și astfel va fi considerat mai important în acel document.

Ambii algoritmi sunt folosiți pentru a crea reguli care vor ajuta la clasificarea intenției unui fișier analizat.

Rezultate așteptate

Proiectul de diplomă reprezintă un efort de cercetare și dezvoltare pentru a oferi o protecție suplimentară față de un antivirus. Scopul proiectului este de a furniza o modalitate mai precisă și mai eficientă de a detecta și a clasifica fișiere dăunătoare prin utilizarea unui set de tehnologii și algoritmi de inteligență artificială.

După rularea proiectului, rezultatul ar trebui să specifice dacă un fișier este dăunător sau nu, oferind o clasificare corectă și o protecție mai bună împotriva amenințărilor cibernetice.

Bibliografie

[1] Cisco, "What is malware?" https://www.cisco.com/site/us/en/products/security/what-is-malware.html, 2023, Ultima accesare: 11.03.2023.

[2] T. H. News, "How to build a custom malware analysis sandbox," https://thehackernews.com/2022/03/how-to-build-custom-malware-analysis.html, 2022, Ultima accesare: 11.03.2023.

[3] Cuckoo Foundation, "Cuckoo sandbox," https://cuckoosandbox.org/, Accesat 11.03.2023.

[4] Any.run, "Malware research with any.run," https://any.run/why-us/, 2023, Ultima accesare: 11.03.2023.

[5] Fortinet, "FortiSandbox," https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiSandbox.pdf, 2023, Ultima accesare: 11.03.2023.

[6] T. Alrawashdeh, R. Alshammari, and A. Almomani, "Combined dynamic multi-feature and rule-based behavior for accurate malware detection," *Journal of Cybersecurity Education, Research and Practice*, vol. 2020, no. 1, pp. 16–28, 2020. [Online]. Available: https://doi.org/10.1177/1550147719889907