

# Detekcia malvéru pomocou hlbokého učenia založeného na vízii \*

Jakub Martinak

Slovenská technická univerzita v Bratislave

Fakulta informatiky a informačných technológií

xmartinak@stuba.sk

11. oktober 2021

## Abstrakt

Kedže v 21. storočí je čím ďalej tím viac potreba chrániť naše elektronické zariadenia pred nebezpečným malvériom tak sa chcem zamerat na túto tému v oblasti informačnej bezpečnosti a implementovanie strojového učenia do nej. V tomto článku na začiatku objasní modelovanie v softvérovom inžinierstve a ako to súvisí s mojou témiou a neskôr sa budem zameriavať na presnosť určenia či sa jedná o malware alebo nie pomocou Deep Learning Vision a taktiež budem rozoberať problémy a výhody spojené s touto formou detektie, výhody a nevýhody klasickej detektie malvéru a jeho limity oproti strojovému učeniu.

## 1 Úvod

Túto tému som si vybral z dôvodu nárastu kybernetických útokov vo svete a následnej obrane voči nim pomocou moderných technológií a využitím umelej inteligencie. V prvej časti článku sa budem venovať modelovanie v softwarovom inžinierstve 2. Druhá časť sa bude zaoberať nedávnemu pokroku v kybernetickej bezpečnosti 3, z ktorej následne prejdem na hlavnú tému tohto článku Detekcia malwaru pomocou hlbokého učenia založeného na vízii 4. Záverečné poznámky prináša časť 5.

## 2 Modelovanie v Softvérovom inžinierstve

Softvérové modelovanie je oveľa viac ako len algoritmus v programe alebo samotná funkcia, malo by poukazovať na celý softvérový desing, vrátane rozhrania, interakcií s iným softvérom a všetky softvérové funkcie. Pre objektovo-orientované programy, je používaný objektovo modelovací jazyk ako UML, ktorý je použitý na vytvorenie softvérového dizajnu. Takmer vo všetkých prípadoch je použitý určitý druh modelovacieho jazyka na vytvorenie dizajnu. Tento prístup umožňuje dizajnérový programu vyskúšať rôzne dizajny a vyvodiť, ktorý bude

\*Semestrálny projekt v predmete Metódy inžinierskej práce, ak. rok 2021/22, vedenie: Fedor Lehocki

najlepší ako finálne riešenie.

Je to podobný proces ako pri navrhovaní štruktúry a dizajnu domu, začne sa náčrtom skice poschodí a rozložením izieb. Kreslenie je v tomto prípade modelovací jazyk a výsledkom toho je návrh, ktorý môže byť použitý ako finálny dizajn. Následne sa bude pokračovať upravovaním náčrtu až návrh nebude obsahovať všetky naše potreby, jedine vtedy by sme mali začať s využívaním materiálu, v našom prípade písaním kódu. Výhodou dizajnovania programu použitím modelovacieho jazyka je nájdenie problémov v skorom štádiu a jeho vyriešením bez nutnosti menenia kódu.

### 3 Nedávne pokroky v Kybernetickej Bezpečnosti

#### 3.1 Pokročilá detekcia Malvéru

Napriek pokrokom v metodológii programovania, tak táto metodológia má stále veľký vplyv na bezpečnosť softvéru. Komunita zaoberajúca sa kybernetickou bezpečnosťou, sa hlavne sústredí na detekciu samotného malvéru. Práve vtedy keď všetkých záujem je v zamedzení zneužitia chýb, tak existuje zhoda, že pri extémne komplexnom a časovo náročnom kóde to je priam nemožné zabrániť takýmto chybám.

Kým klasické metódy detektie malvéru spočívajú v zhode aplikačného kódu bez zmien, tak moderné metódy sú založené na kontrole správania, aby sa zisťilo či ide o neprijateľnú aktivitu alebo nie. Kontrola správania je možná, vďaka dynamickému zabezpečeniu virtuálnych mašín, kde je následne možné bezpečne spustiť nebezpečný súbor. Bez takýchto virtuálne uzavretých prostredí by takáto analýza bola príliš nebezpečná pre produkčné systémy.

Moderný výskum v detekcii malvéru zahŕňa strojové učenie, ktoré je ná pomocné v identifikovaní škodlivého kódu na báze vzoriek. Tak isto ako sú AI-Systémy neustále hústené obrázkami rôznych zvierat aby sa ich naučili rozoznávať, tak to isté sa deje aj v kybernetickej bezpečnosti len namiesto fotiek zvierat je vkladaných veľké množstvo obrázkov" súborov, ktoré sú infikované malvérom. Techniky hlbokého učenia využívajú paralelizmus na vylepšenie efektivity algoritmov.

#### 3.2 Dospelosť softvérového procesu

Mnohí odborníci v softvérovej bezpečnosti sa zhodli, aby sa namiesto priamej kontroly softvéru na prítomnosť škodlibého softvéru sústredili na samotný proces tvorby tohto softvéru a podla toho skúmali zraniteľnosti. Táto teória je do značnej miery založená na skúsenostach, z toho dôvodu, že dobrý kód pochádza od dobre vyškolených vývojárov pracujúcimi s najmodernejšími technológiami v dobre organizovaných vývojových prostrediach.

Presne naopak zlý kód pochádza z rúk slabo vyškolených vývojárov, ktorí pracujú v málo organizovaných vývojových prostrediach a s nepochopiteľnými technológiemi, ktoré už nie sú podporované a pravidelne aktualizované. Z tohto výplývajú určité modely vyspelosti, ktoré nám vedia prepojiť stupeň bezpečnosti

s kvalitou procesu.

To má za následok pozitívny vedľajší účinok v podobe zvýšenej bezpečnosti pre celý kód, ktorý sa objaví v procese. Bežné metódy požadované v takýchto procesoch zahŕňajú automatizáciu, pravidelné penetračné testovanie a správne postupy aktualizácie a údržby softvéru.

### 3.3 Kontrola a skenovanie softvéru

Medzi najtradičnejšie prostriedky na zlepšenie softvérovej bezpečnosti patrí priama kontrola kódu, niekedy aj pomocou nástrojov na skenovanie kódu. Po- kračujúce používanie manuálnej kontroly kódu je v softvérovej komunitе diskutované, mnoho ľudí, hlavne tradicionalisti trvajú na tom, že ľudská kontrola je nevyhnutná na vyprodukovanie najkvalitnejšieho a najbezpečnejšieho produktu. Pri rýchlych cykloch ako sú v prostredí DevOps nie je dostatok času na ľudskú kontrolu zdrojového kódu. Takže jediná možnosť bolo zautomatizovať skenovanie kódu, čo sa už stalo normou v týchto prostrediach, má to svoje pro a proti.

Vzhľadom na to, že to kontroluje počítač tak tam vzniká riziko nezachytenia chyby, ktorá by bola ľahko odhaliteľná človekom, ale v prípade komponentov, ktoré už raz boli úspešne skontrolované a zoskenované, tak to urýchľuje skenovanie, pretože tieto komponenty nie je potreba skenovať znova.

## 4 Detekcia malvéru pomocou hlbokého učenia založeného na vízii

### 4.1 Úvod

Detekcia a klasifikácia malvéru je jedným z najväčších problémov v kybernetickej bezpečnosti. Metódy založené na báze podpisov, sú efektívne iba proti už známym malvérom, ale sú veľmi neefektívne proti neznámym malvérom. Autori malvérov používajú techniky ako šifrovanie, packovanie, atď. na už známom malvéry aby predišli detekcií, čo má za následok vačšie množstvo nového malvéru. Súbory s rovnakým malvérovým správaním zapadajú do rovnakej rodiny malvéru. Tieto súbory sú neustále upravované používaním rozličných taktík, čo ich robí veľmi rozličnými.

Tieto množstvá súborov sú neskôr zaradené do ich reprezentatívnej rodiny pomocou efektívneho klasifikovania a procesu detekcie malvéru. Veľa existujúcich klasifikátorov malvéru extrahuje zásadné vlastnosti zo súborov malvéru a trénuje strojový model s týmito vlastnosťami. Trénovaný model vie potom rozoznať rozdiel medzi malvérom a cleanvériom. Klasifikátory čelia mnoho výzvam, pretože taktiky ako šifrovanie, packing a iné jemné úpravy malvéru, môžu spôsobiť únik pred klasifikátorom, čiže takýto malvér nemusí byť zachytený. Vlastnosti, ktoré sú extrahované z týchto upravených malvérov, nevykazujú žiadne dôkazy pre klasifikátor a teda toto spôsobí nezachytenie malvéru.

Potreba príblížiť detekciu malvéru do bodu kde budu extrahované robustné časti

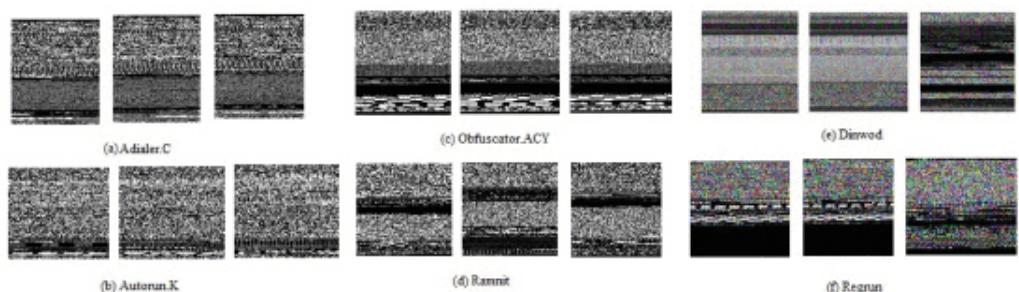
akéhokoľvek upraveného skriptu malvéru. Ďaľšie varianty existujúceho malvéru by mali byť už zachytené týmto systémom.

Sú tu analyzované spustiteľné binárne súbory s malvériom a cleanvériom použitím techniky založenej na analýze videnia. Autori malvéru znova používajú rovnaké segmenty kódu na vygenerovanie nových variant malvéru. Vizualizácia malvéru bola nedávno použitá ako alternatíva a efektívny prístup k malvérovej analýze. Podobnosti variánt nebezpečného kódu sú vizualizované a identifikované. Každá skupina malvéru vystavila určitý vzorec v malvérových obrázkoch.

Tieto vzory v obrázkoch sú veľmi podstatné vo vizuálnych podobách malvéru, ktorý zapadá do jednotlivých skupín. Ďaľšia výhoda Analýzy založenej na vízii je, že nie je potreba dynamickej exekúcie binárnych súborov. Vzory vybraté z obrázkov jednotlivých malvérov sú potom následne použité pri trénovaní klasifikátora. Tieto vlastnosti môžu fungovať ako prezádzajúci faktor na detekovanie výskytu vzorcov v obrázku a teda pomôže nájsť malvér a jeho nové varianty.

Binárne súbory s malvériom sú konvertované do 8 bitových vektorov pozostávajúcich z reťazca nul a jednotiek a sú organizované do dvojdimentzálnej matice formujúcej obrázky v šedých farbách. Autorovia týchto malvérov zmenia malú časť binárneho súboru a obrázky tieto malé zmeny zachytia v globálnej štruktúre. Obrázok 1 zobrazuje niekoľko vzorcov v obrázkoch malvéru v troch data-setoch. Podobnosť vo vzorcoch je vidno viac v jednotlivých skupinách malvéru rovnakej rodiny.

Obr. 1: Podobnosť obrázkov jednotlivých rodín malvéru



Ďaľší krok v procese je extrahovať vlastnosti týchto vzorcov z obrázkov a trénovať klasifikátor s týmito vlastnosťami. Techniky Data miningu a strojového učenia sú použité na vytvorenie inteligentnej detekcie malvéru a systémy klasifikátorov. Hlboké neurónové siete dosiahli veľký úspech v rôznych odvetiach, najmä v odvetí počítačového videnia. Aj keď modely hlbokého učenia sú výkonné, tak majú určité limity v realnych úlobach detekcie, hlavne v bezpečnostných doménach. Efektivita detekcie nekatogarizovaného malvéru a zero-day, je malá.

Modely hlbokého učenia sú trénované na spätnom šírení, kde je model trénovaný použitím stromového učenia. Keď zoberieme v potas všetky faktory, tak najlepší návrh je použit algoritmus Deep forest, ktorý má mnoho výhod oproti existujúcim modelom strojového a hlbokého učenia. Má zlepšenú presnosť de-

tekcie a nízku výpočtovú jednotku. Navrhovaný systém detekcie a klasifikácie škodlivého softvéru dobre zovšeobecňuje problém a je upovedomelý jeho kontextom. Zložitosť modelu, s pôistupom deep forest algoritmom je použitých menej hyper parametrov a v porovnaní s klasickým Deep learning algoritmom funguje dostatočne dobre aj v základnom nastavení. Tým pádom si nevyžaduje dodatočné ladenie parametrov. Deep forest funguje dobre aj s údajmi malého rozsahu, kde zvyčajne klasický deep learning zlyháva. Model nepotrebuje dodatočné výpočtové zdroje, ako napríklad akcelerácia pomocou GPU. Deep forest netrpí nadmerným upravovaním, pretože náhodnosť sa zvyšuje použitím rôznych vzoriek posvných okien a generujú sa vektory tried pomocou krížovej validácie.

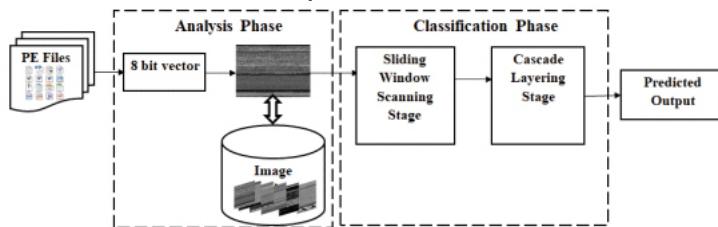
Tento model taktiež predviedol prvotriednu presnosť než existujúce schémy, v percentách 98.86% bez potreby extrahovať lokálne vlastnosti, čo naznačuje navrhovanú metódu ako slubný postup pri zisťovaní nového, zero-day a dokonca aj zamaskovaného malvéru.

## 4.2 Navrhovaný model

Obrázok 2 zobrazuje celkový dizajn navrhovaného systému na detekciu malvéru. Tento model pozostáva z dvoch fáz, fázy analýzy a fázy klasifikácie. Vo fáze analýzy je každý binárny súbor PE transformovaný do 2D poľa a vizualizovaný ako obrázok v odtieňoch sivej. Druhá fáza zahŕňa klasifikáciu malvéru do zodpovedajúcich tried na základe obrazových vzorov. V tejto fáze sa používa Deep forest algoritmus na detekciu a klasifikáciu malvéru. Deep forest zahŕňa dve fázy, a to skenovanie a kaskádové vrstvenie posuvných okien.

Motivovaný konceptom konvolučných neurónových sietí (CNNs), fáza skenovania posuvných okien je prijatá na zachovanie priestorového vzťahu medzi nespracovanými pixelmi. Každý binárny obrázok v trénovacej množine je daný ako vstup do fázy klasifikácie. Prvá etapa začína skenovaním vstupného obrazu s paralelným spracovaním dvoch posuvných okien. Sada menších inštancií sa získa z každého posuvného okna a trénuje sa s dvoma súbormi. Predpovede z oboch súborových forestov vracajú vektory pravdepodobnosti triedy. Tieto vektory tried z oboch posuvných okien sú zretazene, aby vytvorili viacrozmerné vektory prvkov, ktoré umožňujú modelu zvýšiť výkon.

Obr. 2: Navrhovaný model na detekciu malvéru



### 4.3 Uzavretie

Navrhovaný model ukázal mieru detekcie 98,65 %, 97,2 % a 97,43 % pre množiny malvérových údajov Malimg, BIG 2015 a MaleVis. Prístup sa vyznačuje vrstvením Deep forest súborov a nízkou zložitosťou modelu a prekonáva hlboké neurónové siete pri zistovaní malvéru. Navrhovaný model identifikuje neznáme vzorky škodlivého softvéru, ktoré patria do trénovaných rodín malvéru. Vzorky škodlivého softvéru, ktoré patria do iných rodín, ktoré nie sú trénované modelom, môžu vykazovať nesprávne predpovede. Budúca práca môže zahŕňať identifikáciu neznámych vzoriek netrénovaných rodín pomocou thresholdu. Oblasť kybernetickej bezpečnosti je veľmi rýchla, odborníci sa stále musia prípravovať na nové výzvy, teraz je ľahko povedať či tento model bude stále vhodným návrhom pri komplexnejších malvéroch v tejto dobe.

## 5 Záver

V tejto práci som sa venoval základnému pojmu Modelovanie v Softvérovom inžinierstve za pomoci [2], v Sekcii 3 som rozobral nedávne pokroky v Kybernetickej bezpečnosti, kde som sa venoval porovnaniu klasickej detekcie malvéru s pokročilejšími metódami vybraných z článku [1]. A ako hlavnú tému som rozobral Detekciu malvéru pomocou hlbokého učenia 4 kde som rozobral navrhovaný model na detekciu malvéru a jeho možné vylepšenie v budúcnosti, v článku [3].

## Literatúra

- [1] Edward Amoroso. Recent progress in software security. 35(2):11–13, March 2018.
- [2] Joanne M. Atlee, Robert France, Geri Georg, Ana Moreira, Bernhard Rumpe, and Steffen Zschaler. Modeling in software engineering. IEEE, May 2007.
- [3] S. Abijah Roseline, S. Geetha, Seifedine Kadry, and Yunyoung Nam. Intelligent vision-based malware detection and classification using deep random forest paradigm. 8:206303–206324, 2020.