UNIVERSITATEA POLITEHNICA DIN BUCUREȘTI

Școala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. 940 din 21.10.2022

REZUMAT TEZĂ DE DOCTORAT

Ing. Cristian PASCARIU

UTILIZAREA TEHNICILOR INTELIGENȚEI ARTIFICIALE ÎN ANALIZA MALWARE

USING ARTIFICIAL INTELLIGENCE TECHNIQUES FOR MALWARE ANALYSIS

COMISIA DE DOCTORAT

Prof. Dr. Ing. Ion MARGHESCU Universitatea Politehnica din București	Președinte
Prof. Dr. Ing. Ioan BACIVAROV Universitatea Politehnica din București	Conducător de doctorat
Prof. Dr. Ing. Mircea POPA Universitatea Politehnica Timișoara	Referent
Prof. Dr. Ing. Gheorghe ȘERBAN Universitatea din Pitești	Referent
Prof. Dr. Ing. Paul ȘCHIOPU Universitatea Politehnica din București	Referent

BUCUREȘTI 2022

Cuprins (Rezumat)

Cuprins (Teză de doctorat)

Capitolul 1

Introducere

Tehnologia informației este unul dintre domeniile care a cunoscut o dezvoltare semnificativă în ultimele decenii, ceea ce a contribuit decisiv la îmbunătățirea și modernizarea metodelor de comunicare și procesare a informațiilor în format digital. În prezent sistemele de calcul au devenit indispensabile datorită gradului ridicat de utilizare în societatea modernă. Siguranța în funcționare (*dependability*) [1] a sistemelor informatice este un element foarte importat și a căpătat un interes deosebit în ultima perioadă deoarece funcționarea necorespunzătoare a acestor sisteme va conduce la un evident impact economic, dar poate afecta calitatea vieții omenești.

Securitatea cibernetică reprezintă un domeniu care are la bază trei factori importanți: confidențialitatea, integritatea și disponibilitatea informațiilor prelucrate de un sistem de calcul. Riscurile cu privire la incidentele și brețele de securitate au un impact major asupra bunei funcționare a organizațiilor, dar mai important și asupra nivelului vieții pentru utilizatorii tehnologiei informației. Metodologiile și soluțiile existente pentru detectarea și analiza atacurilor și a virușilor cibernetici au limitări care au fost identificate și catalogate ca urmare a brețelor de securitate documentate public.

1.1 Prezentarea domeniului tezei de doctorat

Pentru prezentarea domeniului tezei de doctorat am abordat conceptul de digitalizare care presupune că o serie de procese care erau bazate pe documente fizice au fost transformate și implementate digital. Pe baza etapei inițiale, unde am stabilit gradul de importanță și aspectul critic al sistemelor de calcul în societatea modernă, în etapa următoare am abordat domeniul securității informației și a sistemelor de calcul. Am documentat aspectele fundamentale ale acestui domeniu ca fiind confidențialitatea, integritatea și disponibilitatea informațiilor, orice *acțiune care degradează sau afectează într-un mod negativ unul sau mai multe dintre aceste aspecte fiind considerată o amenințare cibernetică*. Ulterior am abordat dezvoltarea substanțială a noilor domenii precum *Internetul Obiectelor* (IoT - Internet of Things), *Cloud* și *Orașe inteligente* (Smart Cities), concepte moderne care au schimbat modul de abordare a securității cibernetice. În etapa finală a prezentării domeniului tezei de doctorat am prezentat provocările actuale, care constau în limitarea capabilităților și a soluțiilor

existente de a detecta și împiedica atacurile cibernetice, lipsa unei resurse umane calificate în domeniu și nivelul ridicat de complexitate al virușilor informatici.

Atât instituțiile publice, cât și organizațiile private utilizează sisteme de calcul pentru a oferi servicii ce au la bază procesarea informațiilor în format digital. Acestea au înlocuit procesele tradiționale bazate pe documente și formulare fizice, care au fost înlocuite cu documente digitale. Gartner definește fenomenul de digitalizare ca „*utilizarea tehnologiilor digitale pentru a schimba modul de a oferi servicii"* [3].

Pornind de la premisa că sistemele de calcul au devenit o componentă integrată și indispensabilă în modul în care organizațiile oferă servicii, rezultă că siguranța în funcționare a acestor sisteme, atât în buna desfășurare a activităților normale, cât și pentru protejarea datelor, a devenit un obiectiv strategic, de maximă importanță. Securitatea informațiilor și a sistemelor de calcul are la bază trei aspecte fundamentale care sunt definite de standardul ISO/IEC 27000 [4]:

- *Confidențialitatea datelor:* „informațiile nu sunt puse la dispoziție sau dezvăluite persoanelor, entităților sau proceselor neautorizate";
- *Integritatea datelor*: reprezintă „acuratețea și completitudinea datelor" stocate sau procesate de un sistem de calcul;
- *Disponibilitatea datelor*: informațiile sunt „accesibile și utilizabile la cerere de către o entitate autorizată" [5].

Orice factor care degradează sau are un impact negativ asupra unuia sau mai multor factori ai securității informației este considerat o *amenințare cibernetică (threat)* [5]. Pe baza analizei prezentate în acest raport, ENISA Threat Landscape 2021 identifică și se concentrează asupra următoarelor 8 grupuri principale de amenințări cibernetice (Tabelul 1.1).

Tabelul 1.1 *Principalele amenințări cibernetice în 2020-2021 (conform ENISA) [16].*

Nivel importanță	Tip amenințare
1	Ransomware
2	Malware
3	Cryptojacking
4	Amenințări legate de poșta electronică
5	Amenințări la adresa datelor
6	Amenințări privind disponibilitatea și integritatea serviciilor
7	Dezinformare
8	Amenințări non-malițioase

1.2 Scopul tezei de doctorat

Securitatea cibernetică a devenit un domeniu important, care stă la baza funcționării organizațiilor și instituțiilor în prezent. Scopul tezei de doctorat este de a efectua o analiză a provocărilor actuale, atât tehnice cât și organizatorice, pe baza căreia am elaborat, testat și propus soluții de îmbunătățire a capabilităților și proceselor ce fac parte din strategia de apărare cibernetică.

În contextul provocărilor legate de implementarea măsurilor organizatorice, obiectivul principal este de a identifica metodologiile de securitate cibernetică orientate pe amenințări pe baza cărora procese și fluxuri de lucru sunt implementate pentru a îmbunătății eficiența cu are o organizație răspunde la incidentele de securitate, reduce riscul breșelor de securitate precum și a impactului acestora asupra organizației.

Capabilitățile de detecție și prevenție a atacurilor cibernetice sunt o componentă importantă a strategiei de apărare. În această teză de doctorat am identificat și am analizat limitările și oportunitățile în ceea ce privește detecția malware, pe baza cărora am propus soluții complementare pentru identificarea atacurilor cibernetice folosind algoritmi din domeniul inteligenței artificiale.

Scopul cercetărilor desfășurate în perioada stagiului doctoral a constat în dezvoltarea unor soluții destinate minimizării riscurilor atacurilor cibernetice și atenuării impactului pe care breșele de securitate îl pot avea asupra confidențialității, integrității și disponibilității datelor. Un alt scop al lucrării este de a pune în evidență oportunitățile de transfer de cunoștințe din mediul academic în mediul comercial, dar și atragerea de fonduri și granturi de cercetare din mediul comercial în mediul academic, construind o relație de colaborare cu beneficii pentru ambele părți. În ceea ce privește transferul de cunoștințe din mediul academic, algoritmii avansați de procesare a datelor pot fi implementați pentru a rezolva problemele reale cu care organizații de toate dimensiunile și profilurile se confruntă în domeniul securității informației.

1.3 Conținutul tezei de doctorat

Teza de doctorat este structurată în 5 capitole împreună cu lista tabelelor, lista figurilor și lista abrevierilor folosite. Lucrarea se încheie prin expunerea referințelor bibliografice.

În **Capitolul 1** am prezentat partea introductivă a domeniului tezei de doctorat referitoare la securitatea informației și a sistemelor de calcul. Am făcut o prezentare evolutivă a sistemelor de calcul și a termenilor actuali care le caracterizează. Am indicat factorii ce au contribuit la evoluția majoră a sistemelor de calcul și totodată a riscurilor și a impactului ce pot rezulta în urma incidentelor și breșelor de securitate. Am realizat un studiu pe baza căruia am identificat provocările actuale pe care organizațiile și companiile le au în domeniul securității informației, una dintre cele mai importante fiind lipsa de resurse și experți în domeniu. În paralel am făcut un alt studiu asupra evoluției bibliotecilor ce implementează algoritmi din domeniul inteligenței artificiale, iar pe baza acestuia am definit obiectivul principal al tezei de doctorat ca fiind analiza și implementarea de algoritmi inteligenți pentru automatizarea și simplificarea proceselor de detecție și analiză a atacurilor cibernetice și a virușilor informatici. Capitolul continuă cu prezentarea obiectivelor principale ale tezei.

Capitolul 2 detaliază conceptul de securitate a informației prin abordarea componentelor de bază precum confidențialitatea, integritatea și disponibilitatea datelor. Tot în acest capitol sunt analizate tipurile de atacuri cibernetice și clasificarea

virușilor informatici. Capitolul continuă printr-o analiză a schimbării paradigmei de securizare a sistemelor de calcul, care în trecut se implementa la nivelul rețelei, unde sistemele ce se află în perimetrul rețelei sunt considerate ca fiind sigure, iar cele din afară sunt considerate ostile și trebuie verificate. Am continuat prin prezentarea aprofundată a noi concepte precum Cloud Computing și IoT, unde paradigma de protecție la nivel de rețea nu mai poate fi aplicată cu succes. Am continuat prin a efectua o analiză a riscurilor și a tehnicilor de securizare pentru orașe inteligente (Smart Cities). Capitolul continuă cu un studiu al metodologiilor propuse de organizații al căror scop este de a dezvolta standarde, politici și controale de securitate. Pe baza acestui studiu am propus două metodologii care reprezintă fundamentul pentru următoarele capitole.

Capitolul 3 debutează printr-un studiu al abordărilor existente în ceea ce privește strategia de apărare cibernetică și mă voi concentra pe strategia de apărare orientată pe amenințări. Voi propune o arhitectură de referință pentru un mediu izolat folosind o soluție de virtualizare pentru simularea și analiza breșelor de securitate bazat pe tehnologii open-source. Malware precum și alte tehnici ofensive vor fi folosite pentru simularea atacurilor în mod controlat; voi continua cu analiza a capabilităților și tehnicilor existente de detectare a atacurilor cibernetice atât la nivel de rețea, cât și la nivel de sistem de calcul individual. Pe baza atacurilor cibernetice simulate, îmi propun să identific limitările tehnicilor de detecție, dar și a oportunităților unde tehnici din domeniul inteligenței artificiale se pot aplica cu succes.

Capitolul 4 prezintă într-o primă etapă o analiză amănunțită a oportunităților unde algoritmi din domeniul inteligenței artificiale pot fi aplicați pentru rezolvarea problemelor de clasificare. Am identificat trei etape: etapa de pre-infectare, etapa de infectare și etapa de post-compromitere. Am continuat prin analizarea caracteristicilor paginilor de phishing și am propus o soluție de detectare a acestora pe baza analizei automate a similitudinilor. Pentru etapa de infectare m-am concentrat pe analiza ierarhiei proceselor pentru descoperirea de șabloane care identifică când procese legitime ale sistemului de calcul sunt folosite pentru a infecta un sistem și am continuat cu dezvoltarea unei soluții bazate pe rețele neuronale, capabilă să identifice aplicații malware. Pentru etapa de post-compromitere am efectuat analiza malware într-un mediu virtual izolat a unui tip de Ransomware din familia Stampado. Pe baza indicatorilor obținuți în urma analizei am implementat o soluție de tip honeypot pentru detectarea propagării virușilor de tip Ransomware într-o rețea de calculatoare și de asemenea pentru detectarea pacientului 0, mai precis primul sistem de calcul care a fost infectat.

Capitolul 5 este dedicat principalelor contribuții și rezultate privind analiza și dezvoltarea de soluții pentru detectarea atacurilor cibernetice bazate pe algoritmi din domeniul inteligenței artificiale. În final am identificat și documentat câteva direcții de dezvoltare care pot aduce îmbunătățiri soluțiilor prezentate în această lucrare de doctorat.

Capitolul 2

Securizarea sistemelor de calcul

În **Capitolul 2** am efectuat o analiză detaliată a riscurilor și amenințărilor cibernetice pe baza incidentelor și breșelor de securitate care s-au întâmplat în ultimul deceniu și au fost documentate în spațiul public. Am continuat prin a face un studiu asupra impactului pe care aceste breșe de securitate îl are asupra cetățenilor de rând și asupra organizațiilor, unde datorită fenomenului de digitalizare, incidentele de securitate pot reduce sau chiar opri activitățile de zi cu zi, ceea ce implică un impact financiar aferent. Am efectuat de asemenea o analiză asupra metodologiilor existente, metodologii care propun tehnici de detecție și analiză a atacurilor și virușilor informatici. Am propus metode de abordare care pot fi însușite de organizații pentru identificarea, analiza și prevenirea atacurilor cibernetice bazate pe metodologii în vigoare dezvoltate de comunitatea globală de analiști de securitate. „Cyber Kill Chain" este o metodologie utilizată pentru a aborda atacurile cibernetice ca pe o serie de etape pe care atacatorul trebuie să le parcurgă pentru ca atacul să aibă succes. A doua metodologie prezentată este MITRE ATT&CK: aceasta conține o colecție cu definiții de tipuri de atac bazate pe categorii.

2.2 Analiza bibliotecilor SSL pentru dispozitive IoT

Printre contribuțiile personale notate în lucrarea [34] se numără și analiza riscului și a vulnerabilităților platformelor IoT. Printr-o serie de teste și revizuirea bibliotecilor disponibile am identificat vulnerabilități cauzate de lipsa implementării protocoalelor standard pentru SSL/TLS.

În situațiile când certificatele digitale sunt revocate ca urmare a unei breșe, există protocoale precum lista de revocare a certificatelor (CRL - Certificate Revocation List). RFC 5280 [44] ce descrie un CRL ca „o structură de date marcată și semnată pe care o autoritate de certificare (CA) sau un emitent de CRL o emite periodic pentru a comunica starea de revocare a certificatelor digitale afectate". Am identificat o bibliotecă pentru soluții IoT care nu implementează tehnici precum CRL și/sau OSCP care vor continua să inițieze comunicații cu un serviciu al cărui certificat digital a fost revocat. Acesta reprezintă un risc și totodată și o vulnerabilitate [45].

Analiza inițială a fost efectuată în anul 2016, revizitând platforma hardware, însă aceasta nu mai este disponibilă [46], iar producătorul recomandă folosirea unei alte platforme actualizate. Platforma software și bibliotecile nu au mai fost actualizate din anul 2017 conform paginii de Github unde poate fi regăsit codul sursă [47]. Acest lucru duce ca o serie de produse IoT, după o perioadă de funcționare de câțiva ani, deși funcționale, să reprezinte oportunități de atac în plan public sau privat [48].

2.3 Utilizarea platformelor IoT pentru securizarea rețelelor informatice

Riscuri și vulnerabilități există de asemenea și în platformele IoT, extinzând astfel expunerea la atacuri cibernetice. Totodată, datorită creșterii puterii de calcul și a resurselor ce sunt la dispoziție dispozitivelor IoT, precum și costului scăzut al acestora, este creată oportunitatea de apariție a dispozitivelor de securitate IoT.

În articolul „*Network security monitoring with embedded platforms*” [52] am contribuit, folosind dezvoltările și rezultatele din [53], la o soluție pentru detectarea atacurilor cibernetice la nivel de rețea folosind platforma Raspberry Pi [54]. Folosind limbajul de programare Python [55] și biblioteca Scapy [56] pentru analiza traficului și a pachetelor de date, am implementat o soluție capabilă să detecteze atacurile de tip ARP Spoofing (Address Resolution Protocol) [57] prin care un atacator care are deja acces la rețea încearcă să falsifice identitatea router-ului pentru a putea intercepta traficul de la anumiți utilizatori. Tehnica de detecție se bazează pe identificarea răspunsurilor ARP care au o adresă IP a gateway diferită de cea originală.

2.5 Măsuri organizatorice de îmbunătățire a securității cibernetice

Transformarea digitală, tehnologiile cloud și un peisaj sofisticat de amenințări obligă organizațiile să regândească funcțiile fiecărui rol în echipele lor de securitate. Cu miliarde de oameni de pe tot Globul, care lucrează de acasă, schimbările în practica zilnică de implementare a securității cibernetice se accelerează. Organizațiile trec de la apărarea unui perimetru de rețea tradițional la strategii mai eficiente precum *Zero Trust*. Această transformare aduce schimbări tehnologice și, de asemenea, deschide întrebări despre cum vor arăta rolurile și responsabilitățile oamenilor în această lume nouă.

În același timp, modelele de livrare continuă necesită ca echipele de securitate să se implice mai îndeaproape în timpul planificării și dezvoltării aplicațiilor pentru a gestiona eficient riscurile cibernetice (comparativ cu abordările tradiționale de securitate „la distanță maximă”). Acest lucru necesită ca specialiștii în securitate să înțeleagă mai bine contextul de afaceri și să colaboreze mai strâns cu părțile interesate din afara securității [72].

Capitolul 3

Detectarea atacurilor cibernetice

În **Capitolul 3** m-am concentrat pe evaluarea strategiilor de apărare și capabilităților de detecție și analiză a atacurilor cibernetice. Din punct de vedere al strategiei de apărare am concluzionat că abordarea tradițională, orientată pe vulnerabilități, are limitări în ceea ce privește detectarea atacurilor cibernetice moderne. Am propus utilizarea strategiei de apărare orientată pe amenințare, ce presupune un proces continuu de detecție și analiză, cât și identificarea oportunităților de îmbunătățire.

Am continuat prin a analiza eficiența capabilităților de detecție, precum și limitările acestora. Pe baza simulării atacurilor cibernetice într-un mediu controlat și izolat am identificat potențiale limitări în ceea ce privește capabilitățile tradiționale bazate pe reguli. Deși aceste capabilități pot detecta virușii deja cunoscuți, atacatorii pot modifica sau crea viruși noi, pentru care gradul de detecție este scăzut.

Printr-un studiu detaliat al amenințărilor am evidențiat că atacurile cibernetice, datorită varietății tehnicilor folosite, dar și a complexității atacurilor cibernetice, nu există o singură metodă sau un sistem prin care acestea pot fi detectate. Detectarea cu succes a atacurilor cibernetice se bazează pe mai multe capabilități ce sunt integrate între ele și funcționează în tandem, acestea putând fi clasificate în două mari categorii: la nivel de rețea și la nivel de sistem. Am constatat o strategie de apărare bazată numai pe capabilități automate de detecție nu este suficientă, iar o organizație are nevoie de analiști în domeniul securității cibernetice pentru efectuarea analizei prin corelarea mai multor surse de date.

3.2 Simularea atacurilor cibernetice

Am implementat o soluție pentru simularea atacurilor cibernetice, care va permite atât simularea atacurilor într-un mediu controlat, cât și utilizarea și testarea eficienței și randamentului capabilităților de detecție și analiză a acestor atacuri. Această tehnică este des utilizată de specialiștii în securitate cibernetică care analizează și studiază comportamentul malware [83].

Ca platformă am optat pentru folosirea unei soluții de virtualizare VMware Worksation [84]. În Figura 3.2 este ilustrat mediul de simulare și analiză a atacurilor cu toate componentele. Am simulat o rețea de calculatoare prin crearea de mașini virtuale

cu sisteme de operare atât Windows cât și Linux. Conectată la aceeași rețea este și o mașină virtuală Kali Linux [86], cu rolul de a simula sistemul atacatorului. Kali Linux este folosit de experții în securitate pentru a simula atacuri asupra sistemelor de calcul și aplicațiilor.

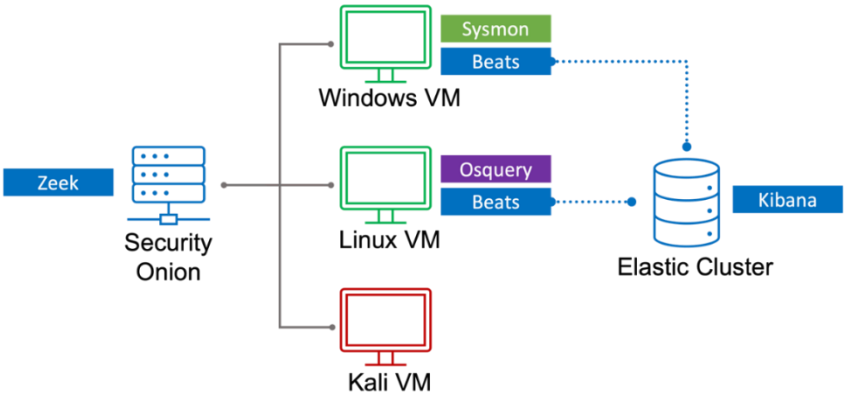

Figura 3.2 *Mediu virtual de simulare și analiză a atacurilor.*

Pe mașina virtuală Windows VM am instalat și configurat programul Sysmon [87], acesta monitorizează evenimente importante precum crearea de procese noi, comenzi WMI și activitatea la nivel de rețea care este inițiată de procese. Osquery [90] este o soluție de monitorizare și detecție a evenimentelor și setărilor de configurare pentru sisteme de calcul pentru sistemele Linux. Pentru monitorizarea traficului din rețea am utilizat soluția Security Onion [91]. Una dintre soluțiile importante de tip IDS (Intrusion Detection System) care face parte din platforma Security Onion este Zeek [92], cunoscut și sub numele de Bro. Elastic Stack [93] este o platformă pentru a colecta și stoca log-uri, oferind analiștilor de securitate oportunitatea de a analiza evenimente legate de securitate. Platforma Elastic are la bază trei componente: Elasticsearch [94] - componenta de stocare, Kibana [95] - interfața web și Beats [97] - agenții instalați pe sistemele de calcul pentru a colecta log-uri.

3.3.3 Detectarea atacurilor cibernetice pe baza anomaliilor

Am simulat un atac cibernetic folosind un virus de tip „backdoor” în mediul izolat, după care am continuat prin efectuarea analizei la nivel de rețea a datelor înregistrate pe baza de traficului generat de virus. În reprezentarea din Figura 3.15 se poate observa cum conexiuni de date au loc la intervale constante de timp, precum și cantitatea constantă a numărului de pachete, iar în Figura 3.16 se poate observa cum evenimentele sunt înregistrate la fiecare 10 secunde. Aceste impulsuri sunt generate de pe sistemul infectat, care încearcă să se conecteze la serverul controlat de către atacator.

Am continuat analiza la nivel de sistem de calcul prin efectuarea unei căutări pentru a identifica procese malițioase care vor să fure detalii de autentificare din alte procese folosind un cod specific al drepturilor de acces, și anume 0x1010. În Figura

3.31 am identificat un proces malițios care utilizează această tehnică pentru extragerea parolelor și a codurilor unice din procesul *lsass*.

Figura 3.15 *Detecția anomaliilor pe baza intervalelor de timp dintre conexiuni.*

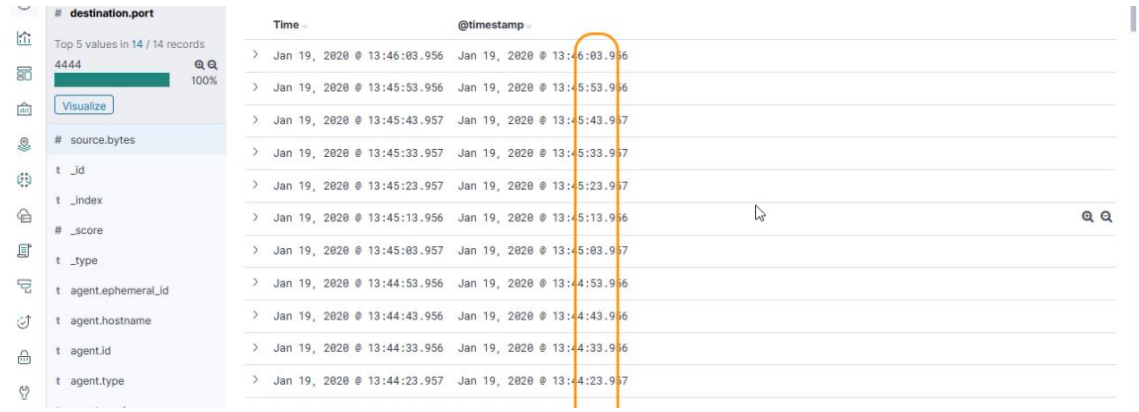

Figura 3.16 *Detecția traficului de tip „beaconing”.*

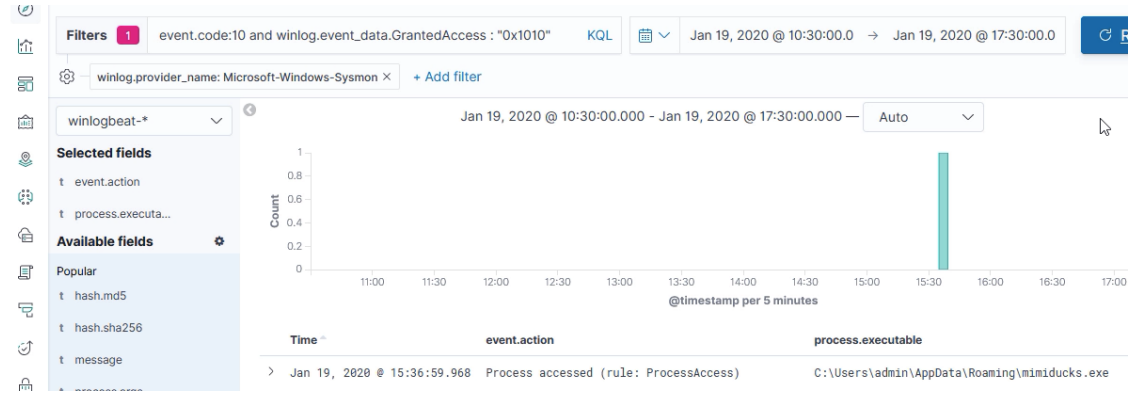

Figura 3.31 *Identificarea unui proces malițios prin intermediul drepturilor de acces.*

Adițional, în Figura 3.34 am identificat o succesiune de comenzi PowerShell incluse una în alta pentru a evita detecția. Prima comandă conține un set de comenzi codat folosind algoritmul Base64. Următorul eveniment este generat pentru aceeași comandă, numai că este decodată oferind oportunitatea unui analist de securitate pentru a extrage indicatori. Am identificat de asemenea și virusul care este utilizat pentru furtul de parole din memoria sistemului.

Figura 3.34 *Detecția execuției malware folosind comenzi PowerShell.*

3.5 Corelarea evenimentelor la nivel de sistem cu cele la nivel de rețea

Pentru determinarea scopului și impactului unui atac cibernetic sunt necesare identificarea și documentarea tuturor acțiunilor efectuate pe parcursul atacului, ceea ce presupune corelarea evenimentelor și indicatorilor înregistrați la nivel de rețea cu cei la nivel de sistem de calcul.

În Figura 3.50 am identificat o succesiune de evenimente suspecte, pornind de la un indicator menit să detecteze procese suspecte al căror fișier a fost șters de pe disc, am identificat un proces cu un nume suspect dar și o adresă IP. Pe baza acestei adrese am efectuat o nouă căutare unde am identificat alte procese legitime care au fost executate pentru a facilita atacul. Corelarea evenimentelor înregistrate la nivel de sistem cu evenimentele înregistrate la nivel de rețea oferă analiștilor de securitate care efectuează investigația o perspectivă de ansamblu. Acest set de date extins, precum și capabilitatea de a formula filtre și condiții, permit analiștilor de securitate să identifice lanțul complet al atacului cibernetic.

```
osquery> SELECT DISTINCT p.pid, p.name, p.path, s.remote_address, s.remote_port FROM processes AS
 p JOIN process_open_sockets AS s ON p.pid=s.pid WHERE p.on_disk=0;
+-------+-------+------------+-----------------+-------------+
| pid   | name  | path       | remote_address  | remote_port |
+-------+-------+------------+-----------------+-------------+
| 10599 | PwUcb | /tmp/PwUcb | 192.168.253.162 | 4444        |
| 10599 | PwUcb | /tmp/PwUcb | 192.168.253.162 | 4433        |
+-------+-------+------------+-----------------+-------------+
osquery> SELECT DISTINCT p.pid, p.name, s.remote_address, s.remote_port FROM processes AS p JOIN
process_open_sockets AS s ON p.pid=s.pid WHERE s.remote_address == "192.168.253.162";
+-------+--------+-----------------+-------------+
| pid   | name   | remote_address  | remote_port |
+-------+--------+-----------------+-------------+
| 10347 | python | 192.168.253.162 | 4444        |
| 10348 | bash   | 192.168.253.162 | 4444        |
| 10599 | PwUcb  | 192.168.253.162 | 4444        |
| 10599 | PwUcb  | 192.168.253.162 | 4433        |
+-------+--------+-----------------+-------------+
```

Figura 3.50 *Identificarea proceselor suspecte pe baza conexiunilor cu o adresă IP.*

Capitolul 4

Utilizarea tehnicilor inteligenței artificiale în analiza malware

În **Capitolul 4**, în urma unui studiu al soluțiilor care au la bază algoritmi din domeniul inteligenței artificiale, am concluzionat că acestea au anumite limitări în ceea ce privește modul de abordare (și nu fiabilitatea algoritmilor). Această concluzie este susținută și de alți autori care au efectuat experimente și au demonstrat eficiența scăzută a acestor soluții atunci când setul de date este diferit față de cel de antrenare. Ca urmare, am propus un set de soluții ce aderă principiilor sistemelor inteligente, precum luarea deciziilor în condiții de incertitudine și formarea inferențelor folosind o bază de cunoștințe proprii, menite să ajute un analist de securitate prin automatizarea sarcinilor manuale pe care acesta trebuie să le efectueze în timpul unei investigații.

Am concluzionat de asemenea că orice algoritm de învățare automată reprezintă un modul în cadrul unei soluții mai ample și algoritmul în sine nu reprezintă soluția în sine. În urma experimentelor am observat gradul ridicat de importanță pe care îl are selecția atributelor unei sarcini de analiză a unui atac atunci când aceste atribute servesc ca set de date de intrare pentru algoritmul de învățare automată.

4.1 Studiu privind tehnicile de detecție a website-urilor de phishing

Phishing-ul reprezintă o tehnică de inducere în eroare și înșelare a utilizatorilor unui serviciu web sau ai unei platforme digitale prin intermediul unei pagini web similare cu cea originală, dar cu scopul de a fura detaliile de autentificare. Studiul soluțiilor existente în domeniu a condus la identificarea mai multor abordări pentru combaterea atacurilor cibernetice ce folosesc pagini web de phishing pentru furtul de detalii de autentificare.

Detecția bazată pe adresa Uniform Resource Locator (URL) se concentrează pe indicatorii cheie extrași din adresa URL, cum ar fi domeniul, subdomeniul, protocolul, directorul web și alți parametri ai adresei URL. Atacatorii folosesc tehnica denumită „typosquatting” [125] pentru a înregistra în mod deliberat domenii similare celor legitime în care un singur caracter (o literă sau o cifră) pot fi diferite. Această

tehnică se bazează pe erorile care pot fi comise de utilizatori atunci când tastează o adresă web.

O altă tehnică îngrijorătoare este atunci când atacatorii vor crea un subdomeniu identic cu cel legitim pentru domeniul lor rău intenționat [126]. Browserele web vor scurta lungimea adresei URL complete, iar victimele vor considera că vizitează serviciul legitim atunci când, de fapt, îl vizitează pe cel rău intenționat. În Figura 4.2 am ilustrat un website de phishing cu o adresă foarte lungă, iar subdomeniul înregistrat conține numele serviciului legitim Paypal.

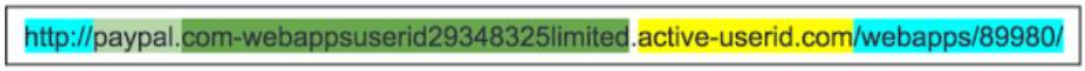

Figura 4.2 *Domeniu malițios ce folosește domeniul legitim ca un subdomeniu.*

4.2 Soluție de detectare a paginilor de phishing pe baza similitudinilor

Am propus o metodă nouă de detectare a site-urilor web de phishing pe baza analizei de similitudini dintre o pagină legitimă și una de phishing care încearcă să o imite. Această analiză este efectuată atât la nivel de adresă URL, cât și la nivel de conținut. Pentru analiza URL am folosit un algoritm pentru identificarea similitudinilor șirurilor de caractere (Longest Common Subsequence - LCS) [130] pentru a detecta domeniile similare. Analiza bazată pe conținut este utilizată pentru a identifica paginile web de phishing care imită pe cele legitime pe baza similarității cuvintelor cheie din titlu, precum și a existenței cuvintelor cheie specifice paginilor de autentificare. Un alt avantaj al soluției propuse este că nu necesită un set amplu de date pentru antrenare, informațiile fiind colectate folosind adresa URL și conținutul paginilor legitime. Pe baza acestora, toate site-urile web suspecte vor fi scanate, caracteristicile acestora vor fi extrase și comparate cu caracteristicile paginilor legitime. Lipsa necesității antrenării algoritmilor de învățare automată precum și setul redus de caracteristici care sunt extrase și procesate scad cantitatea de resurse de calcul necesare, lucru care face ca soluția să fie rapidă.

Tabelul 4.1 ilustrează caracteristicile bazate pe adresele URL. Una dintre cele mai importante este caracteristică domeniului similar. În limbajul Python am folosit modulul *Difflib* pentru a genera procentajul de similitudine la nivel de șir de caractere.

Tabelul 4.1 *Funcții bazate pe URL.*

Caracteristică	Descriere
Domeniu similar	Gradul de similitudine dintre domeniul suspect și cel legitim
Subdomeniu	Domeniu legitim folosit ca subdomeniu al domeniului dăunător

Tabelul 4.2 conține caracteristicile bazate pe conținut folosite de soluția propusă pentru a detecta dacă în conținutul site-ului web scanat sunt cuvinte cheie care se potrivesc cu serviciul legitim, dar conține și elemente tipice ale unei pagini de login.

Tabelul 4.2 *Funcții bazate pe conținut.*

Caracteristică	Descriere
Cuvinte cheie de titlu	Cuvintele individuale sunt extrase și comparate între site-ul web scanat și linia de bază
Cuvinte cheie de autentificare	Set generic de cuvinte cheie care pot fi găsite în paginile de conectare generice, cum ar fi „Sign in”, „Log in”, „Authenticate”, „<input type = ”password”>”

4.2.3 Testare și rezultate

Site-urile web de phishing au o durată de viață scurtă [131], de la câteva ore la mai multe zile, până când acestea sunt descoperite și eliminate de către furnizorii de servicii de găzduire web. Ca alternativă, am optat pentru a utiliza o listă de pagini de phishing care sunt deja cunoscute și pentru a testa eficiența detectării unor nume de domenii similare.

Tabelul 4.3 *Rezultatele detecției adreselor URL [123].*

Domeniu	Raportul de similaritate
googlej [.] com	95%
googled [.] com	95%
xn - oole-z7bi [.] com	59%
yahoo [.] com	63%
hotmail [.] com	57%
microsoft [.] com	52%

Tabelul 4.3 [123] evidențiază rezultatele pentru un set de domenii în comparație cu domeniul „google.com”, care a fost selectat ca domeniu de referință și datorită popularității. Se poate observa că domeniile rău intenționate cunoscute, similare domeniului de bază, au generat un procent de peste 90%, în timp ce alte domenii legitime au generat un scor mai mic, de 75%. Extinzând testele și analiza pe domenii similare pentru google.com, am obținut circa 264 de domenii unice care sunt similare cu *google.com*. Lista domeniilor a fost extrasă din serviciul online DNStwist [132] care generează domenii înregistrate cu greșeli (intenționate) de ortografie. Acestea au fost folosite ca set pentru datele de test. Rezultatele analizei sunt ilustrate în Tabelul 4.4. Dintre acestea, 40% din domenii au obținut un scor de similaritate mai mare de 90%.

Tabelul 4.4 *Analiza domeniului similar.*

Similitudini (%)	Număr domenii	Detalii
> 90%	105 (40%)	Domenii similare
70% - 89%	74 (28%)	Domeniul legitim face parte din domeniul scanat
<60%	85 (32%)	Domenii Unicode

Pentru a testa eficiența detecției bazate pe conținut, am utilizat *Social Engineer Toolkit* (SET) [133], o soluție pentru efectuarea evaluărilor de securitate concentrate pe ingineria socială (*social engineering*). În scopuri de testare, pagina generată de Social Engineer Toolkit a fost analizată în raport cu pagina legitimă de conectare Gmail. Rezultatele acestei analize sunt indicate în Tabelul 4.5.

Tabelul 4.5 *Rezultatele detectării conținutului.*

Funcții bazate pe conținut	Scor rău intenționat
Asemănarea titlului	100%
Cuvinte cheie de autentificare	(3/5)

Am continuat testarea eficienței soluției pentru un scenariu mai realist. Am ales ca țintă platforma Easychair. În acest sens am înregistrat domeniul *Easychalr.org*, unde litera „i” este înlocuită cu litera „l”, în așa fel încât un utilizator nu poate depista eroarea la prima vedere.. Apoi am folosit programul SET pentru a crea o copie a paginii de autentificare pentru platforma Easychair.

Am continuat prin efectuarea analizei de similitudini folosind soluția propusă la linia de comandă, unde am constatat rezultatele pozitive generate. Analiza de similitudine a adresei URL a generat un scor de 92%, așa cum este ilustrat în Figura 4.5.

Figura 4.5 *Raportul analizei de similitudini a adresei URL.*

În ceea ce privește analiza conținutului am constatat următoarele rezultate (așa cum sunt ilustrate în Figura 4.6):

- a fost identificată o similitudine a titlului cu un scor de 97%;
- a urmat identificarea cuvintelor cheie („login”, „log in”) și a parametrilor specifici paginilor de autentificare (*password input field*).

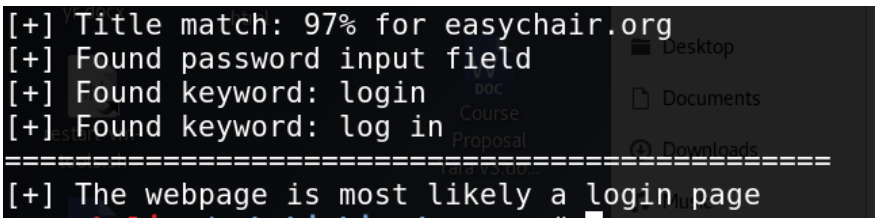

Figura 4.6 *Raportul analizei de similitudini a conținutului.*

4.3 Analiza ransomware (Stampado)

Înainte de a propune un mecanism de detecție a infecțiilor ransomware într-o rețea am efectuat analiza malware a unui tip de ransomware denumit Stampado.

Am utilizat serviciul VirusTotal.com, pentru analiza statică pe baza căreia am observat scorul ridicat de detecție. Conform rezultatelor din Figura 4.7, un număr de 54 de soluții antivirus au detectat fișierul ca fiind malițios.

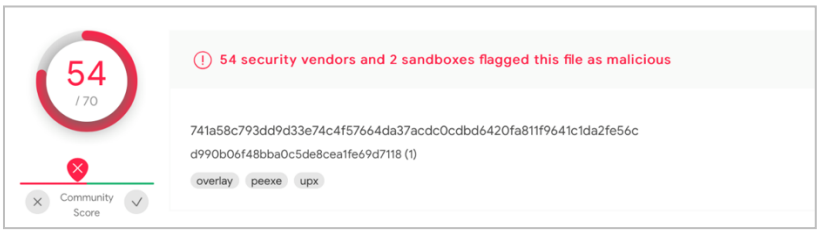

Figura 4.7 *Scorul de detecție pentru virusul ransomware Stampado.*

Folosind soluția sandbox Hybrid-Analysis pentru analiza dinamică, am identificat în Figura 4.11 că virusul a fost livrat inițial folosind un document infectat. Un alt indicator important este numele procesului scvhost.exe, nume similar cu un proces legitim al sistemului de operare Modul în care am stabilit că procesul nu este cel legitim este pe baza locației pe disc.

Figura 4.11 *Ierarhia de execuție a proceselor în cadrul infectării cu Stampado.*

Am continuat să analizez virusul în mediul izolat de testare, am identificat două mecanisme de propagare. Primul, ilustrat în Figura 4.14, utilizează funcția *autoplay* [139] a sistemului de operare pentru lansarea programelor prin intermediul fișierului *autorun.inf*: în funcție de setările și politicile sistemului, virusul poate fi executat automat atunci când dispozitive periferice de stocare precum memoriile USB sunt conectate la sistemul de calcul.

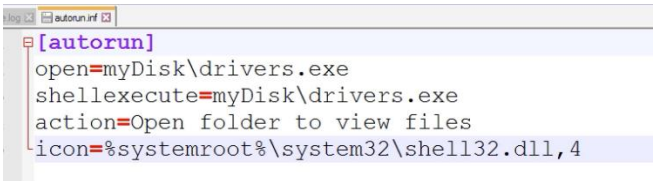

Figura 4.14 *Fișier autorun.inf generat de ransomware pentru executare automată.*

Al doilea mecanism de propagare, ilustrat în Figura 4.15, folosește fișiere de tip .LNK [140] sau scurtătură pentru a fi executat. Atunci când un alt utilizator va accesa acest fișier se va executa o comandă pentru lansarea în execuție a virusului.

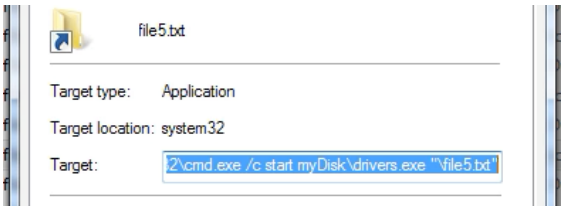

Figura 4.15 *Fișier de tip shortcut utilizat pentru executarea ransomware.*

4.4 Soluție honeypot pentru detecția ransomware

Am propus o soluție de detecție [144] concepută pentru a detecta atacurile ransomware care se răspândesc printr-o rețea de calculatoare. Această platformă va găzdui documente și date fără valoare, înșelând virușii ransomware pentru a le infecta și a crea oportunitatea pentru analiști să investigheze infecția. Soluția, ilustrată în Figura 4.18, este compusă din biblioteci și servicii standard care pot emula servicii de partajare a fișierelor.

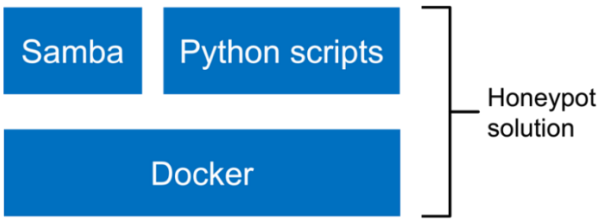

Figura 4.18 *Platforma hardware și software pentru soluția honeypot.*

Pentru a asigura un strat de protecție suplimentară împotriva fișierelor infectate și a posibilelor mostre de malware, întreaga soluție va fi implementată într-un container folosind tehnologia Docker. Într-un container vor exista două module pentru a implementa soluția: serviciul Samba [147], și un set de script-uri dezvoltate folosind limbajul de programare Python, care codifică logica pentru detectarea infecțiilor ransomware. Serviciul Samba a fost configurat prin activarea modulului VFS Full Audit [148] pentru a înregistra operațiunile efectuate asupra fișierelor partajate.

Mecanismul de detecție a infecției cu ransomware este implementat într-un program scris în limbajul de programare Python, care gestionează toată logica de detecție. Unul dintre conceptele importante este utilizarea fișierelor de tip „decoy”, cu scopul de a fi sacrificate în cazul unei infecții cu ransomware. Pentru detectarea infectărilor cu ransomware, programul de detecție va utiliza informații atât din fișierele „decoy” care vor fi stocate și partajate prin intermediul serviciul Samba, cât și din log-urile care conțin operațiuni de acces la fișiere (Figura 4.20). La inițializare programul va genera o serie de fișiere „decoy” împreună cu valorile hash ale acestora.

Acestea din urmă sunt necesare pentru a verifica integritatea fișierelor; atunci când conținutul unui fișier este modificat, generarea valorii hash va produce o altă valoare.

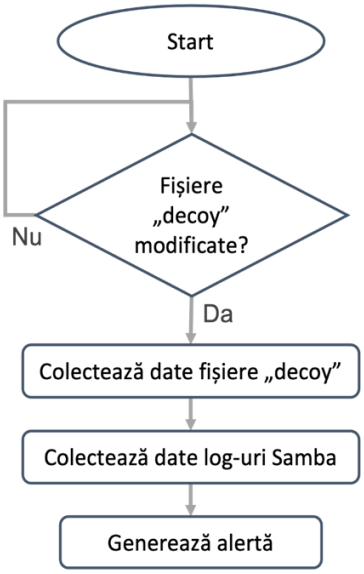

Figura 4.20 *Schema logică a modelului de detecție ransomware.*

Programul va monitoriza periodic atât existența acestor fișiere „decoy", cât și integritatea lor. În momentul când acestea au fost șterse sau modificate, atunci încep o serie de tehnici de detecție. Programul va scana extensii comune utilizate de virușii ransomware. În cazul în care fișierele „decoy" au fost modificate, se continuă cu analiza log-urilor, urmând a fi identificat utilizatorul și adresa IP a sistemului care a fost conectat la serviciul Samba și a efectuat aceste acțiuni. În acest fel poate fi identificat și pacientul 0.

Am efectuat un set de teste pentru a mă asigura că soluția finală poate detecta etapa de infectare a unui ransomware Stampado, analizat pe larg în capitolul 4.3. Figura 4.21 ilustrează alerta generată după infectarea cu ransomware și prezintă aspectele importante: unul din fișierele de tip „decoy" a fost șters, ceea ce a inițiat analiza automată a log-urilor Samba unde extensia „.locked" a fost identificată și inclusiv pacientul 0, utilizatorul și adresa IP a mașinii virtuale de la care a provenit infectarea.

```
Ransomware Alert!
------------------------------------------------
[!] Decoy file removed: file7.txt
[!] Ransomware extension detected: *.locked
[!] Patient 0: win7-victim (192.168.55.128) @ 08:19:39
```

Figura 4.21 *Alertă detectare ransomware.*

Am continuat prin analiza log-urilor pentru a verifica corectitudinea informațiilor din alerta generată. În Figura 4.22 am identificat atât modificarea fișierelor de tip „decoy", cât și generarea de fișiere cu extensia „.locked", care este o extensie folosită de virusul Stampado.

```
08:19:39 : win7-victim|192.168.55.128|RShare|pwrite|ok|Mallory/5B294E575745FABD9D192F2E96BB8FF8685F.locked
08:19:39 : win7-victim|192.168.55.128|RShare|pwrite|ok|Mallory/file7.txt
08:19:39 : message repeated 2 times: [ win7-victim|192.168.55.128|RShare|pwrite|ok|Mallory/file7.txt]
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/file7.txt|Mallory/~hfspbvz.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~hfspbvz.tmp|Mallory/~mrzdacr.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~mrzdacr.tmp|Mallory/~nfsjixz.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~nfsjixz.tmp|Mallory/~apgkvzm.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~apgkvzm.tmp|Mallory/~jrxvjqx.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~jrxvjqx.tmp|Mallory/~ijgqnmo.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~ijgqnmo.tmp|Mallory/~kurlkkc.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~kurlkkc.tmp|Mallory/~vtzopio.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~vtzopio.tmp|Mallory/~hyldufk.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|rename|ok|Mallory/~hyldufk.tmp|Mallory/~wtlokvs.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|unlink|ok|Mallory/~wtlokvs.tmp
08:19:39 : win7-victim|192.168.55.128|RShare|pwrite|ok|Mallory/5B294E575745FABD9D1F2F2E96BB8FF8685F.locked
```

Figura 4.22 *Detectarea fișierelor .locked.*

Un alt aspect identificat pe baza log-urilor înregistrate în timpul infecției este volumul mare de evenimente generate într-o perioadă de timp foarte scurtă, așa cum este ilustrat în Figura 4.24. În Python am utilizat biblioteca Matplotlib [150] pentru a genera o diagramă, așa cum se poate observa în Figura 4.24 (codul conceput este prezentat în detaliu în Anexa tezei de doctorat) pe baza căreia un analist de securitate poate interpreta aceste date vizual pentru a stabili că există o anomalie și poate iniția o investigație mai amănunțită.

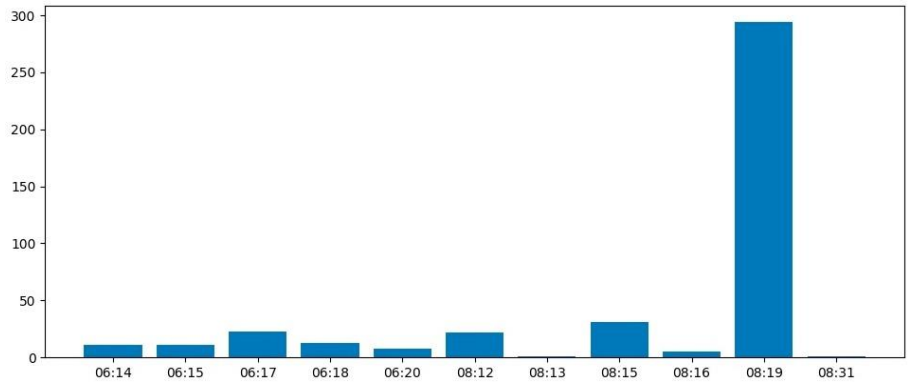

Figura 4.24 *Volum mare de evenimente la un anumit interval.*

4.6 Aplicarea algoritmilor IA în domeniul securității cibernetice

Am efectuat experimente pentru testarea fiabilității acestor algoritmi observând că soluțiile propuse în articolele științifice produc rezultate favorabile doar în contextul setului de date pe care au fost antrenate și tipului de detecție pe care îl implementează. Orice variație a tehnicilor de atac utilizate va conduce la un scor de detecție redus. Aceste concluzii sunt susținute de către alți experți în domeniu, precum G. Apruzzese și M. Colajanni, care au efectuat o analiză a tehnicilor de învățare automată aplicate la detectarea breșelor de securitate, aplicațiilor malware și mesajelor spam [175]. Analiza efectuată de aceștia a avut două obiective: primul a fost evaluarea maturității actuale a

soluțiilor de detecție ce au la bază algoritmi de învățare automată. Rezultatele obținute oferă dovezi că tehnicile actuale de învățare automată au limitări care le reduc eficiența pentru securitatea cibernetică. Toate abordările necesită reantrenare continuă și reglare atentă a parametrilor și nu pot fi automatizate atunci când sunt utilizate tehnici diferite de atac.

În Figura 4.26 am ilustrat procesul tradițional de detecție, în care capabilitățile și soluțiile de detectare a atacurilor pe bază de reguli sunt utilizate pentru a clasifica un volum mare de evenimente, urmând ca un analist de securitate să inspecteze și să analizeze aceste alerte pentru stabilirea existenței unui atac cibernetic. Ca obiectiv principal am propus utilizarea tehnicilor din domeniul inteligenței artificiale ca o capabilitate intermediară pentru a complementa capabilitățile existente de detecție și de a automatiza parțial sau total sarcinile de analiză ale specialistului în domeniu.

Pornind de la lucrarea publicată de Zadeh [176], am identificat caracteristicile pe care trebuie să le îndeplinească un sistem pentru a fi considerat inteligent și anume: capabilitatea de a raționa pe baza cunoștințelor acumulate în baza de date și capacitatea de a lua decizii în condiții de incertitudine. În baza acestor caracteristici am propus o serie de soluții care au rolul de a ajuta un analist de securitate în sarcinile sale de a investiga incidente și a efectua analiza aplicațiilor malware în etape diferite din cadrul unui atac cibernetic.

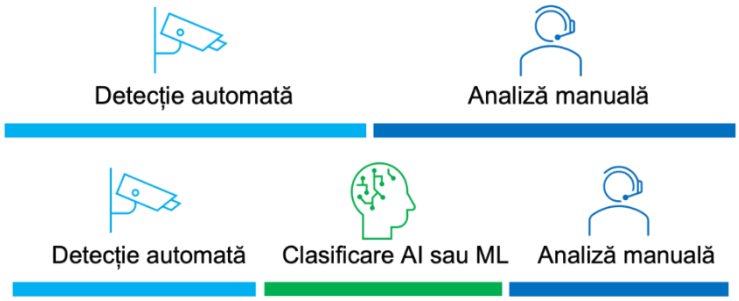

Figura 4.26 *Implementarea tehnicilor inteligenței artificiale în fluxul de lucru. (a) Proces tradițional de detecție și analiză; (b) Proces modern de detecție și analiză*

4.7 Analiza malware dinamică folosind rețele neuronale

În acest capitol am propus o soluție de analiză dinamică malware ce utilizează o rețea neuronală pentru a identifica modele specifice în care malware-ul va folosi programe și utilitare legitime pentru a se instala singur într-un mod autonom. Aceste modele se bazează pe istoricul executării procesului. Sistemul de analiză comportamentală este compus din patru module (Figura 4.27), iar rolul lor este de a colecta și a procesa datele, iar ulterior acestea vor fi trimise către rețeaua neuronală artificială pentru clasificare. Pentru sarcina de a culege informații despre procesele nou create, precum și sursa lansării în execuție a acestora, într-un sistem informatic am folosit programul Sysmon.

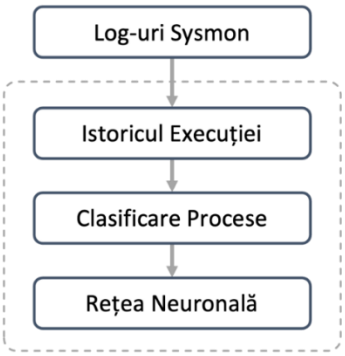

Figura 4.27 *Componentele soluției de analiză.*

Al doilea modul va prelucra evenimentele generate de Sysmon atunci când un proces este lansat în execuție și va genera istoricul execuției (Figura 4.28).

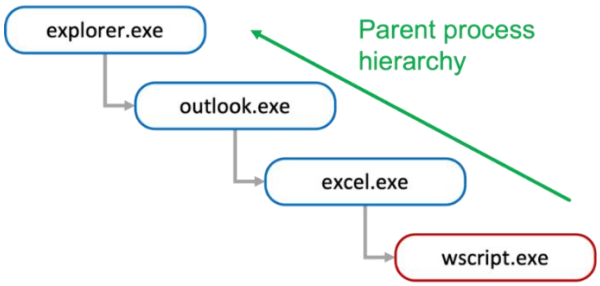

Figura 4.28 *Ierarhia proceselor în execuție [179].*

Clasificarea proceselor se realizează prin intermediul unui codificator care va primi ca intrare toate cele cinci nume de procese din modulul anterior. Scopul acestui modul este de a atribui un coeficient de risc în funcție de tipul de proces, iar în acest sens a fost creat Tabelul 4.9, care conține valorile asociate acestor coeficienți de risc.

Tabelul 4.9 *Clasificarea proceselor [179].*

Categorie	Proces	Valoare
Necunoscut	Necunoscut	0
OS (1-3)	Explorer.exe	1
	Svchost.exe	2
	noparent	1
Scripting (4-6)	Cscript.exe	3
	Wscript.exe	3
	Powershell.exe	3
	Cmd.exe	4
Utilizator (7-9)	Winword.exe	7
	Excel.exe	7
	Notepad.exe	8
	Calc.exe	9
	Iexplore.exe	7
	Outlook.exe	7

Pentru ca rețeaua neuronală artificială să interpreteze datele și să le dea sens, valorile numerice trebuie să fie trimise ca intrări. Toate informațiile necesare sunt deja disponibile, lucru care permite utilizarea rețelelor de tip *feed forward*. Rețeaua neuronală ilustrată în Figura 4.29 este folosită pentru a recunoaște diferitele modele detectate și procesate de modulele anterioare pentru a stabili dacă execuția unui proces face parte din una din următoarele trei categorii: *Legitim, Suspect* sau *Virus*.

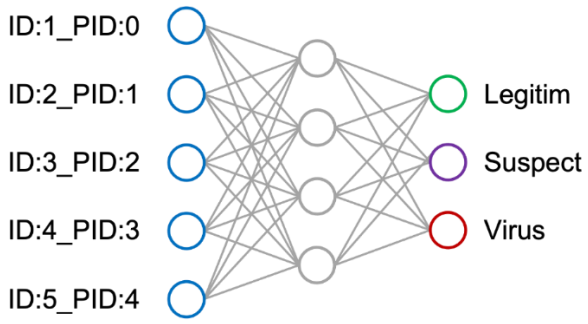

Figura 4.29 *Structura rețelei neuronale.*

Pentru a antrena rețeaua neuronală am folosit un algoritm de învățare supervizat deoarece sunt cunoscute atât datele curente, cât și capacitățile de detectare dorite, creând modele pentru antrenament și testare. În ceea ce privește algoritmul în sine, am optat pentru folosirea backpropagation [185], acesta fiind un algoritm foarte popular pentru antrenarea rețelelor neuronale de tip feed-forward, cu o rată de eficiență ridicată.

4.7.6 Model de date

Am creat trei modele de execuție malware, ilustrate în Figura 4.30, valorile numerice atribuite proceselor fiind corespunzătoare cu cele din Tabelul 4.9. Pentru aceste modele se poate observa cum toate procesele inițiale fac parte din categoria celor de sistem (OS), urmând apoi să fie lansate procese din categoria celor executate de utilizator, iar în cazul documentelor infectate acestea vor invoca și executa procese din categoria celor de scripting.

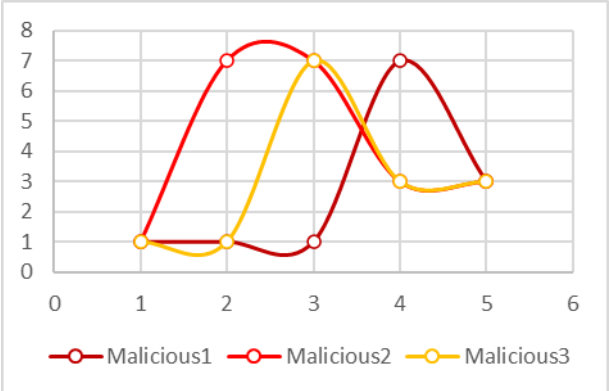

Figura 4.30 *Reprezentarea numerică a virușilor.*

Beneficiul real al rețelelor neuronale artificiale este capacitatea de a clasifica comportamentul pe baza diferitelor modele. Pentru ca aplicația să fie eficientă și să poată distinge atât comportamentul malware, cât și cel legitim, am generat modelele de comportament normal pentru a antrena rețeaua neuronală (Figura 4.31).

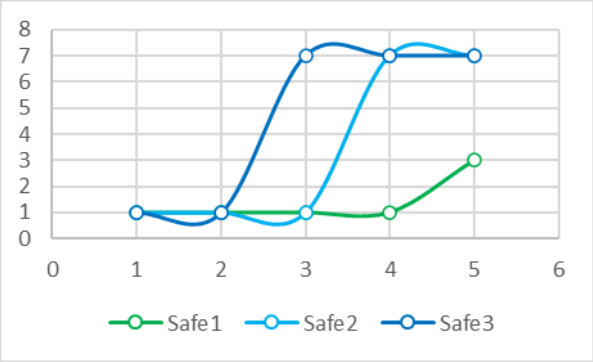

Figura 4.31 *Reprezentarea numerică a proceselor legitime.*

Atunci când toate procesele din ierarhie fac parte din categoria celor de sistem sau când procesele din categoria utilizator nu execută alte procese precum cele din categoria scripting, aceste modele vor descrie *activitatea legitimă*. Scopul principal al modelării datelor este de a identifica virușii informatici care sunt livrați prin intermediul documentelor Office sau PDF și care încearcă să ruleze scripturi rău intenționate prin pornirea proceselor din categoria scripting.

Pe de altă parte, rularea proceselor de scripting (precum powershell.exe sau prompt-ul de comandă din sistemul de operare) este considerată activitate legitimă. Același comportament normal este luat în considerare atunci când rulează programe din categoria utilizator executate din același context de sistemul de operare.

În concluzie, folosind modelele furnizate pentru a antrena rețeaua, rezultatul a avut succes și rețeaua neuronală artificială reușește să conveargă. Într-un mediu de test, la executarea unui document infectat cu malware acesta a fost detectat cu succes, deoarece ierarhia proceselor este similară cu cele a modelelor pe baza căreia rețeaua neuronală a fost antrenată. Succesul acestei tehnici la scară mică crește interesul pentru cercetări mult mai profunde în domeniu.

Pornind de la conceptul de aplicare a algoritmilor de învățare automată la analiza comportamentală a virușilor informatici, se poate concluziona că una dintre provocări este de a modela datele produse de instrumentele de monitorizare a securității în modele reprezentate numeric. Acestea pot fi învățate de o rețea neuronală artificială cu scopul final de a clasifica o mare varietate de evenimente de securitate pentru a preveni viitoare infectări cu viruși informatici și alte aplicații malware.

Capitolul 5

Concluzii

În acest capitol am făcut o sinteză referitoare la principalele aspecte prezentate în cadrul tezei. Am evidențiat rezultatele obținute, contribuțiile originale și lista lucrărilor publicate pe parcursul stagiului de doctorat. Datorită faptului că amenințările cibernetice sunt într-o continuă evoluție din punct de vedere tehnic, am identificat câteva direcții de dezvoltare și îmbunătățire a soluțiilor prezentate în această lucrare.

5.1 Rezultate obținute

Unul din obiectivele principale ale tezei de doctorat a constat în identificarea metodelor de detecție și analiză a atacurilor și virușilor cibernetici la care se pot aplica tehnici din domeniul inteligenței artificiale. Algoritmii specifici rețelelor neuronale au fost și sunt aplicați cu succes pentru probleme de clasificare. În cadrul tezei de doctorat am analizat și implementat o serie de soluții ce au la bază principiile fundamentale ale sistemelor inteligente cu scopul de a îmbunătăți eficiența acestora în ceea ce privește detecția malware și a reduce timpul de analiză.

În **Capitolul 2** am evidențiat aspectele cele mai importante ale securității informațiilor precum confidențialitatea, integritatea și disponibilitatea datelor. Pe baza acestora am definit amenințarea cibernetică ca orice acțiune care afectează componentele securității informațiilor. Am efectuat o analiză amănunțită a riscurilor și amenințărilor cibernetice pe baza incidentelor și breșelor de securitate care au avut loc în ultimul deceniu și au fost documentate în spațiul public.

Am continuat prin a face un studiu asupra impactului pe care aceste breșe de securitate l-au avut asupra utilizatorilor, cum ar fi furtul datelor cu caracter personal și asupra organizațiilor, unde datorită fenomenului de digitalizare (care presupune că organizațiile folosesc intens sisteme de calcul și soluții informatice), incidentele de securitate pot reduce sau chiar opri activitățile de zi cu zi, ce se pot asocia cu un impact financiar aferent.

Pentru a adresa amenințările cibernetice într-un mod corespunzător în care impactul este minim, am efectuat o analiză asupra metodologiilor existente precum MITRE ATT&CK Framework și Lockheed Martin Cyber Kill Chain care propun metode de detecție și analiză a atacurilor și virușilor informatici.

Capitolul 3 se axează pe detecția și analiza atacurilor cibernetice pornind de la un studiu asupra capabilităților de securitate existente. Aceste sunt clasificate în două mari categorii: o primă categorie o reprezintă capabilitățile de detecție la nivel de rețea - precum sistemele de detecție și prevenție a intruziunilor (Intrusion Detection System - IDS, Intrusion Prevention System - IPS). Cea de-a doua categorie a capabilităților de detecție este la nivel de sistem de calcul, precum programe antivirus sau sisteme de colectare a evenimentelor (Endpoint Detection and Response - EDR).

Am continuat prin a analiza eficiența acestor capabilități de detecție, dar și limitările acestora. Cel mai important aspect este că regulile și indicatorii utilizați pot detecta virușii care sunt deja cunoscuți și analizați. Orice amenințare care creează și utilizează noi viruși nu poate fi detectată decât după analiza malware în urma căreia noi reguli pot fi generate. Printr-un studiu detaliat al amenințărilor am evidențiat că atacurile cibernetice încep să abuzeze programe și utilitare legitime care există deja într-un sistem de calcul pentru a facilita o infectare și a putea menține controlul asupra unui sistem de calcul de la distanță. Pe baza acestui studiu am creat un mediu de analiză folosind tehnologii open-source pentru a colecta o gamă mult mai largă de evenimente la nivel de rețea, fapt care a facilitat detectarea de anomalii ce pot identifica indicatori ai unui atac cibernetic.

Capitolul 4 abordează obiectivul principal regăsit și în titlul tezei de doctorat și anume identificarea și implementarea de algoritmi din domeniul inteligenței artificiale pentru a îmbunătăți eficiența capabilităților de detecție a atacurilor cibernetice și a reduce timpul și resursele necesare analizei malware.

Am efectuat un studiu amănunțit asupra capabilităților existente ce folosesc euristici și algoritmi din domeniul inteligenței artificiale și am identificat trei subdomenii de aplicare:

- Mesaje de spam și phishing;
- Detectarea intruziunilor și a sistemelor compromise;
- Clasificarea malware de tip polimorf și metamorfic în funcție de familie.

Pe baza acestui studiu am generalizat și am identificat trei mari categorii în care algoritmii din domeniul inteligenței artificiale pot fi aplicați. Prima categorie poartă numele de etapa de pre-compromitere, în care adversarii cibernetici folosesc o serie de tehnici pentru a putea iniția un atac și a infecta un sistem de calcul sau o rețea de sisteme de calcul. În a doua etapă, etapa infectare, una sau mai multe componente malware sunt instalate și prin intermediul cărora un adversar cibernetic va obține acces și control neautorizat asupra unuia sau mai multor sisteme de calcul. În etapa post-compromitere, adversarul cibernetic, pe baza accesului obținut, va executa o serie de acțiuni prin care va dori să își consolideze poziția prin instalarea de tehnici de persistență și să evite detecția. Tot în această etapă adversarul poate exfiltra informații și infecta alte sisteme din rețea.

La nivelul etapei de pre-compromitere am efectuat un studiu asupra tehnicilor de phishing utilizate și am analizat în detaliu scenariul în care pagini web legitime sunt clonate și găzduite pentru a induce utilizatori în eroare și a îi face pe aceștia să introducă detalii de autentificare precum nume de utilizator, parolă, dar și coduri asociate cu

autentificarea multi-factor. Am dezvoltat și implementat un algoritm de detectare al paginilor de phishing pe baza similitudinilor dintre pagina originală și pagina de phishing pe baza similitudinilor la nivel de adresă web, dar și pe baza analizei similitudinilor la nivel de conținut. Pentru testarea eficienței soluției propuse am folosit o serie de unelte precum SET (Social-Engineer Toolkit) pentru a genera website-uri de phishing pe baza celor legitime.

În cadrul etapei de infectare am efectuat un studiu asupra detectării malware pe baza relației de părinte-fiu la nivel de proces de execuție. Pe baza acestuia am propus o soluție ce utilizează rețele neuronale artificiale pentru a identifica procese ce sunt folosite în scop malițios incluzând procese legitime. Pentru antrenarea rețelei am folosit indicatori extrași din investigații precedente, iar pentru testare am folosit o serie de unelte într-un mediu izolat pentru a testa eficiența soluției propuse.

Pentru etapa post-compromitere am analizat un malware de tip ransomware din familia Stampado. În urma analizei am descoperit doi indicatori de compromitere prin care infecția se poate răspândi și la alte calculatoare din rețea. Pentru detectarea într-o rețea de calculatoare a infectării cu viruși de tip ransomware am dezvoltat și implementat o soluție de tip honeypot bazată pe un serviciu de partajare de fișiere la care se pot conecta toate sistemele de calcul dintr-o rețea. Modul de detecție se bazează pe faptul că în momentul infecției cu ransomware, fișiere de tip „decoy” sunt monitorizate continuu, și orice modificare a acestora a declanșa o alertă.

Rezultatele obținute în urma cercetărilor doctorale au fost diseminate în cadrul unor serii de activități desfășurate într-un mediu profesional și consider că au contribuit la creșterea gradului de conștientizare privind implementarea securității cibernetice în mediul organizațional. Printre aceste activități pot să enumăr:

- facilitarea unor simulări de incidente pentru identificarea deficiențelor la nivel de proces, dar și de formare a echipei ce răspunde la incidente de securitate;
- elaborarea unor cursuri și chestionare pentru dezvoltarea capabilităților de analiză malware;
- dezvoltarea de cursuri în domeniul IoT și al tehnologiilor specifice;
- conceperea unor cursuri la nivel global, cu un număr de circa 27.000 de vizitatori și o medie de peste 5.000 de cursanți în ultimii 5 ani (2017 - 2021). Printre cursurile susținute amintesc: *Threat Intelligence: The Big Picture*, *Getting Started Analyzing Malware Infections*, *Threat Hunting with Yara*, *Advanced Malware Analysis: Ransomware*.

5.2 Contribuții originale

În continuare prezint lista integrală a contribuțiilor originale din lucrare. Acestea au fost obținute în urma simulărilor, experimentelor și implementărilor efective fie direct în mediul online sau organizațional (pentru contribuțiile eligibile), fie folosind mașini virtuale și medii de test izolate (pentru contribuțiile cu impact potențial malițios).

1. Am propus o soluție de detectare a paginilor web de phishing **[A1]** bazată pe analiza similitudinilor dintre pagina originală și cea falsă. Pe baza unui studiu al atributelor specifice dintre pagina de phishing și cea originală am extras un set specific ce facilitează detecția cu succes a paginilor clonate.
2. Am implementat o soluție de detectare a virușilor de tip ransomware bazată pe tehnologii de tip honeypot **[A2]** în care, pe baza unui serviciu de partajare a fișierelor, am creat un program care monitorizează continuu integritatea fișierelor și poate genera alerte atunci când integritatea a fost compromisă. Soluția poate identifica de asemenea și „pacientul 0", adică primul sistem care a inițiat infectarea.
3. Am propus o soluție pentru analiza malware dinamică utilizând rețele neuronale **[A3]**, soluție care se bazează pe clasificarea proceselor în categorii specifice. Detecția se efectuează pe baza analizei anomaliilor din ierarhia de execuție pentru fiecare proces **[D1]**. Clasificarea proceselor în categorii face posibilă îmbunătățirea și modificarea listei de procese fără a fi necesară reantrenarea rețelei neuronale.
4. Am analizat static și dinamic un tip de virus ransomware - Stampado **[B7]** - și am extras indicatorii de compromitere, dar și comportamentul acestora în legătură cu răspândirea infectării într-o rețea de calculatoare prin servicii de partajare a fișierelor.
5. Am analizat și sintetizat aplicarea tehnicilor de IA în contextul detecției atacurilor cibernetice identificând trei categorii majore: detectarea intruziunilor la nivel de rețea, detectarea malware și spam/phishing.
6. Am realizat un studiu privind bibliotecile SSL pentru dispozitive IoT **[B5] [B6]**. Am identificat o vulnerabilitate la nivelul bibliotecilor SSL, cauzată de lipsa implementării protocoalelor CLR și OCSP utilizate pentru validarea certificatelor de criptare expirate sau compromise. O altă vulnerabilitate identificată a constat în lipsa actualizării și menținerii bibliotecilor pentru platforma hardware studiată.
7. Am efectuat un studiu asupra capabilităților și tehnicilor de detecție și analiză a virușilor informatici la nivel de sistem și la nivel de rețea. Am analizat comparativ abordarea detecției atacurilor cibernetice între două paradigme, cea orientată pe vulnerabilitate (care presupune că o organizație va lua măsuri după ce un incident de securitate s-a derulat) și apărarea orientată pe amenințare, ce presupune abordarea proactivă în care o organizație va lua măsuri de prevenție înainte ca un incident să se producă.
8. În contextul măsurilor pe care o organizație trebuie să le ia la apariția unui incident (fizic sau logic) care conduce la un efect critic (nefuncționare / lipsa furnizării unui serviciu), am contribuit la elaborarea unei analize Fault Tree Analysis (FTA) **[A4]** pentru a evalua cauzele care pot defecta un server Web ținând cont de aspecte la nivel hardware și software.
9. Am propus o arhitectură de referință bazată pe tehnologii open-source pentru un mediu izolat de simulare a atacurilor cibernetice, testare a tehnicilor și a mecanismelor de detecție. Acest mediu a fost utilizat la generarea datelor pentru antrenarea algoritmilor de detecție bazați pe tehnici din domeniul IA.
10. Am realizat un studiu asupra provocărilor legate de securizarea sistemelor de calcul. Pe baza rapoartelor și sondajelor efectuate de organizații din domeniul securității

cibernetice am identificat factorii importanți care stau la baza provocărilor legate de securizarea sistemelor de calcul. Printre acestea se numără: lipsa analiștilor și a experților în domeniul securității informației, precum și creșterea atât a volumului, cât și a complexității atacurilor cibernetice.

11. Am elaborat un studiu asupra metodologiilor de detectare și analiză a atacurilor cibernetice complexe **[D2]** și am propus utilizarea noilor metodologii pentru abordarea atacurilor: din punctul de vedere al Kill Chain, abordarea atacurilor ca o serie consecutivă de stagii, iar din punctul de vedere al MITRE, clasificarea pe baza tehnicilor utilizate, nu numai a tipului sau familiei de viruși informatici folosiți.

12. Am efectuat o analiză a atacurilor cibernetice care au avut un impact major **[B4]** atât asupra organizațiilor care au fost victime, cât și asupra cetățenilor de rând care utilizează serviciile acestor organizații **[D4]**. Am analizat impactul acestora precum și cauza inițială a breșelor de securitate pe baza rapoartelor publicate de experți în domeniu.

13. Am definit și implementat un plan de simulare a atacurilor cibernetice într-o organizație, ce a avut ca scop îmbunătățirea nivelului de pregătire al analiștilor din cadrul departamentului de securitate cibernetică și capacitatea acestora de a detecta și analiza atacuri cibernetice moderne. Ca relevanță am propus simularea de incidente ca urmare a unui atac cu virus de tip ransomware **[D3]**. Unele exerciții au avut la bază evaluarea capacității de restaurare a serviciilor critice precum Active Directory.

14. Am contribuit la un studiu comparativ **[B8]** în ceea ce privește organizarea în cadrul unui departament de securitate. Mai precis am evaluat rolurile analiștilor **[B9]** în cadru SOC (Security Operations Center) și cum migrarea la SIC (Security Intelligence Center) aduce beneficii în ceea ce privește modul și eficiența în combaterea atacurilor cibernetice.

15. Pe baza caracteristicilor comportamentale ale virușilor informatici am creat în scop educațional astfel de aplicații malware folosind tehnologii pentru simularea atacurilor cibernetice atât pentru platformele Windows, cât și Linux. Aceasta a facilitat simularea de atacuri în vederea testării capabilităților de detecție și analiză.

16. Am propus metode de detecție a atacurilor la nivel de rețea pe baza prelucrării statistice a traficului dintr-o rețea de calculatoare **[D1]**. Pe baza acestor metode am identificat atât atacuri volumetrice de epuizare a resurselor de tip DoS, furtul de date prin intermediul tunelelor DNS, precum și identificarea de site-uri de phishing.

17. Am efectuat o analiză comparativă a metodelor de detecție malware la nivel de sistem: pe bază de semnături hash, pe bază de reguli Yara **[D5]** și pe baza evenimentelor înregistrate la nivel de sistem de operare. Am elaborat asupra metodelor de detecție a persistenței malware pe un sistem și am finalizat prin detecția malware pe baza corelării evenimentelor înregistrate la nivel de sistem cu evenimentele corespunzătoare la nivel de rețea.

18. Am propus **[A2] [B1] [B2]** și am contribuit **[A5]** la soluții de detectare a atacurilor cibernetice bazate pe platforme IoT **[B3]** ca alternative tactice sau complementare la soluțiile hardware sau cloud strategice.

5.3 Lista lucrărilor publicate

A. Articole științifice în publicații indexate ISI / IEEE Xplore

[A1] C. Pascariu, I.C. Bacivarov, *Detecting Phishing Websites Through Domain and Content Analysis*, 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitești, România, 2021, eISBN: 978-1-6654-2534-6, DOI: 10.1109/ECAI52376.2021.9515165.

[A2] C. Pascariu, I.D. Barbu, *Ransomware Honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family*, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitești, România, 2019, eISBN: 978-1-7281-1624-2, DOI: 10.1109/ECAI46879.2019.9042158, WOS: 000569985400166.

[A3] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Dynamic analysis of malware using Artificial Neural Networks. Applying Machine Learning to identify malicious behavior based on parent process hierarchy*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, România, 2017, eISBN: 978-1-5090-6458-8, DOI: 10.1109/ECAI.2017.8166505, WOS: 000425865900121.

[A4] G. Petrică, I.D. Barbu, S.D. Axinte, **C. Pascariu**, *Reliability analysis of a Web server by FTA method*, The 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, 2017, pp. 683-686, DOI: 10.1109/ATEE.2017.7905101, WOS: 000403399400133.

[A5] I.D. Barbu, **C. Pascariu**, I.C. Bacivarov, S.D. Axinte, M. Firoiu, *Intruder monitoring system for local networks using Python*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, România, 2017, eISBN: 978-1-5090-6458-8, DOI: 10.1109/ECAI.2017.8166457, WOS: 000425865900073.

B. Articole științifice în publicații indexate BDI

[B1] C. Pascariu, *Getting Started with Vulnerability Disclosure and Bug Bounty Programs*, International Journal of Information Security and Cybercrime (IJISC), Vol. 11, No. 1, 2022, pp. 25-30, ISSN: 2285-9225, DOI: 10.19107/IJISC.2022.01.03.

[B2] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Network security monitoring with embedded platforms*, Proc. of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN: 1842-3566.

[B3] C. Pascariu, I.D. Barbu, *Using Embedded Platforms to Monitor Network Security*; International Journal of Information Security and Cybercrime (IJISC), Vol. 7, No. 2, 2018, pp. 9-13, ISSN: 2285-9225, DOI: 10.19107/IJISC.2018.02.01.

[B4] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Investigative Analysis and Technical Overview of Ransomware Based Attacks. Case Study: WannaCry*, International Journal of Information Security and Cybercrime (IJISC), Vol. 6, No. 1, 2017, pp. 57-62, ISSN: 2285-9225, DOI: 10.19107/IJISC.2017.01.06.

[B5] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *WannaCry ransomware analysis. 1 day, 150 countries, >57k infected computers*, Asigurarea Calității - Quality Assurance, Vol. XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410.
[B6] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Secure Smart Cities*, Proceedings of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 161-166, ISSN 1842-3566.
[B7] C. Pascariu, I.D. Barbu, *Ransomware - an emerging threat*, International Journal of Information Security and Cybercrime (IJISC), Vol. 4, No. 2, 2015, pp. 27-32, ISSN: 2285-9225, DOI: 10.19107/IJISC.2015.02.03.
[B8] I.D. Barbu, **C. Pascariu**, I.C. Bacivarov, *Migration of a SOC to SIC. Security Operations Center vs. Security Intelligence Center. The use of honeypots for threat intelligence*, Proc. of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 150-155, ISSN 1842-3566.
[B9] I.D. Barbu, **C. Pascariu**, *Information security analyst profile*, International Journal of Information Security and Cybercrime (IJISC), Vol. 3, No. 1, 2014, pp. 29-36, ISSN: 2285-9225, DOI: 10.19107/IJISC.2014.01.03.

C. Prezentări în conferințe de specialitate

[C1] C. Pascariu, *Crowdsourcing Information Security*, Digital 2021 ISF World Congress, eveniment online.
[C2] C. Pascariu, *Adversary Emulation: Building your Purple Team*, ISF Congress 2020, eveniment online.
[C3] C. Pascariu, *Cyber Deception: Hunting for Ransomware*, ISF Congress 2019, Dublin, Irlanda.

D. Rapoarte științifice în cadrul programului de doctorat

[D1] C. Pascariu, *Prelucrarea statistică a evenimentelor de securitate*, Raport științific nr. 1, iunie 2016.
[D2] C. Pascariu, *Detectarea atacurilor cibernetice la nivel de rețea*, Raport științific nr. 2, decembrie 2016.
[D3] C. Pascariu, *Analiza virușilor de tip ransomware*, Raport științific nr. 3, iunie 2017.
[D4] C. Pascariu, *Analiza riscurilor și securizarea orașelor inteligente (Smart Cities)*, Raport științific nr. 4, decembrie 2017.
[D5] C. Pascariu, *Analiza și clasificarea virușilor cibernetici folosind reguli Yara*, Raport științific nr. 5, iunie 2018.

Bibliografie

[1] V.M. Cătuneanu, I.C. Bacivarov, *Fiabilitatea sistemelor de telecomunicații*, Ed. Militară, București, 1985.

[3] Gartner Glossary, Digitalization, https://www.gartner.com/en/information-technology/glossary/digitalization#:~:text=Digitalization%20is%20the%20use%20of,roadmap%20for%20digital%20business%20transformation.

[4] ISO, ISO/IEC 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary, https://www.iso.org/standard/73906.html.

[5] ISO, ISO/IEC 27000:2018(en), https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en.

[16] ENISA Thread Landscape report - 2021, https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends.

[34] C. Pascariu, *Analiza riscurilor și securizarea orașelor inteligente (Smart Cities)*, Raport științific nr. 4, decembrie 2017.

[44] RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, https://www.ietf.org/rfc/rfc5280.txt.

[45] R. Sanders, *What is a Certificate Revocation List (CRL) vs OCSP?*, https://www.keyfactor.com/blog/what-is-a-certificate-revocation-list-crl-vs-ocsp/.

[46] Adafruit WICED WiFi Feather - STM32F205 with Cypress WICED WiFi - Discontinued, https://www.adafruit.com/product/3056.

[47] Github, Adafruit WICED Feather Arduino BSP, https://github.com/adafruit/Adafruit_WICED_Arduino.

[48] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *WannaCry ransomware analysis. 1 day, 150 countries, >57k infected computers*, Asigurarea Calității - Quality Assurance, Vol. XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410.

[52] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Network security monitoring with embedded platforms*, Proceedings of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN 1842-3566.

[53] I.D. Barbu, C. Pascariu, I.C. Bacivarov, S.D. Axinte, M. Firoiu, *Intruder monitoring system for local networks using Python*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, România, 2017, eISBN: 978-1-5090-6458-8, DOI: 10.1109/ECAI.2017.8166457, WOS: 000425865900073.

[54] C. Pascariu, I.D. Barbu, *Using Embedded Platforms to Monitor Network Security*, International Journal of Information Security and Cybercrime (IJISC), Vol. 7, No. 2, 2018, pp. 9-13, ISSN: 2285-9225, DOI: 10.19107/IJISC.2018.02.01.

[55] Python, https://www.python.org.

[56] Scapy Project, https://scapy.net.

[57] V. Ramachandran, S. Nandi, *Detecting ARP Spoofing: An Active Technique*, Information systems security: first international conference, ICISS 2005, Kolkata, India, December 19-21, 2005, p. 239, ISBN 978-3-540-30706-8.

[72] C. Pascariu, *Getting Started with Vulnerability Disclosure and Bug Bounty Programs*, International Journal of Information Security and Cybercrime (IJISC), Vol. 11, No. 1, 2022, pp. 25-30, ISSN: 2285-9225, DOI: 10.19107/IJISC.2022.01.03.

[83] L. Zeltser, *How to get and set up a free Windows VM for Malware Analysis*, https://zeltser.com/free-malware-analysis-windows-vm/.

[84] VMware Workstation PRO, desktop hypervisor, https://www.vmware.com/nl/products/workstation-pro.html.

[86] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, https://www.kali.org.

[87] Sysmon | System Monitor, https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon.

[90] Osquery | Performant endpoint visibility, https://osquery.io.

[91] Security Onion 2 | Security monitoring and log management, https://securityonionsolutions.com/software.

[92] Zeek (Bro), https://zeek.org.

[93] Elastic Stack, https://www.elastic.co/elastic-stack/.

[94] Elasticsearch, https://www.elastic.co/elasticsearch/.

[95] Kibana, https://www.elastic.co/kibana/.

[97] Beats, https://www.elastic.co/beats/.

[123] C. Pascariu, I.C. Bacivarov, *Detecting Phishing Websites Through Domain and Content Analysis*, 13th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 2021, eISBN: 978-1-6654-2534-6, DOI: 10.1109/ECAI52376.2021.9515165.

[125] Kaspersky, What is Typosquatting? - Definition and Explanation, https://www.kaspersky.com/resource-center/definitions/what-is-typosquatting.

[126] D. O'Regan, *How scammers use sub-domains*, https://easykey.uk/computer-safety/how-scammers-use-sub-domains.

[130] N. Jaiswal, SequenceMatcher in Python, 2019, https://towardsdatascience.com/sequence matcher-in-python-6b1e6f3915fc.

[131] S. Coble, Most Phishing Pages are Short-lived, Infosecurity magazine, 2021, https:// www.infosecurity-magazine.com/news/most-phishing-pages-are-shortlived/.

[132] DNStwist phishing domain scanner, https://dnstwist.it.

[133] The Social-Engineer Toolkit (SET), https://www.trustedsec.com/tools/the-social-engi neer-toolkit-set/.

[139] Microsoft, Using and Configuring Autoplay, https://docs.microsoft.com/en-us/previous-versions/windows/desktop/legacy/cc144212(v=vs.85).

[140] Shell Link | LNK binary file format, https://docs.microsoft.com/en-us/openspecs/ windows_protocols/ms-shllink/16cb4ca1-9339-4d0c-a68d-bf1d6cc0f943.

[144] C. Pascariu, I.D. Barbu, *Ransomware Honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family*, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, Romania, 2019, eISBN: 978-1-7281-1624-2, DOI: 10.1109/ECAI46879.2019.9042158, WOS: 000569985400166.

[147] SMB | Samba sharing service, https://www.samba.org.

[148] Samba VFS Full Audit Config, https://www.samba.org/samba/docs/current/man-html/ vfs_full_audit.8.html.

[150] Matplotlib: Visualization with Python, https://matplotlib.org.

[175] G. Apruzzese, M. Colajanni, *On the effectiveness of Machine and Deep Learning for Cyber Security*, NATO CCD COE Publications, Tallinn, 2018.

[176] L.A. Zadeh, *Fuzzy logic, neural networks, and soft computing*, Commun. ACM 37, 3, 1994, 77-84, DOI: 10.1145/175247.175255.

[179] C. Pascariu, I.D. Barbu, I.C. Bacivarov, *Dynamic analysis of malware using Artificial Neural Networks. Applying Machine Learning to identify malicious behavior based on parent process hierarchy*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Romania, 2017, eISBN 978-1-5090-6458-8, DOI: 10.1109/ECAI.2017.8166505, WOS: 000425865900121.

[185] D.E. Rumelhard, *Backpropagation: The Basic Theory*, Backpropagation: Theory, Architectures, and Applications, SUA: Library of Congress, 1995, pp. 1-35.