UNIVERSITETI I PRISHTINËS "HASAN PRISHTINA"

Fakulteti i Shkencave Matematike-Natyrore

Departamenti: *Matematikë* | Programi: *Shkenca Kompjuterike*

LËNDA: INTELEGJENCË ARTIFICIALE

Tema: Përdorimi I Inteligjencës Artificiale në sulmet kibernetike

Profesori i lëndës: Eliot Bytyqi

Asistent: Besnik Duriqi

Anëtarët e grupit: Erë Dedinca,
Rreze Vrapcani,
Rubina Berisha

Prishtinë, 2023

Abstrakt

Përparimet e fundit në teknologjitë e inteligjencës artificiale (AI) kanë nxitur rritje të jashtëzakonshme në inovacion dhe automatizim. Historikisht, komuniteti i sigurisë ka përdorur Inteligjencën Artificiale përkatësisht Machine Learning (ML) në një mënyrë mbrojtëse - defanzive, për shembull përmes klasifikimit binar ose gjetjen e trafikut anormal të rrjetit. Edhe tani, startup-et vazhdojnë të shfaqin teknika të reja reklamimi për zbulimin e kërcënimeve hyrëse. Megjithëse këto teknologji të AI-it ofrojnë përfitime të konsiderueshme, ato mund të përdoren për qëllime të dëmshme. Sulmuesit po ndryshojnë vazhdimisht dhe po përmisojnë strategjitë e tyre me theks të veçantë në aplikimin e të ashtuquajturave 'AI-driven techniques' ne procesin e sulmit të quajtur 'AI-driven cyberattack' i cili mund të përdoret në lidhje me teknikat konvencionale të sulmit për të shkaktuar më shumë dëme. Aftësia e algoritmeve të machine learning për të klasifikuar të dhënat e papara më parë dhe për të parashikuar të dhënat e ardhshme do të thotë se ata kanë një gamë të gjerë përdorimesh ne mbrojtjen kibernetike. Sidoqoftë, të njejtat tipare të mësimit mund të përdoren në mënyrë të barabartë në kontekste me qëllim të keq. Andaj çdo herë e më shumë po bëhet edhe përpjekje në drejtim të përdorimit të AI si armë. Në kuadër të këtij punimi seminarik, janë shqyrtuar disa sulme kibernetike të realizuara me AI.

Përmbajtja

Lista e shkurtesave

AI – Artificial Intelligence
ML – Machine Learning
OCR – Optical Character Recognition
DL – Deep Learning
NLP - Natural Language Processing

1. Hyrje

1.1 Hyrje

Për dekada me radhë, organizatat, duke përfshirë agjencitë qeveritare, spitalet dhe institucionet financiare,kanë qenë objektiv i sulmeve kibernetike. Këto sulme kibernetike janë kryer nga hakerë me përvojë që ka përfshirë përpjekje manuale. Vitet e fundit ka pasur një ngritje në zhvillimin e inteligjencës artificiale (AI),e cila ka mundësuar krijimin e mjeteve softuerike që kanë ndihmuar në automatizimin e detyrave të tilla si:

- Parashikimi (prediction),
- Nxjerrja e informacionit (information retrieval) dhe
- Sinteza e mediave (media synthesis)

Gjatë gjithë kësaj periudhe, anëtarët e akademisë dhe industrisë kanë përdorur inteligjencën artificiale (AI)në kontekstin e përmisimit të gjendjes së mbrojtjes kibernetike dhe analizës së kërcënimeve (threat analysis). Megjithatë, AI është gjithashtu gjithnjë e më i dukshëm si një mjet sulmi, ku shpesh referohet si“offensive AI”. AI na ka dhënë mundësinë për të automatizuar detyrat, për të nxjerrë informacion nga sasitë mëdha të të dhënave dhe për të sintetizuar media që janë pothuajse të padallueshme nga ato reale. Megjithatë, mjetet pozitive mund të përdoren edhe për qëllime negative. Pavarësisht disa studimeve mbi AI dhe sigurinë, studiuesit nuk kanë përmbledhur sulmet kibernetike të bazuara në AI mjaftueshëm për të kuptuar veprimet e kundërshtarit dhe për të zhvilluar mbrojtjen e duhur kundër sulmeve të tilla.

Gjatë viteve të fundit, teknologjitë e inteligjencës artificiale (AI) kanë përparuar me shpejtësi të madhe dhepërdorimet e saj janë shtrirë në shumë fusha (domene) të ndryshme. Çdo gjë po shkon në drejtim të së ashtuquajturës teknologji e mençur. AI po kthen vërshimin e të dhënave në informacion të zbatueshëm. Këto teknologji të inteligjencës artificiale janë të dobishme për fushën e sigurisë kibernetike duke mbledhursasi të mëdha të të dhënave dhe më pas duke i filtruar ato për të detektuar paterne (modele) të dëmshme (malicious) dhe sjellje anormale. Prandaj, është

publikuar shumë me fokus në avancimet e AI, por pak vëmendje i është dhënë rreziqeve të AI. Përdorimi me qëllim të keq i AI po ndryshon hapësirën e kërcënimeve të mundshme kundër një game të gjerë aplikacionesh të dobishme. Veçanërisht, përdorimi meqëllim të keq i AI mund të kërcënojë sisteme më komplekse siç janë sistemet inteligjente kibernetike-fizike [1], të cilat nuk janë studiuar tërësisht më parë. Ndikimi i kërcënimeve të mundshme kibernetike është zgjeruar nga përdorimet me qëllim të keq të teknologjive të AI për të mundësuar sulme në shkallë më të gjerë dhe më të fuqishme. Kriminelët kibernetikë kanë filluar të përmirësojnë teknikat e tyre duke përfshirëhakime IoT, malware, ransomware dhe AI për të nisur sulme më të fuqishme. Duke kryer këto lloj sulmesh,të gjithë janë në rrezik për shkak të ndërlidhjes dhe inteligjencës së sulmeve. Nga ky këndvështrim, edhe nëse përparimi i kërkimit mbi aplikimin e AI për t'u mbrojtur kundër sulmeve kibernetike ka filluar tashmëshumë vite më parë [2], ka ende pasiguri se si të mbrohemi kundër përdorimit të AI si një mjet keqdashës.

1.2 Motivimi

Sulmet kibernetike po bëhen gjithnjë e më të sofistikuara dhe të shpeshta. Kriminelët kibernetikë po adoptojnë në mënyrë të pashmangshme teknika të Inteligjencës Artificiale (AI) për të shmangur hapësirënkibernetike dhe për të shkaktuar dëme më të mëdha pa u vënë re. Studiuesit në fushën e sigurisë kibernetikenuk e kanë hulumtuar mjaftueshëm konceptin prapa sulmeve kibernetike të fuqizuara nga AI për të kuptuarnivelin e sofistikimit që posedon ky lloj sulmi. Ky punim seminarik ka për qëllim që në rend të parë të analizoj kërcënimin e shfaqur nga sulmet kibernetike të fuqizuara nga AI, të shqyrtoj ndonjë nga rastet e përdorimit të AI për sulm si dhe të paraqes mënyrat e mbrojtjes duke shfrytëzuar inteligjencën artificiale.

2. Intelegjenca Artificiale

2.1 Ç'është Intelegjenca Artificiale

Sipas John McCarthy, i cili njihet si themeluesi i Inteligjencës Artificiale (AI):
"AI është shkenca dhe inxhinieria e prodhimit të makinave inteligjente, veçanërisht programeve kompjuterike." [3]

AI (Inteligjenca Artificiale) është aftësia e një makine për të kryer funksione njohëse siç bëjnë njerëzit, të tilla si perceptimi, të mësuarit, arsyetimi dhe zgjidhja e problemeve. Qëllimi kryesor shkencor i AI është të kuptojë parimet bazë të sjelljes inteligjente që zbatohen në mënyrë të barabartë për sistemet njerëzore dhe artificiale. Në botën e sotme, teknologjia po rritet shumë shpejt dhe ne jemi në kontakt me teknologji të ndryshme dhe të reja ditë pas dite. Këtu, një nga këto teknologjitë në rritje, të shkencës kompjuterike është Inteligjenca Artificiale, e cila është gati të krijojë një revolucion të ri në botë duke bërë makina inteligjente. Inteligjenca Artificiale është tani kudo rreth nesh. Aktualisht është duke punuar me një sërë nënfushash, duke filluar nga e përgjithshme në atë specifike, si makina që drejtojnë vetë, të luajnë shah, të provojnë teorema, të luajnë muzikë, të pikturojnë, etj. AI ka nëngrupe të ndryshme që kontribuojnë në të, si machine learning, deep learning, NLP, Expert System, etj.

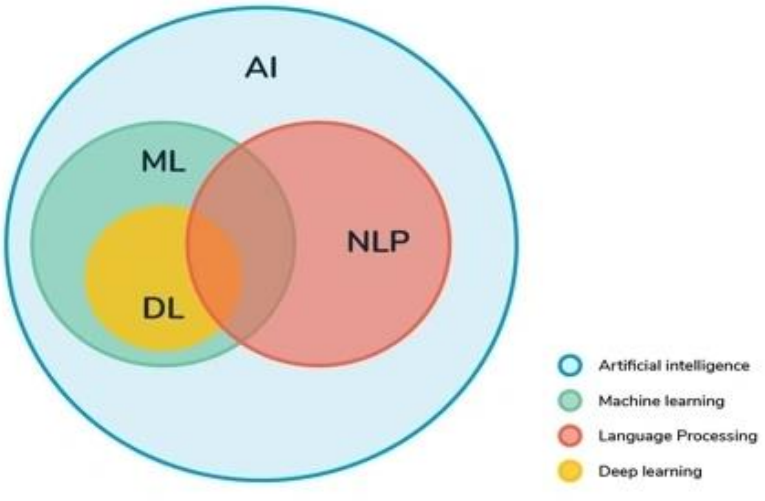

Figura 1. Nëngrupet e AI

2.2 Llojet e Inteligjencës Artificiale

Klasifikimi i AI mund të bëhet në disa mënyra:

- **AI i dobët – weak AI**: Njihet gjithashtu si narrow AI, i cili është krijuar për të kryer një detyrëspecifike. Vepron sikur mund të 'mendojë'.

- **AI i fortë – strong AI**: Njihet gjithashtu si inteligjencë e përgjithshme artificiale e cila kapërgjithësuar aftësitë njohëse të njeriut. Është mjaft inteligjente për të gjetur një zgjidhje.

AI i dobët - Weak AI	AI i fortë - Strong AI
I mirë në detyra specifike	Inteligjenca e pabesueshme e nivelit njerëzor
Përdor mësimin e mbikëqyrur dhe të pambikëqyrur	Përdor grupimin dhe shoqërimin
Psh. Siri, Alexa etj.	Psh. Advanced Robotics (robotë të avancuar)

Figura 2. Dallimet në mes Weak AI dhe Strong AI

Klasifikime tjera të AI [4] konsiderohen edhe:

- **Narrow AI** – AI e ngushtë: është një lloj AI që ju ndihmon të kryeni një detyrë të dedikuar me inteligjencë.

- **General AI -** AI e përgjithshme: është një lloj inteligjence e AI që mund të kryejë çdo detyrë intelektuale me efikasitet si një njeri.

- **Rule-based AI -** AI i bazuar në rregulla: bazohet në një grup rregullash të paracaktuara që zbatohennë një grup të dhënash hyrëse. Sistemi më pas prodhon një dalje përkatëse.

- **Decision Tree AI -** Pema e vendimeve AI: është e ngjashme me AI të bazuar në rregulla në atë qëpërdor grupe rregullash të paracaktuara për të marrë vendime. Megjithatë, pema e vendimit gjithashtu lejon për degëzimin dhe ciklin për të marrë në konsideratë opsione të ndryshme.

- **Super AI**: është një lloj AI që lejon kompjuterët të kuptojnë gjuhën njerëzore dhe të përgjigjen në një mënyrë natyrale.

- **Robot Intelligence** - Inteligjenca robotike: është një lloj AI që lejon robotët të kenë aftësi kompleksenjohëse, duke përfshirë arsyetimin, planifikimin dhe mësimin.

3. Sulmet Kibernetike

Një sulm kibernetik është çdo përpjekje për të fituar akses të paautorizuar në një kompjuter, sistem kompjuterik. Shfrytëzimi i madh i hapësirës kibernetike me qëllim të çasjes së paautorizuar, spiunazhit, deaktivizimit të rrjetave dhe vjedhjës së të dhënave dhe e parave cilësohet si sulm kibernetik. Sulmet e tillajanë shtuar në numër dhe kompleksitet gjatë viteve të fundit. Ka pasur një mungesë të njohurive rreth këtyre sulmeve që ka bërë shumë individë, agjenci, organizata të pasigurtë ndaj këtyre sulmeve [5].

Një sulm kibernetik ndodh kur kriminelët kibernetikë përpiqen të fitojnë akses të paligjshëm në të dhënat elektronike të ruajtura në një kompjuter ose një rrjet. Qëllimi mund të jetë shkaktimi i dëmtimit të reputacionit ose dëmtimi i një biznesi ose personi, ose vjedhja e të dhënave të vlefshme. Sulmet kibernetikemund të synojnë individë, grupe, organizata ose qeveri [6].

3.1 Motivi I sulmeve kibernetike

Objektivat kryesore të sulmeve kibernetike janë të dhënat ose informacionet e faqeve qeveritare, faqet e internetit të institucioneve financiare, forumet e diskutimit në internet dhe faqet e internetit të lajmeve dhemediave apo edhe të rrjeteve ushtarake/mbrojtëse [7]. Qëllimi dhe motivet e sulmit kibernetik përfshin disa procese, ato janë:

- Çasja e informacionit
- Kundërshtimi i masave të sigurisë kibernetike ndërkombëtare

- Vonesa e proceseve të vendimmarrjes
- Mohimi në ofrimin e shërbimeve publike
- Ulja e besimit publik
- Reputacioni i vendit te prishet
- Shkatërrimi i interesit ligjor

3.2 Klasifikimi i sulmeve kibernetike

Klasifikimi i sulmeve kibernetike mund të kategorizohet si më poshtë:

- Në bazë të qëllimit
- Klasifikimi Ligjor
- Bazuar në ashpërsinë e përfshirjes
- Bazuar në Fushëveprimin
- Bazuar në Llojet e Rrjetit

Disa nga shembujt e sulmeve të zakonshme kibernetike përfshijnë [8]:

- Vjedhja e identitetit (Identity theft), mashtrimi (fraud)
- Malëare, phishing, spamming, spoofing, spyëare, trojans, viruses
- Paisje të vjedhura, të tilla si laptop ose paisje celulare
- Denial-of-service / distributed denial-of-service attacks
- Shkelja e aksesit (Breach of access)
- Password sniffing
- System infiltration
- Website defacement
- Private and public Web browser exploits
- Instant messaging abuse
- Intellectual property (IP) theft or unauthorized access (Vjedhja e IP-së)

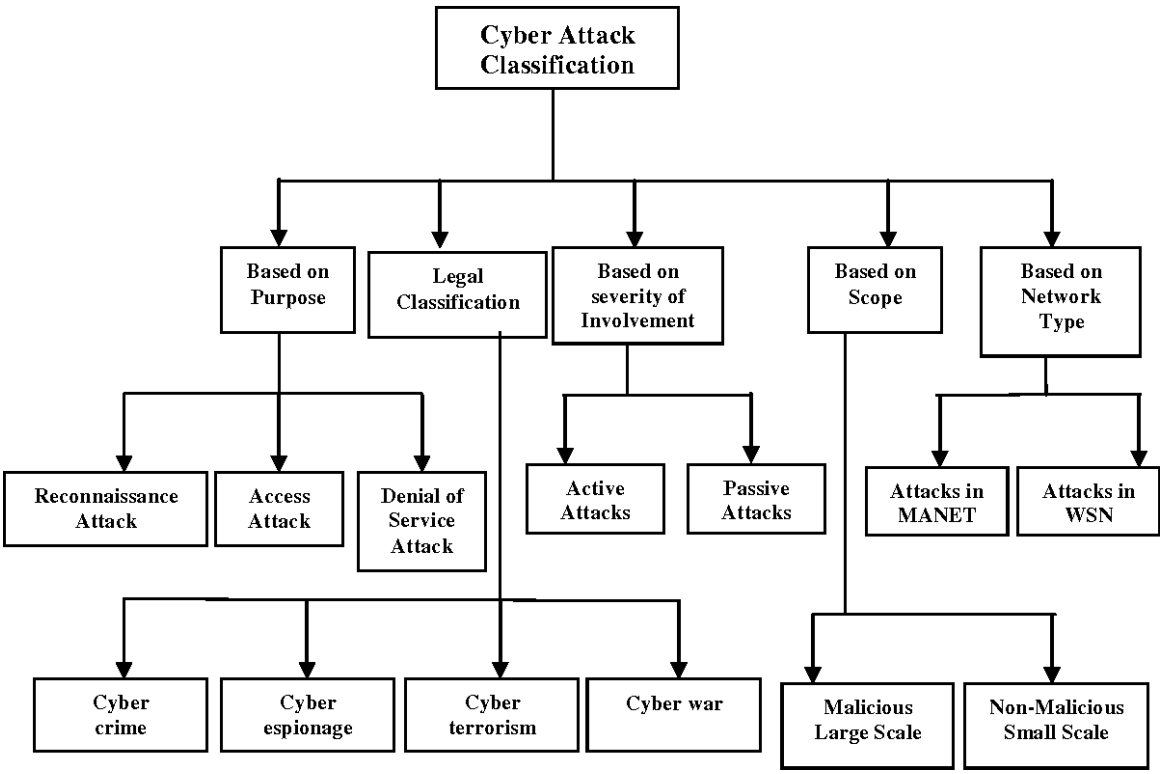

Figura 3. Klasifikimi i Sulmeve Kibernetike

3.3 Si mund të reduktohen sulmet kibernetike

Organizatat mund të zvogëlojnë sulmet kibernetike me një sistem efektiv të sigurisë kibernetike. Siguria kibernetike është praktikë e mbrojtjes së sistemeve kritike dhe informacioneve të ndjeshme nga sulmet dixhitale, duke përfshirë teknologjinë, njerëzit dhe proceset. Një sistem efektiv i sigurisë kibernetike parandalon, zbulon dhe raporton sulmet kibernetike duke përdorur teknologjitë kryesore të sigurisëkibernetike [8] dhe praktikat më të mira, duke përfshirë:

- Menaxhimi i identitetit dhe aksesit
- Një platformë gjithëpërfshirëse e sigurisë së të dhënave
- Informacioni i sigurisë dhe menaxhimi i ngjarjeve
- Shërbimet e sigurisë sulmuese dhe mbrojtëse dhe inteligjenca e kërcënimeve

3.4 Pse është e rëndësishme siguria kibernetike?

Krimi kibernetik mund të prishë dhe dëmtojë bizneset. Në vitin 2021, për shembull, kostoja mesatare e njëshkeljeje të të dhënave ishte 4.24 milionë dollarë globalisht dhe 9.05 milionë dollarë në Shtetet e Bashkuara [8][9]. Këto kosto përfshijnë zbulimin dhe reagimin ndaj shkeljes, koston e kohës së ndërprerjes dhe të ardhurave të humbura, dhe dëmtimin afatgjatë të reputacionit të një biznesi dhe markës së tij. Dhe në rastetë caktuara, mund të çojë në humbje të besimit të klientit, gjoba rregullatore dhe madje edhe veprime ligjore.

3.5 AI në botën e sulmeve kibernetike

Ndërsa kompanitë janë tërhequr më thellë në epokën dixhitale, nevoja për mbrojtje kundër kërcënimeve kibernetike është e domosdoshme. Në fakt, një studim i kohëve të fundit tregon se një sulm kibernetik ndodh çdo 39 sekonda [10]. Inteligjenca artificiale (AI) është një strategji efektive për të penguar numrin në rritje të sulmeve të vendosura ndaj organizatave sot – si luftimi i zjarrit me zjarr. Jo vetëm që AI po rritshpejtësinë dhe saktësinë e mbrojtjes, por gjithashtu po kursen kohë dhe burime.

Në të kaluarën, monitorimi i kërcënimeve të sigurisë kibernetike ishte një detyrë e lodhshme manuale. Kohae shpenzuar për monitorimin dhe veprimin ndaj këtyre sulmeve ishte intensive dhe rezultatet ishin më pakefektive. Përdorimi i AI në këtë hapësirë ka transformuar të gjithë procesin, duke optimizuar aftësinë tonë për të zbuluar dhe luftuar kërcënimet [10]. Duke automatizuar mbrojtjen, kompanitë mund të vendosin një bazëmbrojtjeje dhe t'i besojnë teknologjisë për të identifikuar këto kërcënime përpara se të bëhen sulme.

3.6 Si përdoret AI për të kryer sulme kibernetike?

AI po përdoret nga kriminelët për të vendosur strategji komplekse të hakimit. Në të njëjtën mënyrë që AI përdor të dhënat për të detektuar kërcënimet, ajo mund të përdoret gjithashtu për të identifikuar dobësitë endryshme. Disa kriminelë mund të ndryshojnë (reverse engineer) modele të inteligjencës artificiale për të shkelur të dhënat e ndjeshme dhe në mënyrë që të kontrollojnë sigurinë kibernetike të një kompanie [10]. Pothuajse çdo taktikë që përdor një kriminel kibernetik mund të përmirësohet me AI.

Sulmet kibernetike të fuqizuara nga AI nuk janë një koncept hipotetik i së ardhmes. Të gjitha blloqet e nevojshme ndërtuese për përdorimin e "offensive AI" tashmë ekzistojnë: malware shumë i sofistikuar, kriminelë të motivuar financiarisht, të gatshëm të përdorin çdo mjet të mundshëm për të rritur kthimin e tyre nga investimi dhe projekte open-source (duke përdorur inteligjencën artificiale) që bëjnë informacionshumë të vlefshëm në dispozicion për domenin publik [11].

3.7 Sulmet që përdorin AI

Jo vetëm që asnjë sektor nuk është komplet i mbrojtur nga sulmet kibernetike, por edhe niveli i sofistikimit të kërcënimeve me të cilat përballen po rritet vazhdimisht. Nuk ka dyshim se inteligjenca artificiale (AI) do të përdoret nga sulmuesit për të nxitur përmirësimin madhor të radhës në "armatimin" kibernetik dhe përfundimisht do të jetë pionier i përdorimit keqdashës të AI.

Edhe pse ka një shumëllojshmëri të gjerë të detyrave të AI që mund të përdoren në sulme, këto janë ndër më të zakonshmet:

Prediction (parashikimi): kjo është një detyrë për të bërë një parashikim bazuar në të dhënat e vëzhguara më parë. Shembuj të zakonshëm përfshijnë: klasifikimin, zbulimin e anomalive dhe regresioni. Kurse shembuj të parashikimit për një qëllim të keq përfshijnë identifikimin e goditjeve të tasteve në një smartphone duke u bazuar në lëvizje [12] [13] [14] , zgjedhjen e lidhjes më të dobët në zinxhirin për të sulmuar [15] dhe lokalizimin e dobësive të softuerit për shfrytëzim [16].

Generation (gjenerimi): Kjo është detyra e krijimit të përmbajtjes që i përshtatet një shpërndarjeje të një targeti, e cila, në disa raste, kërkon realizëm në sytë e një njeriu. Shembuj të gjenerimit për përdorime keqdashëse përfshijnë ndryshimin e provave mediatike [17] apo gjetjen "inteligjente" të fjalëkalimit [18]. Deepfakes janë një tjetër shembull i sulmeve përmes AI në këtë kategori. Deepfake është një media e besueshme e krijuar nga një model DL1. Teknologjia mund të përdoret për të imituar një viktimë duke përdor zërin ose fytyrën e saj për të kryer një sulm phishing.

Analysis (analiza): Kjo është detyra e nxjerrjes së njohurive të dobishme nga të dhënat ose një model. Disa shembuj të analizës për sulme janë përdorimi i teknikave të shpjegueshme të AI [19] për të identifikuar se si të fshihen më mirë artifaktet2 (p.sh. në malware) dhe grumbullimi ose futja e informacionit në një organizatë për të identifikuar asetet ose objektivat për social engineering (inxhinierinë sociale).

Retrieval (rikthimi): Kjo është detyra e gjetjes së përmbajtjes që përputhet ose që është semantikisht e ngjashme me një pyetësor (query) të caktuar. Për shembull, në ofendim, algoritmet e rikthimit mund të përdoren për të gjurmuar një objekt ose një individ në një sistem mbikëqyrjeje [20], për të gjetur një punonjës të pakënaqur, duke përdorur analiza semantike në postimet e mediave sociale dhe për të përmbledhur dokumente të gjata [21] në fazën e zbulimit (reconnaissance3).

Decision making (marrja e vendimeve): Detyra e krijimit të një plani strategjik ose koordinimi i një operacioni. Shembuj të kësaj në sulmet përmes AI janë përdorimi i swarm inteligjencës për të operuar një botnet autonome [22] dhe përdorimin e grafikëve të sulmeve heuristike për të planifikuar sulme optimale në rrjete [23].

3.8 Ndikimi i "offensive AI"

Pse një sulmues do ta konsideronte përdorimin e AI për sulmet e tij ndaj ndonjë objektive?

3.8.1 Motivet kryesore

Ekzistojnë tre motive thelbësore [24] për një kundërshtar që të përdorë AI në një ofensivë kundër një organizate apo objektivi tjetër: mbulimi, shpejtësia dhe suksesi.

Coverage (mbulimi): Duke përdorur AI, një sulmues mund të rrisë operacionet e tij përmes automatizimitpër të ulur punën njerëzore dhe për të rritur mundësitë për sukses. AI mund të përdoret për të bërë sulme spear phishing[4] në mënyrë automatike, për të bërë sulme në mënyrë paralele ndaj organizatave të ndryshmesi dhe për të arritur më shumë informata dhe asete brenda një rrjeti. Me fjalë të tjera, AI u mundëson sulmuesëve të targetojnë më shume organizata me sulme me një saktësi më të lartë duke përdorur një fuqipunëtore më të vogël.

Speed (shpejtësia): Duke përdorur AI, sulmuesi mund t'i arrijë qëllimet e tij shumë më shpejt. Për shembull, machine learning mund të përdoret për nxjerrjen e kredencialeve, për gjetjen e objektivit më të mire, për të gjetur zero-days[5] në softuer etj. Duke arritur deri te qëllimi më shpejt, sulmuesit jo vetëm që kursejnë kohën për sulme tjera, por gjithashtu mund të minimizojë praninë (kohëzgjatjen) e tij brenda rrjetittë mbrojtësit.

Success (suksesi): Duke përmirësuar operacionet e tij me AI, një sulmues rrit gjasat e tij për sukses. Gjegjësisht, ML mund të përdoret për (1) ta bëjë operacionin më të fshehtë duke minimizuar ose kamufluartrafikun e rrjetit, dhe duke shfrytëzuar dobësitë në modelet e mbrojtësit, siç është ML-based intrusion detection system (IDS), (2) për të identifikuar objektiva të mira për sulme të social engineering dhe dobësitë reja, (3) për të mundësuar vektorë më të mirë të sulmit si përdorimi i deepfakes në sulmet spear phishing, (4) planifikim të strategjive optimale sulmi dhe (5) forcimin e qëndrueshmërisë në rrjet.

3.9 Shembuj të sulmeve kibernetike që përdorin AI

Në këtë seksion paraqiten të ashtuquajturat "offensive AI capabilities" [24], te ndara ne 7 kategori të ndryshme.

1. Automation (Automatizimi):
    - Attack Adaptation
    - Attack Coordination
    - Next hop targeting
    - Phishing Campaigns
    - Point of Entry Detection
    - Record Tampering

2. Campaign Resilience (Qëndrueshmëria e fushatës)
    - Campaign Planning
    - Malware Obfuscation
    - Persistent Access
    - Virtualization Detection

3. Credential Theft (Vjedhja e kredencialeve)
    - Biometric spoofing
    - Cache mining
    - Implicit key logging
    - Password Guessing
    - Side Channel Mining

4. Exploit Development
    - Reverse Engineering
    - Vulnerability Detection

5. Information Gathering (Mbledhja e informacionit)
    - Mining OSINT
    - Model Thef
    - Spying

6. Social Engineering (Inxhinieria sociale)
    - Impersonation (Identity Theft)
    - Persona Building
    - Spear Phishing
    - Target Selection
    - Tracking

7. Stealth (Vjedhja)
    - Covering tracks
    - Evading HIDS (Malware Detectors)
    - Evading NIDS (Network Intrusion Detection Systems)
    - Evading Insider Detectors
    - Evading Email Filter
    - Propagation & Scanning

Figura 4. Rezultatet për aftësitë sulmuese të AI, të renditura sipas pikës së tyre të kërcënimit, nga e majta në të djathtë

Profit (Përfitimi): Sasia e përfitimit, duke përdorur AI krahasuar me përdorimin e metodave që nuk përdorin AI.

Achievabilty (Arritshmëria): Sa e lehtë është për sulmuesin të përdorë AI për këtë detyrë?

Defeatability (Mundësia e mposhtjes): Sa e lehtë është për mbrojtësin të zbulojë ose parandalojë sulmine bazuar në AI.

Harm (Dëmi): Sasia e dëmit që mund të shkaktohet në aspektin fizik, psikologjik apo monetar

Përdorimi i inteligjencës artificiale për qëllime keqdashëse do të ndikojë në hapësirën e sigurisë në tremënyra kryesore [25]:

1. Imitimi i përdoruesve të besuar

   Sulmet e AI do të jenë shumë të përshtatura, por do të funksionojnë në shkallë. Këto malëare do të jenënë gjendje të mësojnë nuancat e sjelljes dhe gjuhës së një individi duke analizuar komunikimet me email dhe mediat sociale. Ata do të jenë në gjendje ta përdorin këtë njohuri për të përsëritur stilin e të shkruarit të një përdoruesi, duke krijuar mesazhe që duken shumë të besueshme. Prandaj, mesazhet e shkruara nga malëare i AI do të jenë pothuajse të pamundura të dallohen nga komunikimet e vërteta.

2. Përzierja

   Sulmuesit shpesh mund të mbajnë një prani afatgjatë në mjediset e tyre të synuara për muaj të tërë, pa u zbuluar. Ata lëvizin ngadalë dhe me kujdes, për t'iu shmangur kontrolleve tradicionale të sigurisë dheshpesh janë në shënjestër të individëve dhe organizatave të veçanta. AI do të jetë gjithashtu në gjendjetë mësojë kanalet dominuese të komunikimit, portat dhe protokollet më të mira për t'u përdorur për të lëvizur nëpër një sistem, duke u përzier në mënyrë diskrete. Kjo aftësi për t'u maskuar mes zhurmës do të thotë se është në gjendje të përhapet me profesionalizëm brenda një mjedisi dixhital dhe të kompromet ojë fshehurazi më shumë pajisje se kurrë më parë. Malëare i AI do të jetë gjithashtu në gjendje të analizojë vëllime të mëdha të të dhënave me shpejtësinë e makinës, duke identifikuar me shpejtësi se cilat grupe të dhënash janë të vlefshme dhe cilat jo. Kjo do t'i kursejë sulmuesit shumë kohëdhe përpjekje.

3. Sulme më të shpejta me pasoja më efektive

Sulmet më të sofistikuara të sotme kërkojnë që njerëz të aftë të kryejnë kërkime mbi objektivin e tyre dhe të identifikojnë individët me interes, të kuptojnë rrjetin e tyre social dhe të vëzhgojnë me kalimin e kohës se si ndërveprojnë me platformat dixhitale. Në botën e së nesërmes, një inteligjencë artificialekeqdashëse do të jetë në gjendje të arrijë të njëjtin nivel të sofistikimit në një pjesë të vogël të kohës, dhe në shkallë shumë më të madhe.

Jo vetëm që sulmet e drejtuara nga AI do të jenë shumë më të përshtatura dhe rrjedhimisht më efektive,aftësia e tyre për të kuptuar kontekstin do të thotë se ato do të jenë edhe më të vështira për t'u zbuluar. Kontrollet tradicionale të sigurisë do të jenë të pafuqishme ndaj këtij kërcënimi të ri, pasi ato mund të dallojnë vetëm aktivitet të parashikueshëm dhe të paramodeluar. Inteligjenca artificiale po zhvillohet vazhdimisht dhe do të bëhet gjithnjë e më rezistente ndaj kategorizimit të kërcënimeve.

3.10 Përdorimi i Machine Learning në sulmet kibernetike

Përderisa machine learning është përdorur në sigurinë kibernetike për të identifikuar malware të ngjashëmdhe linqe të pasigurta, në lidhje me krimet kibernetike përdoret edhe për tejkalimin e konfirmimit të CAPTCHA-ve, dhe gjenerimin e phishing email-ave. Kur krahasohen të dyja, siguria kibernetike duket seka përdorime shumë më të konsoliduara për machine learning. Por tendencat e ardhshme drejt malware evazive dhe phishing mund të përbëjnë një kërcënim serioz për industrinë e sigurisë kibernetike [26].

Password brute-force

Algoritmet e machine learning mund të përdoren gjithashtu për të gjeneruar të dhëna të ngjashme me një grup të dhënash të caktuar. Kjo është veçanërisht e dobishme në gjenerimin e fjalëkalimeve jashtë termaveqë lidhen me një përdorues. Machine learning mund të gjenerojë lista fjalëkalimesh shumë më të sakta dhe mund të rezultojë në një përpjekje të suksesshme të brute-force.

Evasive Malware

Machine learning i përdorur në zbulimin e malware mund të konsiderohet si një nga aplikimet e para të vërteta të inteligjencës artificiale në sigurinë kibernetike. Megjithatë, dokumentet e fundit janë publikuar që tregojnë se si malware mund të krijohet për të shmangur këto zbulime përmes përdorimit të machine learning.

Advanced phishing

Sulmet e phishing kanë ekzistuar për më shumë se 20 vjet dhe kanë vazhduar të jenë të suksesshme edhe pse njohuritë e publikut për to janë rritur. Për të rritur gjasat e një mashtrimi të suksesshëm, mbledhja manuale e informacionit mund të bëhet në një objektiv të caktuar. Kjo mund të arrijë deri në 45% norma tëklikimeve (CTR[7]) në një link të pasigurtë. Megjithatë, ky proces është shumë më i ngadalshëm se metodate automatizuara. Një dokument i publikuar nga Blackhat ka përdorur machine learning për ta automatizuarkëtë, duke përdorur profilin e një përdoruesi të Twitter dhe duke gjeneruar postime të synuara nga llogaritëbot. Kjo metodë u zbulua se ishte 4 herë më e shpejtë se manual phishing dhe ruan një shkallë të lartë klikimesh midis 33% dhe 66%, duke e bërë atë po aq të besueshme sa phishing manual në disa skenarë, nëse jo më shumë. Ky është një shembull i botës reale se si automatizimi dhe AI mund të përdoren për të synuar dhe mashtruar përdorues të veçantë [26].

CAPTCHA bypass

CAPTCHA-të janë të pranishme në aplikacionet në ueb në të gjithë internetin, me qëllim që të parandalojnëskriptet e automatizuara nga brute-frocing ose regjistrimi masiv i shumë llogarive bot për qëllime keqdashëse. CAPTCHA-të përfshijnë plotësimin e një sfide të thjeshtë që një robot mund ta ketë të vështirë.Megjithatë, ndërsa machine learning bëhet më i avancuar, modelet mund të bëhen jashtëzakonisht efikase në zgjidhjen e tyre dhe anashkalimin e mbrojtjes. Kjo mund të çojë në sulme me brute-force që mund të kompromëtojnë një llogari.

4. Përfundimi

Me anë të këtij punimi, kemi arritur të hulumtojmë dhe të kuptojmë më shumë në lidhje me rolin e Inteligjences Artificiale në Cyber Security. Për shkak se në ditët e sotme është mjaft I rritur numri I sulmeve kibernetike, Inteligjenca Artificiale ka ndikuar mjaft shumë në parandalimin e këtyre sulmeve dhe në përmirësimin e sigurisë në Internet, mirëpo në të njëjtën kohë, fatkeqësisht po përdoret edhe për qëllime të dëmshme. Mënyra se si ne e shikojmë ndikimin e AI në jetën e përditshme bënë ndryshimin si në anën e mirë të saj ashtu edhe në anën tjetër. Prandaj, na takon ne si përdorues të vendosim se si të shfrytëzojmë dobësitë dhe dobitë e kësaj teknologjie dhe të jemi të kujdesshëm dhe informuar rreth sulmeve në të cilat mund të hasim.

Bibliografia dhe Referencat

[1] R. B. V. Susan M Bridges, "FUZZY DATA MINING AND GENETIC ALGORITHMS APPLIED TO INTRUSION DETECTION," [Online]. Available: https://csrc.nist.rip/nissc/2000/proceedings/papers/005.pdf.

[2] H. 2020, "Leadership in enabling and industrial technologies: Information and Communication Technologies.," 25 Nov 2019. [Online]. Available: https://ec.europa.eu/research/participants/portal4/doc/call/h2020/common/1587758-05i._ict_wp_2014-2015_en.pdf.

[3] J. McCarthy, "Artificial Intelligence Tutorial | AI Tutorial," 2019. [Online]. Available: https://www.tutorialandexample.com/artificial-intelligence-tutorial.

[4] "What is Artificial Intelligence: Introduction, history and types of AI.," 2023. [Online]. Available: https://www.guru99.com/artificial-intelligence-tutorial.html#6.

[5] "Cyber Security: Protecting Our Federal Government From Cyber Attacks, the 2009 data breach," 2019.

[6] M. U. a. G. Padmavathi, "A Survey on Various Cyber Attacks and Their Classification," 2019. [Online]. Available: https://www.semanticscholar.org/paper/A-Survey-on-Various-Cyber-Attacks-and-their-Uma-Padmavathi/ba7b234738e80b027240e9bfd837bfba61c13e17.

[7] "N. Goderdzishvili, Legal Assessment of Cyber Attacks on Georgia, Data Exchange AgencyMinistry," [Online].

[8] "What is a cyberattack?," 2020. [Online]. Available: https://www.ibm.com/topics/cyber-attack.

[9] "How much does a data breach cost in 2021?," 2023. [Online]. Available: https://www.guru99.com/artificial-intelligence-tutorial.html#6.

[10] "How AI Can Help Stop Cyber Attacks: Our Guide.," 2022. [Online]. Available: https://www.sailpoint.com/identity-library/how-ai-can-stop-cyber-attacks/.

[11] "3 ways AI will change the nature of cyber attacks," 19 June 2019. [Online]. Available: https://www.weforum.org/agenda/2019/06/ai-is-powering-a-new-generation-of-cyberattack-its-also-our-best-defence/.

[12] Andreas C. Müller and Sarah Guido, "“Introduction to Machine Learning with Python”".

[13] A. A.-H. A. Z. B. Z. M. M. K. N. B. A. Muzammil Hussain, in *The rise of keyloggers on smartphones: A survey and insight into motion-based tap inference attacks. Pervasive and Mobile Computing 1-25*.

[14] M. O. B. M. A. T. B. a. A. H. A.-B. Abdul Rehman Javed, "AlphaLogger: Detecting motion-based side-channel attack using smartphone keystrokes.Journal of Ambient Intelligence and Humanized Computing 1-14," 2020.

[15] A. V. H. C. a. P. T. Philip Marquardt, "Decoding vibrations from nearby keyboards using mobile phone accelerometers. In Proceedings of the 18th ACM conference on Computer and communications security. 551–562.".

[16] A. I. a. M. R. Y. Abid, in *Sensitive Attribute Prediction for Social Networks Users. In EDBT/ICDT Workshops*, 2019.

[17] X. Y. Y. S. a. H. Z. Jian Jiang, "A Survey of the SoftwareVulnerability Discovery Using Machine Learning Techniques. In International Conference on Artificial Intelligence and Security. Springer, 308–317.," 2019.

[18] T. M. I. S. a. Y. E. Yisroel Mirsky, "Malicious Tampering of 3D Medical Imagery using Deep Learning. In 28th USENIX Security Symposium (USENIX Security 19). USENIX Association, Santa Clara, CA, 461–478.," 2019. [Online]. Available: https://www.usenix.org/conference/usenixsecurity19/presentation/mirsky.

[19] V. G. a. L. Ahuja., "Password Guessing Using Deep Learning.International Conference on Power Energy, Environment and Intelligent Control (PEEIC). IEEE, 38-40," 2019.

[20] S. S. a. C. G. Marco Tulio Ribeiro, "“Why Should I Trust You?”:Explaining the Predictions of Any Classifier. In 22nd ACM SIGKDD Int’l Conf. Knowl. Disc.Data Mining (KDD ’16). ACM, New York, NY, USA, 1135–1144".

[21] M. R. a. Y. W. T. Rahman, "Video-Based Person Re-Identification using Refined Attention Networks. In 2019 16th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). 1–8.," 2019. [Online]. Available: https://doi.org/10.1109/AVSS.2019.8909869.

[22] R. D. P. A. D. S. U. F. a. F. P. Aniello Castiglione, "A botnet-based command and control approach relying on swarm intelligence. Journal of Network and Computer Applications 38 (2014), 22–33.," [Online]. Available: https://doi.org/10.1016/j.jnca.2013.05.002.

[23] M. D. P. T. S. W. K. P. M. a. W. A. C. John A. Bland, "Machine Learning Cyberattack and Defense Strategies. Computers & Security 92 (2020),," 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2020.101738.

[24] Y. MIRSKY., "The Threat of Offensive AI to Organizations.," 2021. [Online]. Available: https://arxiv.org/pdf/2106.15764.pdf.

[25] 2019. [Online]. Available: https://europeansting.com/2019/06/20/3-ways-ai-will-change-the-nature-of-cyber-attacks/.

[26] "How Machine Learning Is Used In Cyber Attacks," 2021. [Online]. Available: https://informer.io/resources/how-machine-learning-is-used-in-cyber-attacks.