SUN’IY INTELLEKTGA ASOSLANGAN ZARARLI DASTURLARNI ANIQLASH VA TAHLIL QILISH

Elshod Haydarov

Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
E-mail: elshodhaydarov1881@gmail.com

K E Y W O R D S

kiberxavfsizlik analitikasi, raqamli kriminalistika tekshiruvi, zararli dasturlarni aniqlash va oldini olish, sun’iy intellekt kriminalistika tekshiruvlarini

A B S T R A C T

Zararli dasturlar (malware) — kiberhujumchilarning eng xavfli qurollaridan biri bo‘lib, ular tobora murakkablashib, tezkor tarqalish va o‘z-o‘zini ko‘paytirish xususiyatiga ega bo‘lib bormoqda. Bundan tashqari, zamonaviy zararli dasturlar kiberjinoyatchilikning eng vayronkor shakllaridan biri hisoblanadi, chunki ular aniqlanishdan qochishi, real vaqtga yaqin raqamli deyarli imkonsiz qilishi mumkin. Murakkab yashirinish strategiyalarining ta’siri esa juda jiddiy va keng ko‘lamli bo‘lishi mumkin. Shu sababli, zararli dasturlarni o‘z vaqtida va avtonom tarzda aniqlash ularni samarali tahlil qilish uchun muhim ahamiyatga ega. Ushbu ishda zamonaviy zararli dasturlarni aniqlash uchun yangi tizimli yondashuv taklif etiladi. Ushbu yondashuv dinamik, chuqur o‘rganishga asoslangan usullarni evristik yondashuvlar bilan birlashtiradi va quyidagi beshta zamonaviy zararli dastur oilasini aniqlash hamda tasniflashga qaratilgan: reklama dasturlari (adware), radware, rootkit, SMS zararli dasturlari, ransomware. Sun’iy intellekt va kiberxavfsizlik analitikasi doirasidagi tadqiqotimiz zararli dasturlarni aniqlash, tahlil qilish va oldini olish imkoniyatlarini yaxshilab, kiberxavflarga chidamli tizimlarni yaratishga xizmat qiladi. Taklif etilgan yondashuv so‘nggi zararli dasturlarni o‘z ichiga olgan maxsus ma’lumotlar to‘plami yordamida tekshirildi. Natijalar modelning samaradorlik va tezkorlik bo‘yicha real hayot talablariga mos kelishini ko‘rsatdi. Tajriba natijalari shuni ko‘rsatadiki, xatti-harakatga asoslangan chuqur o‘rganish va evristik usullarni birlashtirish statik chuqur o‘rganish usullariga qaraganda yuqori natija beradi.

I. Kirish

Telekommunikatsiya tarmoqlarining jadal rivojlanishi va internet metaforasining kengayishi tashkilotlar faoliyatini amalga oshirish usullarini tubdan o‘zgartirdi. Darhaqiqat, texnologiyaning jadal rivojlanishi, raqamlashtirish, bulutli hisoblash, kvant hisoblash [1] hamda ulanish imkoniyatiga ega bo‘lgan obyektlar sonining keskin ortishi misli ko‘rilmagan kiberjinoyat faoliyatining paydo bo‘lishiga olib keldi.

Muhim infratuzilmalarga , ma’lumotlar markazlariga, davlat tashkilotlariga va moliyaviy sektor obyektlariga qaratilgan yashirin kiberhujumlarning ko‘payishi (individual va ijtimoiy nuqtai nazardan) katta muammolarni keltirib chiqarmoqda. Murakkab kiberhujumlar asosan zararli dasturlarga tayanadi va ular moliyaviy talon-toroj, kiberjosuslik, tizim faoliyatini izdan chiqarish, shaxsni o‘g‘irlash, maxfiy ma’lumotlarni noqonuniy chiqarib olish hamda boshqa siyosiy maqsadlar uchun qo‘llaniladi [2].

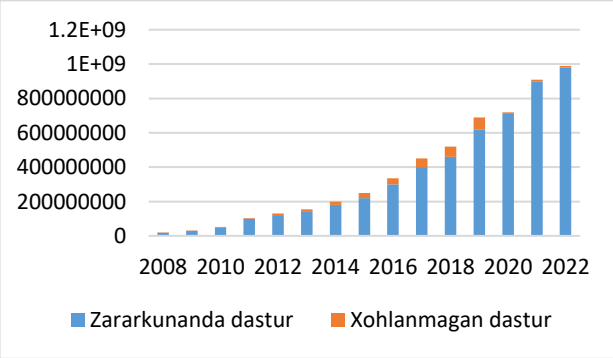
Bugungi kunda kompyuter texnologiyalari sohasida mislsiz yutuqlarga erishilayotgan bo‘lsada, kiberjinoyatchilikning globallashuvi ham ortib bormoqda. Xususan, COVID-19 pandemiyasi davrida raqamli tizimlarga bo‘lgan yuqori bog‘liqlik ransomware kabi zararli dasturlar sonining keskin oshishiga olib keldi. COVID-19 kiberxavflarning ko‘payishida muhim rol o‘ynadi [3], chunki tashkilotlar va foydalanuvchilar yangi, oldindan aytib bo‘lmaydigan sharoitlarga moslashishga majbur bo‘ldi. Bu esa kiberhujumchilarga yanada zamonaviy vositalar va texnikalarni qo‘llash imkonini berdi.

Zamonaviy kiberhujumlar muhiti kiberurush (cyberwarfare) davriga olib keldi. Ushbu jarayonda chegaralar va cheklovlar deyarli yo‘q bo‘lib, faol kiberjosuslik kuzatilmoqda.

© Elshod Haydarov

Kiberurush sharoitida qo‘llaniladigan eng samarali himoya mexanizmlaridan biri zamonaviy zararli dasturlardan foydalanishga asoslanadi.

Kaspersky Security Bulletin (KSB) [2] ma’lumotlariga ko‘ra, 2022-yilda kiberjinoyatchilar foydalanuvchilarga kuniga 400 000 ta yangi zararli fayl bilan hujum qilgan (2021-yilga nisbatan 5% o‘sish). Shuningdek, ransomware ulushi 2021-yilga nisbatan 181% ga oshib, kuniga 9500 ta shifrlovchi faylga yetgan. Android platformasini nishonga olgan zararli fayllar ulushi ham 10% ga oshgan. 2022-yildagi mashhur kampaniyalar — Harly [3] va Triada Trojan— dunyo bo‘ylab minglab Android foydalanuvchilarini zararlagan va ushbu tendensiyaning yaqqol misolidir. 2022-yilgi SpyCloud Ransomware Defense Report hisobotida AQSh, Buyuk Britaniya va Kanada tashkilotlarida faoliyat yurituvchi 300 dan ortiq IT xavfsizlik mutaxassislari ishtirok etgan. Tadqiqot natijalariga ko‘ra, 2022-yilda tashkilotlarning 90% ransomware hujumiga uchragan, bu ko‘rsatkich 2021-yilda 72,5% edi. Symantec ma’lumotlariga ko‘ra, yangi zararli dasturlarning 50% dan ortig‘i mavjud zararli dasturlarning modifikatsiyalari hisoblanadi.



1-rasm. 2008–2022 yillar oralig‘ida zararli dasturlar va xohlanmagan dasturlar soni

Bundan tashqari, AV-TEST instituti har kuni 450 000 dan ortiq yangi zararli dasturlar va potensial istalmagan ilovalarni (PUA) ro‘yxatdan o‘tkazadi [4]. 2008–2022 yillar oralig‘ida zararli dasturlar va PUA’larning umumiy soni sezilarli darajada oshgan (1-rasm).

Kiberhujumchilar ma’lum va noma’lum zaifliklardan foydalanib, muvaffaqiyatli zararlanishlarni amalga oshirishga harakat qiladilar. Ulangan qurilmalar sonining keskin oshishi zararli dastur hujumlarining miqyosini yanada kengaytiradi va bu jiddiy muammolarni keltirib chiqaradi.

Raqamli dunyoda ekotizimlarning sog‘lom ishlashi xizmatlar, operatsiyalar va tranzaksiyalarning ishonchliligi hamda xavfsizligiga bog‘liq bo‘lib, bu ko‘pincha shifrlash algoritmlari orqali ta’minlanadi. Biroq, an’anaviy kompyuterlar uchun ushbu yondashuv yetarli darajada samarali emas. Shu sababli, klassik kriptografiyani takomillashtirish uchun innovatsion yechimlar zarur.

Kvant kriptografiya (kvant mexanikasi va klassik kriptografiya kombinatsiyasi) va kvant kalitlarini taqsimlash (QKD) kvant aloqa hujumlariga qarshi samarali yechim bo‘lishi mumkin [5]. Kvant kriptografiya tasodifiy yaratilgan qubitlarni uzatishga asoslanib, har qanday sharoitda axborot almashinuvining buzilmasligini ta’minlaydi. Qubitlar shifrlash protokollarida kalit sifatida ishlatiladi. Uzoq masofalarga qubitlarni uzatishda fotonlar asosiy tashuvchi vosita hisoblanadi.

Shuningdek, kvant texnologiyalari — kvant aloqa tizimlari va kvant kompyuterlar — an’anaviy kompyuterlarga qaraganda ancha tez va aniq hisoblash imkonini beradi. Bu kvant mashinali o‘qitish rivojiga zamin yaratadi va xavfsiz aloqa tizimlarini shakllantirishga yordam beradi.

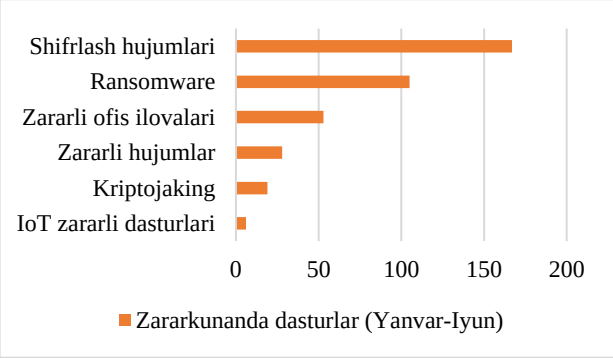
Katta hajmdagi ma’lumotlar, vaqt va murakkablik cheklovlarini hisobga olgan holda, kvant texnologiyalari sun’iy intellekt imkoniyatlarini sezilarli darajada kengaytirishi mumkin. Katta hajmli kvant hisoblash (LSQ) va sun’iy intellekt kombinatsiyasi kiberxavfsizlik sohasida haqiqiy inqilob bo‘lishi mumkin. Shu bilan birga, bu imkoniyatlar noto‘g‘ri qo‘llansa, kiberjinoyatchilar uchun ham halokatli qudratga aylanishi ehtimoli mavjud.

2022-yil yanvar–iyun oylarida zararli dasturlar taqsimoti quyidagicha kuzatildi:

- IoT zararli dasturlari – 6%,
- kriptojacking – 19%,
- zararli intruziyalar – 28%,
- zararli Office va PDF fayllar – 53%,
- ransomware – 105%,
- shifrlangan tahdidlar – 167% [6].

© Elshod Haydarov

ISSN: 3030-3346



2-rasm. 2022-yilga kelib global zararli dasturlarning tendensiyalari

Ma’lum va noma’lum zararli dasturlarga qarshi barqaror himoya mexanizmlarini ishlab chiqish muhim ahamiyatga ega. Biroq, zararli dasturlar oilalari va namunalarining ko‘pligi real vaqt rejimida tezkor va avtomatik javob qaytarishni qiyinlashtiradi. Shu sababli, chuqur o‘qitish(DL) kabi ilg‘or sun’iy intellekt texnologiyalarini joriy etish zarur.

An’anaviy mashinali o‘qitish usullari (RF, DT, SVM) keng qo‘llanilgan bo‘lsa-da, ular zero-day yoki noma’lum zararli dasturlarni aniqlashda yetarli samaradorlik bermaydi. Shu bois tadqiqotlar chuqur o‘rganishga asoslangan yondashuvlarga yo‘naltirildi. Biroq, DL usullari ham real vaqt rejimida murakkab evasion texnikalarini aniqlashda muammolarga duch keladi.

Shu sababli, dinamik chuqur o‘rganishga asoslangan, ishonchli va samarali tizimlar ishlab chiqish dolzarb hisoblanadi. Ushbu ishning asosiy maqsadi — zamonaviy zararli dasturlarni (ma’lum va noma’lum) real vaqt rejimida aniqlash, tahlil qilish va tasniflash imkoniyatlarini kengaytirishdir.

II. Asosiy tushunchalar

Zamonaviy zararli dasturlarni aniqlash va tahlil qilishda tezkor javob beruvchi, real vaqt rejimida ishlaydigan va avtomatlashtirilgan kiberxavfsizlik yechimlarini yaratish uchun, avvalo, mavjud asosiy yondashuvlarni va kiberhujumchilar tomonidan qo‘llaniladigan zararli dasturlarni yashirish texnikalarini chuqur tushunish zarur.

Kiberxavfsizlikning asosiy sohalari quyidagilardan iborat:

- hujumlarni aniqlash va oldini olish (Intrusion Detection/Prevention)
- raqamli kriminalistika (Digital Forensics),
- tahdid razvedkasi (Cyber Threat Intelligence),
- kiberxavfsizlik analitikasi (Cybersecurity Analytics),
- zararli dasturlarni aniqlash va tahlil qilish (Malware Detection/Analysis).



3-rasmda Kiberxavfsizlikning asosiy sohalar

Kiberxavfsizlik analitikasi (Cyber Security Analytics – CSA). Kiberxavfsizlik analitikasi — bu proaktiv yondashuv bo‘lib, u ma’lumotlarni yig‘ish, birlashtirish, bog‘lash va tahlil qilish orqali kiberxavflar va zaifliklarni hujum sodir bo‘lishidan oldin aniqlash, tahlil qilish va zararsizlantirishga xizmat qiladi.

CSA quyidagi tahdidlarga qarshi qo‘llaniladi: ijtimoiy muhandislik, ilg‘or doimiy tahdidlar (APT – Advanced Persistent Threats), zamonaviy zararli dasturlar, DDoS hujumlar, kuchsiz autentifikatsiya ma’lumotlari.

Tahdid razvedkasi (Cyber Threat Intelligence – CTI). Tahdid razvedkasi — bu razvedka usullariga asoslangan fan bo‘lib, kiberxavflarga oid barcha ma’lumotlarni yig‘ish, tuzish va tahlil qilish orqali kiberhujumchilar xaritasini yaratishga hamda tahdidlar tendensiyalarini aniqlashga qaratilgan.

CTI uch asosiy turga bo‘linadi: strategik tahdid razvedkasi, taktik tahdid razvedkasi, operativ tahdid razvedkasi.

CTI hayotiy sikli quyidagi bosqichlardan iborat:

yo‘naltirish → yig‘ish → qayta ishlash → tahlil → tarqatish → qayta aloqa

Raqamli kriminalistika (Digital Forensics –

© Elshod Haydarov

DF). Raqamli kriminalistika — bu kiberjinoyatlar bilan bog'liq raqamli qurilmalardagi dalillarni tiklash va tergov qilishga qaratilgan kriminalistika sohasi.

Hujumlarni aniqlash va oldini olish tizimlari (IDS/IPS)

IDS/IPS tizimlari tarmoqni doimiy ravishda kuzatib boradi va potensial hujumlarni aniqlaydi. Ular: hodisalarni jurnalga yozadi, zararli trafikni bloklaydi, ulanishlarni uzadi, kelajakdagi hujumlarni oldini olish uchun avtomatik moslashadi.

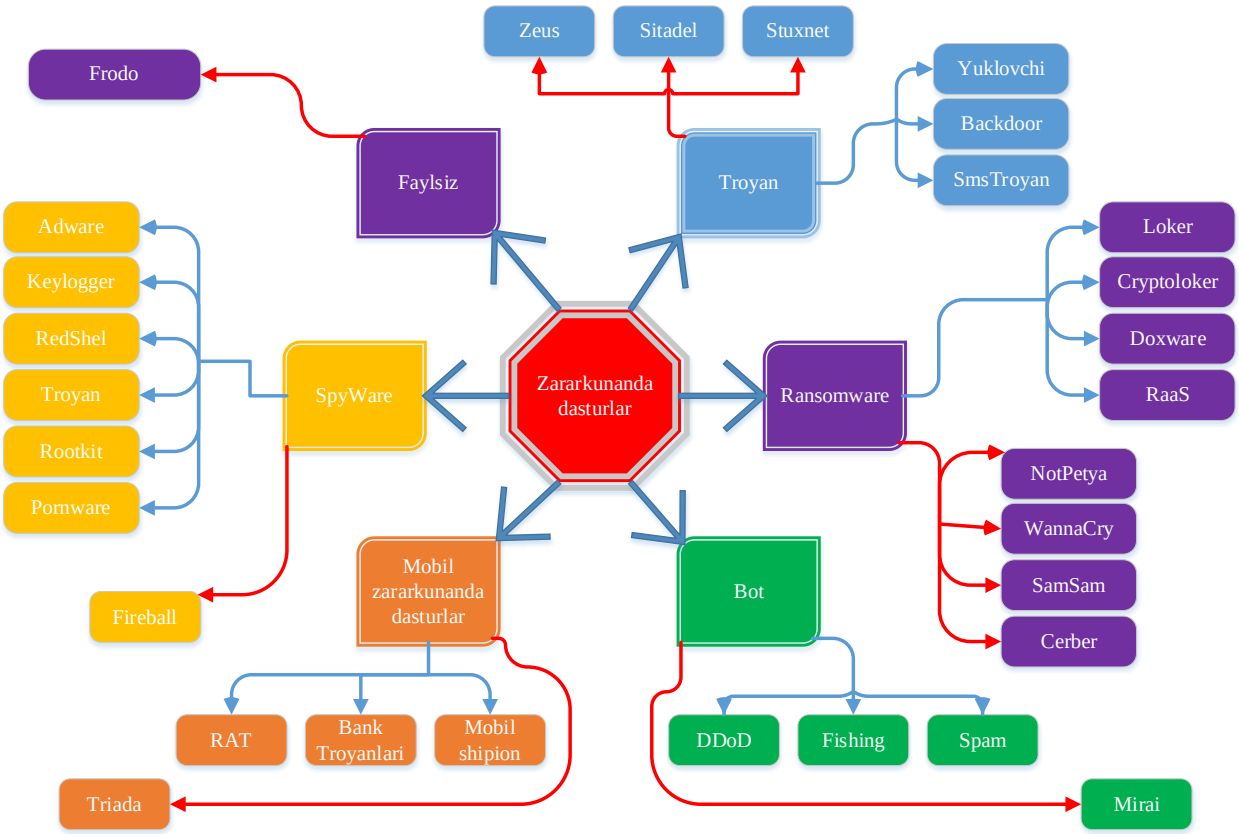
IDS/IPS turlari: tarmoq asosidagi IDS/IPS, xost asosidagi IDS/IPS, tarmoq xatti-harakatlarini tahlil qilish, simsiz tarmoq IDS/IPS.

Zararli dasturlarni aniqlash va tahlil qilish. Bu jarayon zararli yoki istalmagan dasturlarni aniqlash, ularning funksiyalari va tizimga ta'sirini tahlil qilishni o'z ichiga oladi. Natijada: kompromatsiya indikatorlari (IOC) aniqlanadi, zaifliklar topiladi, hujum manbai aniqlanadi, kelajakdagi hujumlar oldindan bashorat qilinadi[5].

Zararli dasturlarni tasniflash. Zararli dasturlar — kompyuter tizimlari, qurilmalar yoki tarmoqlarning normal ishlashini buzish, o'zgartirish yoki yo'q qilishga mo'ljallangan dasturlar yoki dastur qismlaridir. Zararli dasturlar tarixi 1970-yillarga borib taqaladi. Dastlabki zararli dastur — Creeper — masofaviy tizimlarga modem orqali ulanib, "I'M THE CREEPER: CATCH ME IF YOU CAN" xabarini ko'rsatgan.

Bugungi kunda zararli dasturlar: yadroviy sentrifugalar tezligini o'zgartira oladi (Stuxnet, 2010), maxfiy ma'lumotlarni o'g'irlaydi (Flamer, 2012), sun'iy yo'ldoshlar orqali aloqa qiladi (Turla, 2015).

WannaCry (2017) tarixdagi eng yirik ransomware hujumlaridan biri bo'lib, 150 davlatda 230 000 dan ortiq kompyuterni zararlagan. U MS17-010 zaifligidan foydalangan. Shuningdek: Petya / NotPetya, SamSam, DarkSide (RaaS) kabi zamonaviy zararli dasturlar global miqyosda katta talafotlar keltirgan.



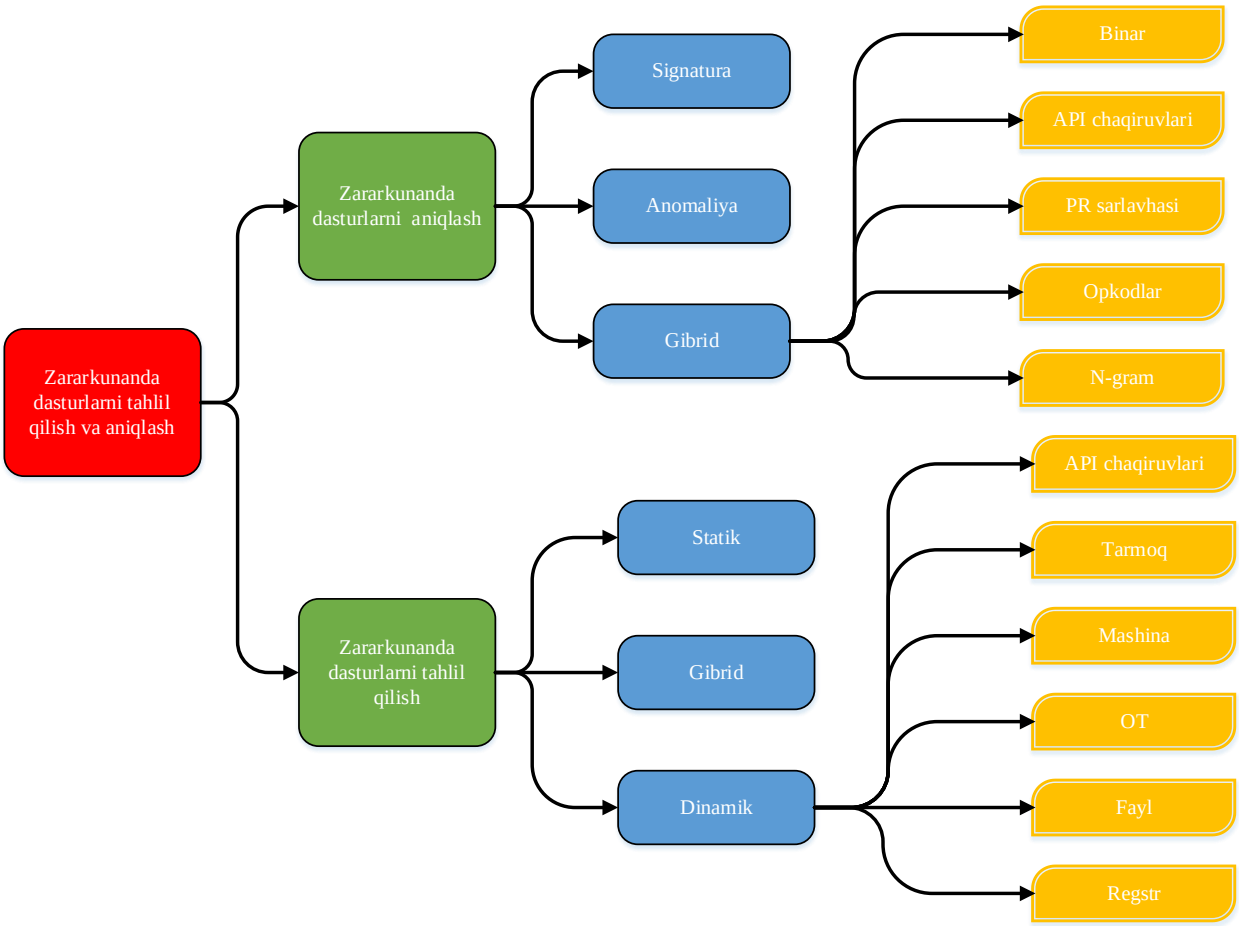
4-rasm. Zararli dasturlar tasnifi

© Elshod Haydarov

Zararli dasturlar maqsadi va ta’siriga ko‘ra tasniflanadi (4-rasm). Asosiy turlari:

- Viruslar – boshqa dasturlarga o‘zini joylashtirib tarqaladi;
- Troyanlar – foydali dastur ko‘rinishida yashirin zarar yetkazadi;
- Botnetlar – masofadan boshqariluvchi zararlangan qurilmalar tarmog‘i;
- Qurtlar (Worms) – tarmoq orqali o‘z-o‘zidan tarqaladi;
- Keyloggerlar – klaviatura bosimlarini yozib oladi;
- Spyware – foydalanuvchi ma’lumotlarini yashirin yig‘adi;
- Ransomware – fayllarni shifrlab, to‘lov talab qiladi.
- Ransomware tizimlarga quyidagi yo‘llar orqali kiradi:
- zero-day zaifliklar,
- fishing,
- botnetlar,
- masofaviy xizmatlar,
- elektron pochta.

An’anaviy zararli dasturlarni aniqlash va tahlil qilish. Zararli dasturlarni tahlil qilish — bajariluvchi fayllarni tekshirib, ularning xatti-harakatlari va funksiyalarini aniqlash jarayonidir[7]. Asosiy uch yo‘nalish mavjud (5-rasm):



5-rasm. Zararkunanda dastrularni aniqlash va tahlil qilish

Statik tahlil (Static Analysis). Zararli dastur ishga tushirilmasdan tahlil qilinadi. Afzalligi — tez va xavfsiz. Kamchiligi — murakkab va yashirilgan zararli dasturlarni aniqlay olmaydi. Misollar: PE Explorer, Androguard

Dinamik tahlil (Dynamic Analysis). Zararli dastur virtual muhitda ishga tushiriladi va real vaqtda xatti-harakatlari kuzatiladi. Afzalligi - aldash texnikalariga chidamli. Vositalar: Wireshark, TCPdump, DroidBox.

Gibrid tahlil (Hybrid Analysis) Statik va dinamik tahlilning kombinatsiyasi.

Zararkunanda dasturlarni aniqlash usullari:

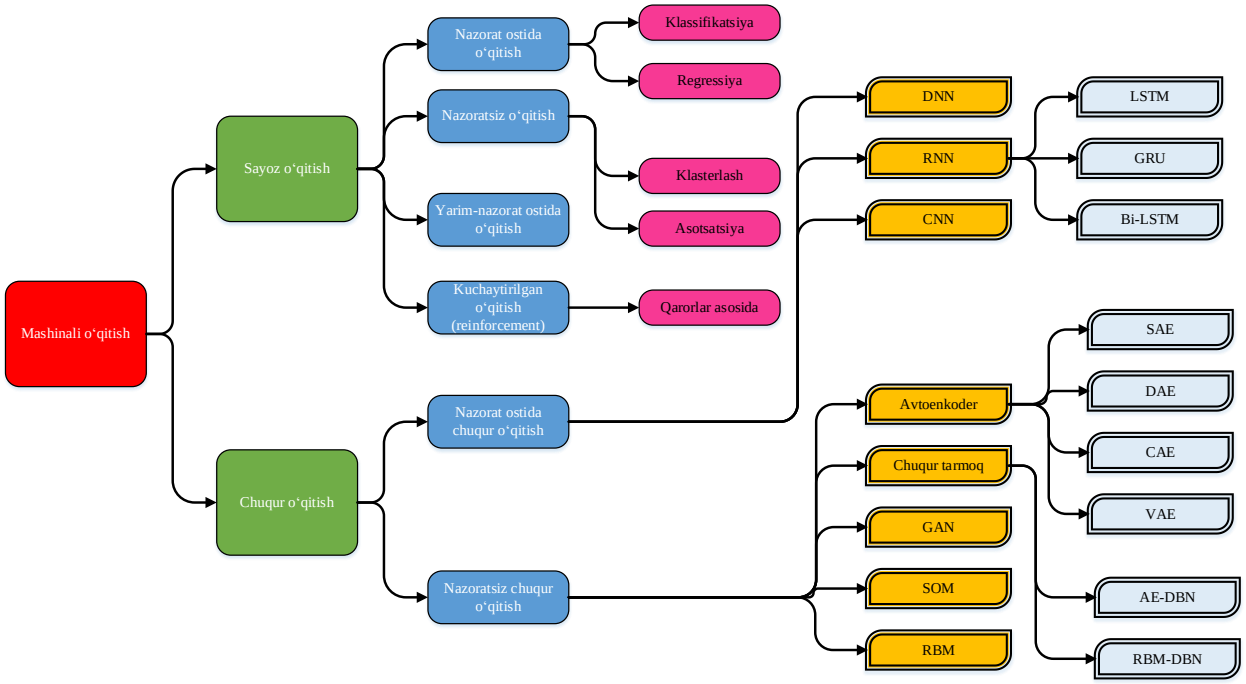
(cc) BY © Elshod Haydarov

Imzo asosida aniqlash (Signature-based Detection). Ma’lum zararli dasturlar uchun tezkor va samarali, ammo zero-day hujumlarda samarasiz.

Xatti-harakatga asoslangan aniqlash (Behavior-based Detection). Uch bosqichdan iborat: ma’lumot yig‘ish, xatti-harakat modelini yaratish, moslikni aniqlash. Zamonaviy zararli dasturlar yashirinish texnikalaridan foydalangani sababli, sun’iy intellektga asoslangan avtomatik tizimlar zarur bo‘lib qolmoqda.

Taklif etilgan yondashuv va metodologiya

Taklif etilgan yondashuv dinamik tahlil, xatti-harakatga asoslangan xususiyatlar va chuqur neyron tarmoqlar kombinatsiyasiga asoslanadi. Taklif etilgan tizimning asosiy maqsadi — ma’lum va noma’lum (zero-day) zararli dasturlarni real vaqt rejimiga yaqin sharoitda aniqlash va ularni tegishli zararli dastur oilalariga tasniflashdan iborat.



6-rasm. Kiberxavfsizlik muammolarini yechishda mashinali o‘qitish

Umumiy tizim arxitekturasi

Taklif etilgan tizim ko‘p qatlamli arxitekturaga ega bo‘lib, u quyidagi asosiy modullardan tashkil topgan (6-rasm):

1. Ma’lumotlarni yig‘ish moduli (Data Acquisition Module)
2. Dinamik tahlil moduli (Dynamic Analysis Module)
3. Xususiyatlarni ajratib olish moduli (Feature Extraction Module)
4. Chuqur o‘rganish moduli (Deep Learning Module)
5. Aniqlash va tasniflash moduli (Detection and Classification Module)

Ushbu modullar ketma-ket va o‘zaro integratsiyalashgan holda ishlaydi.

Ma’lumotlarni yig‘ish va dinamik tahlil. Zararli dasturlarni aniqlashda dinamik tahlil muhim rol o‘ynaydi, chunki zamonaviy zararli dasturlar statik tahlildan qochish uchun murakkab yashirinish texnikalaridan foydalanadi.

Taklif etilgan tizimda: zararli va zararli bo‘lmagan (benign) ilovalar, izolyatsiyalangan virtual muhitda (sandbox) ishga tushiriladi, ularning real vaqt rejimidagi xatti-harakatlari kuzatiladi[8].

Dinamik tahlil jarayonida quyidagi xatti-harakatlar qayd etiladi: tizim chaqiruvlari (system calls), fayl tizimi faoliyati, tarmoq trafiklari, registr (registry) o‘zgarishlari, API chaqiruvlari, jarayonlararo aloqalar. Ushbu yondashuv zararli

© Elshod Haydarov

dastur ishga tushirilgandan keyin namoyon bo‘ladigan yashirin faoliyatni aniqlash imkonini beradi.

Xususiyatlarni ajratib olish (Feature Extraction) Dinamik tahlil natijasida olingan dastlabki ma’lumotlar (raw data) bevosita o‘rganish uchun yaroqsiz bo‘lgani sababli, ular xususiyatlar vektoriga aylantiriladi.

Taklif etilgan tizimda xatti-harakatga asoslangan xususiyatlar quyidagi toifalarga ajratiladi: tizim chaqiruvlari ketma-ketligi, tarmoq paketlarining statistik ko‘rsatkichlari, fayl operatsiyalari chastotasi, xotira va resurslardan foydalanish darajasi, API chaqiruvlarining vaqt bo‘yicha taqsimoti[9].

Har bir ilova uchun ushbu xususiyatlar raqamli vektor ko‘rinishida ifodalanadi va chuqur o‘rganish modeliga uzatiladi.

Odatiy holda CNN (Convolutional Neural Network) tasvirlarni aniqlash uchun ishlatiladi. Maqolada esa zararli dasturlarni tasniflash uchun 1 o‘lchovli CNN (1D CNN) modelidan foydalanildi. 1D CNN 2D yoki 3D CNN bilan ishlash prinsipida bir xil tarzda ishlaydi. Ushbu modelni tanlashning sababi — uning yuqori ishlash samaradorligi va o‘rganish sur’ati bo‘ldi. 1D CNN modelini ishlab chiqish jarayonida yanada yaxshi natijalarga erishish uchun ayrim parametr sozlamalari o‘zgartirildi[10].

7-rasmda ikki toifadagi tasniflash uchun 1D CNN asosidagi model arxitekturasi ko‘rsatilgan. Ma’lumotlar to‘plamini (o‘qitish va baholash ma’lumotlarini) NumPy vektorlariga uchta o‘zgaruvchi (×1, ×2, ×3) bo‘yicha aylantirildi: ×1 — kuzatuvlar soni, ×2 — tadqiqotdagi o‘zgaruvchilar soni, ×3 esa 1 ga teng bo‘lgan boshlang‘ich miqdor.

Model quyidagi qatlamlardan tashkil topgan: bir o‘lchovli konvolyutsion qatlamlar, bunda modelning dastlabki qatlamlari kirish ma’lumotlarining xususiyatlarini ifodalaydi va bog‘lovchi qatlamlar, bunda modelning oxirgi qatlamlari chiqishni ifodalaydi.

Model arxitekturasi quyidagilarni o‘z ichiga oladi:

- kirish (input) qatlami,
- bir nechta yashirin (hidden) qatlamlar,
- chiqish (output) qatlami.
- Har bir yashirin qatlamda:
- og‘irlik koeffitsiyentlari (weights),
- siljish (bias),
- faollashtirish funksiyalari (ReLU, Softmax) qo‘llaniladi.
- Modelni o‘qitish jarayonida:
- orqaga qaytish (backpropagation) algoritmi,
- gradient tushish (gradient descent) usuli ishlatiladi.
- Chiqish qatlami zararli dastur namunalarini quyidagi sinflarga ajratadi:
- adware,
- radware,
- rootkit,
- SMS malware,
- ransomware,
- benign (zararsiz).
- O‘qitish va testlash jarayoni
- Modelni o‘qitish uchun:
- real dunyo zararli dastur namunalaridan tashkil topgan
- muvozanatlangan ma’lumotlar to‘plami ishlatiladi.
- Ma’lumotlar to‘plami:
- o‘qitish (training),
- tekshirish (validation),
- testlash (testing) qismlariga ajratiladi.

1-jadval.

Ma’lumotlar to‘plamining ma’lumotlar taqsimoti

Klassifikat-siya toifasi	Sinflar	O‘qitiluvchi to‘plam	Sinov to‘plami
Multiple	Benign	49767	14880
	Adware	5770	1341
	Ransomware	62471	28220

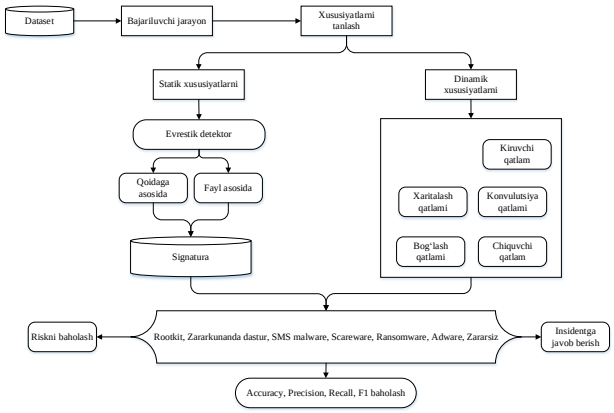
© Elshod Haydarov

	Scareware	13646	3930
	SMS Malware	255487	72816
	Rootkit	79115	21715

Modelni baholashda quyidagi mezonlar qo‘llaniladi:

- aniqlik (Accuracy),
- sezgirlik (Recall),
- aniqlik darajasi (Precision),
- F1-o‘lchov,
- yolg‘on ijobiy natijalar (False Positive Rate).

Ushbu yondashuv modelning real vaqt rejimidagi samaradorligini va umumlashuv qobiliyatini baholash imkonini beradi.



7-rasm. CNN asosidagi tizim arxitekturasi

Taklif etilgan yondashuvning afzalliklari

Taklif etilgan yondashuv quyidagi afzalliklarga ega:

- zero-day zararli dasturlarni aniqlash imkoniyati;
- statik tahlil cheklovlaridan mustaqillik;
- real vaqtga yaqin aniqlash;
- yuqori aniqlik va past yolg‘on ogohlantirish darajasi;
- kengaytiriladigan va moslashuvchan arxitektura.

III. Tajriba natijalari va muhokama

Tajribalar natijalari taklif etilgan yondashuvning aniqlik, barqarorlik va real vaqtga yaqin ishlash qobiliyatini tasdiqlaydi. Tajribalar izolyatsiyalangan virtual muhitda o‘tkaziladi. Barcha zararli va zararsiz namunalar oldindan konfiguratsiya qilingan sandbox muhitida ishga tushirildi.

Ma’lumotlar to‘plami quyidagilardan iborat:

- zamonaviy zararli dasturlar namunalari,
- real dunyo hujum ssenariylariga mos keluvchi xatti-harakatlar,
- zararsiz ilovalar (normal tizim xatti-harakati).
- Zararli dasturlar quyidagi oilalarga ajratildi:
- Adware,
- Radware,
- Rootkit,
- SMS malware,
- Ransomware.

Ma’lumotlar to‘plami o‘qitish (70%), tekshirish (15%) va testlash (15%) qismlariga bo‘lindi. Bunday taqsimot modelning umumlashuv qobiliyatini baholash imkonini berdi. Tajriba natijalari shuni ko‘rsatdiki, taklif etilgan model barcha zararli dastur oilalari bo‘yicha yuqori aniqlikni namoyish etdi.

- Ransomware aniqlash darajasi eng yuqori bo‘lib, bu xatti-harakatga asoslangan yondashuvning shifrlash faoliyatini samarali aniqlay olishini ko‘rsatadi.
- Rootkit va SMS malware turlari ham yuqori aniqlik bilan tasniflandi.
- Adware va Radware turlari nisbatan murakkab bo‘lishiga qaramay, model ularni ishonchli aniqlay oldi.

Modelning umumiy aniqlik ko‘rsatkichi an’anaviy mashinali o‘qitish usullariga nisbatan sezilarli darajada yuqori bo‘ldi.

Taklif etilgan yondashuv quyidagi an’anaviy modellar bilan taqqoslandi:

- Decision Tree (DT),
- Random Forest (RF),
- Support Vector Machine (SVM),
- statik chuqur o‘rganish modellar.

(cc) BY © Elshod Haydarov

Taqqoslash natijalari shuni ko‘rsatdiki:

- an’anaviy ML modellar zero-day zararli dasturlarni aniqlashda past samaradorlik ko‘rsatdi;
- statik DL modellari murakkab texnikalariga qarshi zaif bo‘lib chiqdi;
- taklif etilgan dinamik + chuqur o‘qitish yondashuvi barcha mezonlar bo‘yicha ustunlikka ega bo‘ldi.

Xususan, False Positive Rate sezilarli darajada kamaydi, bu esa tizimning amaliy qo‘llanilishi uchun muhim omil hisoblanadi.

Tadqiqotdan quyidagi xulosalarni chiqarish imkonini berdi:

- Dinamik xatti-harakatga asoslangan tahlil yashirilgan zararli dasturlarni aniqlashda samaraliroq;
- Chuqur o‘qitish murakkab va chiziqli bo‘lmagan bog‘lanishlarni avtomatik o‘rganadi;
- Taklif etilgan model real vaqt rejimiga yaqin ishlashga mos;
- Model yangi va noma’lum zararli dasturlarga nisbatan yuqori moslashuvchanlikka ega.

Biroq, tizimning asosiy cheklovi — hisoblash resurslariga bo‘lgan talabning yuqoriligi bo‘lib, bu yirik korporativ muhitlarda qo‘shimcha optimallashtirishni talab qiladi.

Ushbu tadqiqotda sun’iy intellektga asoslangan, dinamik xatti-harakatlarni tahlil qiluvchi zararli dasturlarni aniqlash va tasniflash tizimi taklif etildi. Tadqiqotning asosiy maqsadi — zamonaviy, murakkab va yashirinish texnikalaridan foydalanadigan zararli dasturlarni real vaqtga yaqin sharoitda aniqlash imkoniyatlarini kengaytirishdan iborat bo‘ldi.

Taklif etilgan yondashuv dinamik tahlil, xatti-harakatga asoslangan xususiyatlar va chuqur o‘rganish modellarini birlashtirish orqali an’anaviy statik va signatura asosidagi aniqlash usullarining asosiy cheklovlarini bartaraf etadi. Ushbu tizim ma’lum va noma’lum (zero-day) zararli dasturlarni aniqlashda yuqori samaradorlikni namoyish etdi.

IV. Xulosa

Tajriba natijalari shuni ko‘rsatdiki, taklif etilgan model: yuqori aniqlik (Accuracy) ko‘rsatkichlariga ega; past yolg‘on ijobiy (False Positive) darajani ta’minlaydi; ransomware, rootkit, SMS malware, adware va radware kabi zararli dastur oilalarini ishonchli tasniflaydi; real vaqt rejimida ishlashga mos keladi.

Bundan tashqari, taqqoslash tahlillari taklif etilgan dinamik chuqur o‘rganish yondashuvi an’anaviy mashinali o‘qitish va statik chuqur o‘rganish modellariga nisbatan ustun ekanligini ko‘rsatdi. Ayniqsa, yashirilgan va murakkab xatti-harakatlarga ega zararli dasturlarni aniqlashda ushbu yondashuv sezilarli afzallik berdi. Shu bilan birga, tadqiqot davomida ba’zi cheklovlar ham aniqlandi. Xususan, dinamik tahlil va chuqur o‘rganish modellarining yuqori hisoblash resurslariga bo‘lgan talabi tizimni cheklangan resursli muhitlarda qo‘llashni murakkablashtirishi mumkin. Bundan tashqari, sandbox muhitida o‘tkaziladigan tahlillar ayrim ilg‘or zararli dasturlar tomonidan aniqlanishi ehtimoli ham mavjud.

Ushbu tadqiqot zamonaviy kiberxavfsizlik muammolaridan biri bo‘lgan zararli dasturlarni aniqlash va tasniflash masalasiga bag‘ishlangan bo‘lib, unda dinamik tahlil va chuqur o‘rganishga asoslangan kompleks yondashuv taklif etildi.

Tadqiqot davomida an’anaviy statik va imzo asosidagi aniqlash usullarining cheklovlari tahlil qilinib, ularning zero-day va yashirin texnikalardan foydalanuvchi zararli dasturlarga nisbatan past samaradorlikka ega ekanligi asoslab berildi.

Taklif etilgan metodologiya zararli dasturlarning real vaqtga yaqin sharoitda xatti-harakatlarini tahlil qilish, xususiyatlarni avtomatik ajratib olish va chuqur neyron tarmoqlar yordamida aniqlash va tasniflashni o‘z ichiga oladi. Ushbu yondashuv adware, radware, rootkit, SMS malware va ransomware kabi asosiy zararli dastur oilalarini aniqlashda yuqori aniqlikni ta’minladi.

Tajriba natijalari shuni ko‘rsatdiki, dinamik xatti-harakatga asoslangan chuqur o‘rganish modeli an’anaviy mashinali o‘qitish va statik chuqur o‘rganish usullariga nisbatan yuqori aniqlik, past yolg‘on ijobiy ko‘rsatkich va

© Elshod Haydarov

yaxshiroq umumlashuv qobiliyatiga ega. Bu esa taklif etilgan tizimning amaliy kiberxavfsizlik muhitida qo‘llanish imkoniyatlarini tasdiqlaydi.

Shu bilan birga, tadqiqot natijalari sun’iy intellektga asoslangan yondashuvlar kiberxavfsizlik sohasida zararli dasturlarga qarshi moslashuvchan, avtomatlashtirilgan va samarali himoya mexanizmlarini yaratish uchun istiqbolli ekanligini ko‘rsatdi. Kelgusida modelni optimallashtirish, resurs sarfini kamaytirish va kvant hisoblash hamda federativ o‘rganish kabi ilg‘or texnologiyalar bilan integratsiya qilish ilmiy tadqiqotlar uchun muhim yo‘nalish bo‘lib qoladi.

V. Adabiyotlar

1. Oz, H.; Aris, A.; Levi, A.; Uluagac, A.S. A survey on ransomware: Evolution, taxonomy, and defense solutions. ACM Comput. Surv. 2022, 54, 1–37.
2. Kaspersky Security Bulletin 2022. Statistics. Available online: https://securelist.com/ksb-2022-statistics/108129/.
3. Harley Malware: New Attack on Android Devices. Available online: https://infosecwriteups.com/harley-malware-new-attack on-android-devices-ae2c599c2217
4. Malware. Available online: https://www.av-test.org/en/statistics/malware/ (accessed on 16 October 2022).
5. Mohurle, S.; Patil, M. A brief study of WannaCry threat: Ransomware attack 2017. Int. J. Adv. Res. Comput. Sci. 2017, 8, 1938–1940.
6. Kraszewski, K. SamSam and the silent battle of Atlanta. In Proceedings of the IEEE 11th International Conference on Cyber Conflict, Tallinn, Estonia, 28–31 May 2019.
7. Catak, F.O.; Yazı, A.F.; Elezaj, O.; Ahmed, J. Deep learning based Sequential model for malware analysis using Windows exe API Calls. PeerJ Comput. Sci. 2020, 6, e285.
8. Karbab, E.B.; Debbabi, M. MalDy: Portable, data-driven malware detection using natural language processing and machine learning techniques on behavioral analysis reports. Digit. Investig. 2019, 28, S77–S87.
9. Rahul; Kedia, P.; Sarangi, S.; Monika. Analysis of machine learning models for malware detection. J. Discret. Math. Sci. Cryptogr. 2020, 23, 395–407.
10. Almashhadani, A.O.; Carlin, D.; Kaiiali, M.; Sezer, S. MFMCNS: A multi-feature and multi-classifier network-based system for ransomworm detection. Comput. Secur. 2022, 121, 102860.

© Elshod Haydarov