Date: 5th June-2026

ZAMONAVIY KIBERXAVFSIZLIK TIZIMLARIDA ZARARLI DASTURLAR TAHDIDI VA ULARNING TASNIFI

Abdullayev Xushnud Raxmatulla o‘g‘li
Axmatov Bekzod Nurali o‘g‘li
Saidov O‘lmasbek Azamatovich
Qo‘ldosheva Dilnavoz Baxodir qizi
Muhammad al-Xorazmiy nomidagi TATU talabalari

Annotation: Mazkur ishda zamonaviy kiberxavfsizlik tizimlarida uchraydigan zararli dasturlar (malware) tahdidi, ularning asosiy turlari va tasnifi o‘rganilgan. Tadqiqot davomida Windows operatsion tizimi muhitida keng tarqalgan troyanlar, josuslik dasturlari, ransomware, rootkit, worm, cryptominer, loader va backdoor kabi zararli dasturlar tahlil qilindi. Shuningdek, PE (Portable Executable) formatining tuzilishi hamda zararli dasturlarni aniqlashda foydalaniladigan statik, dinamik va gibrid tahlil usullari ko‘rib chiqildi. Ishda zamonaviy zararli dasturlarning aniqlashdan qochish mexanizmlari, obfuscation va packing texnologiyalari hamda an’anaviy imzo asosidagi aniqlash usullarining cheklovlari yoritilgan. Tadqiqot natijalari zararli dasturlarni aniqlashda xatti-harakatlarga asoslangan va sun’iy intellekt texnologiyalaridan foydalanishga asoslangan yondashuvlarning istiqbolli ekanligini ko‘rsatadi.

Kalit so‘zlar: Zararli dastur, malware, Windows xavfsizligi, PE format, Trojan, Spyware, Ransomware, Rootkit, Worm, Cryptominer, Backdoor, statik tahlil, dinamik tahlil, gibrid tahlil, sandbox, obfuscation, signature-based detection, kiberxavfsizlik, tahdidlarni aniqlash, sun’iy intellekt.

Raqamli texnologiyalarning jadal rivojlanishi bilan birga axborot xavfsizligiga bo‘lgan tahdidlar ham yanada murakkablashib bormoqda. Hozirgi kunda shaxsiy kompyuterlar, korporativ tarmoqlar, bulut hisoblash infratuzilmalari va sanoat boshqaruv tizimlari zararli dasturiy ta’minotning asosiy nishonlariga aylangan. Zararli dastur (malware - malicious software) deganda foydalanuvchi yoki tashkilot manfaatlariga zarar yetkazish maqsadida yaratilgan har qanday dasturiy ta’minot tushuniladi. Bunday dasturlar tizimga ruxsatsiz kirishni ta’minlash, shaxsiy ma’lumotlarni o‘g‘irlash, tizim resurslarini egallash yoki foydalanuvchi faoliyatini nazorat qilish kabi maqsadlarda qo‘llaniladi.

Windows operatsion tizimi dunyo bo‘yicha shaxsiy kompyuterlar va korporativ ish stantsiyalari bozorida yetakchi o‘rinni egallagan bo‘lib, bu holat uni zararli dastur ishlab chiquvchilarining asosiy maqsadiga aylantirgan. Statcounter ma’lumotlariga ko‘ra, Windows global desktop operatsion tizimlar bozorining 70% dan ortig‘ini tashkil etadi. Mazkur keng tarqalganlik, boy API ekotizimi va murakkab tizim arxitekturasi zararli dastur ishlab chiquvchilari uchun qulay muhit yaratadi. Turli tadqiqotlarga ko‘ra, Windows zararli dasturlari tobora murakkab aniqlashdan qochish usullarini qo‘llayotganligi kuzatilmoqda, bu esa an’anaviy imzo asosidagi aniqlash usullarining samaradorligini keskin kamaytirmoqda.

Windows muhitida zararli dasturlar asosan ikki turdagi fayl orqali tarqaladi: bajariladigan fayllar (.exe) va dinamik kutubxona fayllari (.dll). PE (Portable Executable) format - Windows operatsion tizimida bajariladigan fayllarning standart tuzilmasi bo‘lib, u zararli dasturlarni tahlil qilishda asosiy ob’ekt hisoblanadi. PE faylning sarlavhasi (header), bo‘limlari (sections), import jadvali va eksport jadvali zararli dasturlarni aniqlashda muhim ma’lumot manbalari bo‘lib xizmat qiladi.

Zararli dasturlarning turlari va ularning xususiyatlarini tizimli tushunish kiberxavfsizlik tizimlarini loyihalashda muhim ahamiyat kasb etadi. Quyidagi jadvalda Windows muhitidagi asosiy zararli dastur turlarining tasnifi keltirilgan:

1.1-jadval

Windows muhitidagi zararli dasturlar tasnifi

T/r	Zararli dastur turi	Asosiy xususiyati	Misol
1	Troyan (Trojan)	Qonuniy dastur sifatida ko‘rinib, yashirin zararli amallarni bajaradi	Emotet, TrickBot
2	Josuslik dasturi (Spyware)	Foydalanuvchi faoliyatini kuzatadi, klaviatura bosishlarini yozadi	Agent Tesla, RedLine
3	To‘lov talab qiluvchi dastur (Ransomware)	Fayllarni shifrlaydi va to‘lov talab qiladi	WannaCry, LockBit
4	Ildizkit (Rootkit)	Tizim yadrosiga kirib, o‘z faoliyatini yashiradi	ZeroAccess, Necurs
5	Tarmoq qurti (Worm)	Tarmoq orqali o‘z-o‘zini tarqatadi va ko‘payadi	Conficker, Blaster
6	Kriptomayner (Cryptominer)	Protsessor va GPU resurslarini kriptovalyuta qazish uchun ishlatadi	XMRig, WannaMine
7	Yuklovchi (Loader/Dropper)	Boshqa zararli dasturlarni tizimga yuklab o‘rnatadi	Smoke Loader, GuLoader
8	Backdoor	Masofaviy boshqaruv uchun yashirin kirish kanalini ochadi	Cobalt Strike, AsyncRAT

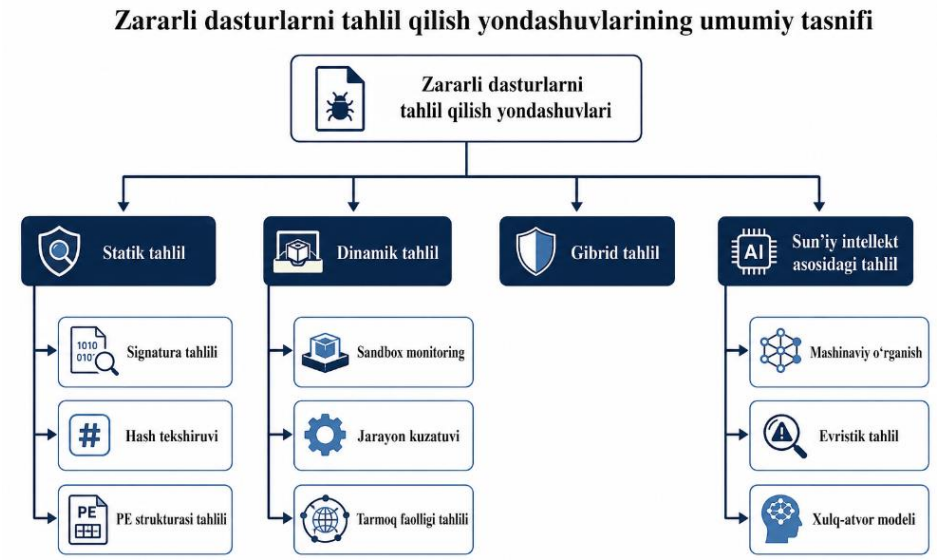
Windows muhitida zararli dasturlarning o‘ziga xos xususiyati shundaki, ular operatsion tizimning o‘z mexanizmlaridan - Windows API, PowerShell, WMI (Windows Management Instrumentation) va COM ob’ektlaridan - foydalanib zararli amallarni bajaradi. Bu holat zararli xatti-harakatni qonuniy tizim faoliyatidan ajratishni sezilarli darajada qiyinlashtiradi.

Zararli dasturlarni tasnif qilishning yana bir muhim jihatini ularning tahlil uslubi bo‘yicha ajratish tashkil etadi. Bu borada ikki asosiy yondashuv mavjud: statik tahlil va dinamik tahlil. Statik tahlilda dastur ishga tushirilmasdan uning kodi va tuzilishi o‘rganiladi - PE sarlavhasi, import jadvali, satrlar (strings), bayt naqshlari va disassembly natijasi tahlil qilinadi. Bu uslub tezroq amalga oshiriladi va kod qamrovini to‘liq ta’minlaydi, biroq kodni yashirish (obfuscation), paketlash (packing) va shifrlash usullarini qo‘llagan zararli dasturlarni aniqlashda qiyinchiliklar yuzaga keladi. Dinamik tahlilda esa dastur izolyatsiyalangan muhitda (sandbox) ishga tushirilib, uning xatti-harakati kuzatiladi:

fayl tizimiga, registrga, tarmoqqa va jarayonlarga qilingan murojaatlar qayd etiladi. Bu yondashuv obfuscation usullariga nisbatan barqarorroq, ammo qurilma resurslarini ko‘proq talab qiladi va murakkab zararli dasturlarning sandbox muhitini aniqlash qobiliyati tufayli cheklovlarga ega.

Gibrid tahlil uslubi ushbu ikki yondashuvning afzalliklarini birlashtirib, kiberxavfsizlik guruhiga ikkala usuldan eng yaxshi natijalarni olish imkonini beradi. Masalan, dinamik tahlil vaqtida zararli kod xotiraga o‘zgartirishlar kiritganda, tizim bu o‘zgarishlarni aniqlab, xotira tasvirida qo‘shimcha statik tahlil o‘tkazishi mumkin.

Zamonaviy zararli dasturlarning muhim xususiyati - ularning aniqlashdan qochish qobiliyatidir. Imzoga asoslangan aniqlash usullari (signature-based detection) uzoq vaqt davomida asosiy himoya vositasi bo‘lib kelgan. Ushbu usulda ma’lum zararli dasturlarning bayt naqshi (imzosi) ma’lumotlar bazasida saqlanadi va yangi fayllar shu bazaga taqqoslanadi. Ammo bu yondashuv yangi va o‘zgartirilgan zararli dasturlarni aniqlashda samarasiz bo‘lib qolmoqda, chunki zararli dastur ishlab chiquvchilari faqat bir nechta baytni o‘zgartirib yoki faylni qayta ishlovchi vositalar orqali qayta ishlab, imzolar bazasini aylanib o‘tishi mumkin.



1.1-rasm. Zararli dasturlarni tahlil qilish yondashuvlarining umumiy tasnifi

Zararli dasturlarning rivojlanishi natijasida yuzaga kelgan murakkab tahdid manzarasi kiberxavfsizlik sohasida yangi, adaptiv aniqlash usullarini ishlab chiqishni taqozo etmoqda. Bunday usullar faqat ma’lum imzolarga tayanmay, balki dasturlarning xatti-harakati va tuzilmasidagi naqshlarni tahlil qilib, noma’lum tahdidlarni ham aniqlash imkonini berishi lozim.

Xulosa

Raqamli texnologiyalarning rivojlanishi va axborot tizimlarining keng miqyosda qo‘llanilishi natijasida zararli dasturlar zamonaviy kiberxavfsizlikning eng jiddiy tahdidlaridan biriga aylandi. Zararli dasturlar foydalanuvchilarning maxfiy ma’lumotlarini o‘g‘irlash, tizim resurslarini noqonuniy ishlatish, xizmatlarning uzilishiga sabab bo‘lish hamda tashkilotlarga katta moliyaviy zarar yetkazish

imkoniyatiga ega. Ayniqsa, Windows operatsion tizimining keng tarqalganligi uni kiberjinoyatchilar uchun asosiy nishonlardan biriga aylantirmoqda.

FOYDALANILGAN ADABIYOTLAR:

1. Computer Security: Principles and Practice. Pearson Education, 5th Edition, 2023.
2. Network Security Essentials. Pearson Education, 7th Edition, 2023.
3. National Institute of Standards and Technology. Computer Security Log Management Guide (SP 800-92). Gaithersburg, USA.
4. National Institute of Standards and Technology. Cybersecurity Framework Documentation.
5. Microsoft Learn - Windows Event Logs Documentation
6. Microsoft Learn - Event Viewer Overview
7. Guide to Computer Forensics and Investigations. Cengage Learning, 7th Edition, 2022.
8. Digital Forensics and Incident Response. Packt Publishing, 2020.
9. Practical SIEM Implementation. Packt Publishing, 2018.
10. The Practice of Network Security Monitoring. No Starch Press, 2013.