ZARARLI DASTURLARNI TAHLIL QILISH VOSITALARI TAVSIFI

Dilshoda Qurbonaliyeva
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
dilshodavaliyevna@gmail.com

Annotatsiya.

Ushbu maqolada zararli dasturlarni aniqlash xususiyatlari o‘rganilgan. Zararli dasturlarni aniqlashda statik va dinamik usullardan foydalanish avzalliklari ularni amalga oshirish bosqichlari to‘liq ko‘rib chiqilgan. Tahlil jarayonida qo‘llaniluvchi vositalarning turlari va tavsifi keltirilgan.

Kalit so'zlar: Zararli dasturlar, statik tahlil, dinamik tahlil, fayl identifikatsiyasi, fayl strukturasi, fayl imzosi, PeView, PEid, ProkMon, Wireshark.

Аннотация.

В этой статье изучаются характеристики обнаружения вредоносных программ.Рассматриваются преимущества использования статических и динамических методов для их выявления. Приведено описание инструментов, применяемых в процессе анализа.

Ключевые слова: Вредоносные программы, статический анализ, динамический анализ, идентификация файлов, структура файлов, файл-имя, PeView, PEid, ProkMon, Wireshark.

Annotation.

This article examines the characteristics of malware detection. The advantages of using static and dynamic methods for detecting malware are discussed. A description of the tools used in the analysis process is provided.

Keywords: Malicious software, static analysis, dynamic analysis, file identification, file structure, file signature, PeView, PEid, ProkMon, Wireshark.

Kirish

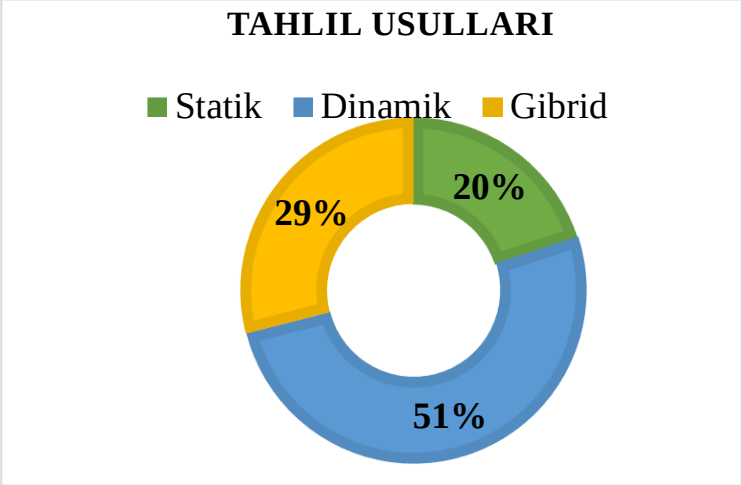
Zararli dastur - bu kompyuter, server, mijoz yoki kompyuter tarmog‘ini buzish, shaxsiy ma’lumotlarni o‘g‘irlash, ma’lumotlar yoki tizimlarga ruxsatsiz kirish, foydalanuvchining kompyuter xavfsizligi va maxfiyligi to‘siqlarini buzib kirgan holda foydalanuvchilarni ma’lumotlarga kirishdan mahrum qiladigan har qanday dasturiy ta’minotdir [1]. Zararli dastur ba’zan hukumat yoki korporativ veb-saytlarga qarshi himoyalangan ma’lumotlarni to‘plash yoki umuman ularning faoliyatini to‘xtatish uchun keng qo‘llaniladi. Biroq, zararli dastur shaxsiy

identifikatsiya raqamlari yoki rekvizitlari, bank yoki kredit karta raqamlari va parollar kabi ma’lumotlarni olish uchun jismoniy shaxslarga qarshi ishlatilishi mumkin.

Statik tahlil

Zararli dastur namunalari ularni aniqlash uchun ishlatilishi mumkin bo‘lgan xususiyatlarni olish uchun tahlil qilinadi. Zararli dasturlarni tahlil qilishning ikkita asosiy usuli mavjud: statik, dinamik va gibrid tahlillar, ular quyida tavsiflanadi.

1-rasm. Zararli dasturlarni tahlil qilish usullarining foydalanish ko‘rsatgichi



*Statik tahlil*da xususiyatlar zararli dastur namunalarini ishga tushirmasdan o‘rganiladi. Har xil statik xususiyatlar tahlildan so‘ng chiqariladi, masalan, xesh qiymati, N-grammlar, opkodlar, satrlar va PE sarlavhasi ma’lumotlari. Bu xususiyatlardan foydalangan holda zararli dasturlarni aniqlash dasturlari ishlab chiqilgan (antivirus, IDS va boshqalar) [1]. Zararli dastur namunasini kod darajasida tekshirish uchun bajariladigan zararli dasturlarning fayllari assembler tili kodiga va qismlarga ajratiladi [2].

Buning uchun ikkilik fayllarni yig‘ish kodiga aylantirish uchun Ollydbg, IDA Pro, cap-stone va WinDbg demontajlari kabi eng ko‘p ishlatiladigan tuzatuvchi va disassemblerlardan foydalaniladi [3]. Assambleya kodi faylning bajarilish oqimini, tuzilmasini yoki zararli faoliyat modelini topish uchun tekshiriladi, ulardan yangi yoki mavjud zararli dasturlarni aniqlash uchun foydalanish mumkin.

Zararli dasturlarning statik tahlilini amalga oshirish zararli fayllar yoki dasturlarning xarakteristikalari va tuzilishini ularni bajarmasdan tekshirishni o‘z ichiga oladi. Bu yerda statik tahlil bilan bog‘liq bosqichlarning umumiy ko‘rinishi:

Fayl identifikatsiyasi: Tahlil qilishimiz uchun shubhali fayl yoki dastur aniqlanadi. Bu bajariladigan fayl, skript, hujjat yoki zararli kodni o‘z ichiga olishi mumkin bo‘lgan boshqa turdagi fayl bo‘lishi mumkin.

Fayllar to‘plami: fayl haqida uning nomi, hajmi va manbasi kabi tegishli ma’lumotlar to‘planadi. Tahlil paytida zararli dastur tasodifiy ishga tushishining oldini olish uchun toza va izolyatsiya qilingan muhitga ega ekanligiga ishonch hosil qilinadi. (1- rasm).

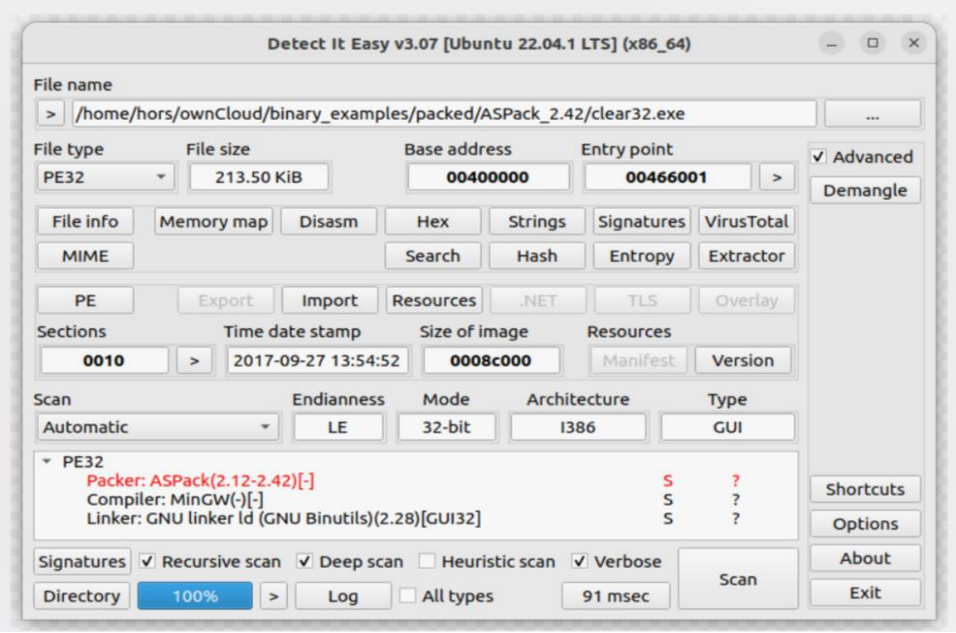
Fayl metadata tahlili: fayldan metadata, jumladan, fayl sarlavhalari, vaqt belgilari, versiya ma’lumotlari va raqamli imzolarni ajratib olinadi. Ushbu metama’lumotlar faylning kelib chiqishi va potentsial zararli niyatlari haqida qimmatli ma’lumotlarni taqdim etishi mumkin.

Statik kod tahlili: Turli xil vositalar va usullardan foydalangan holda fayl kodi tekshiriladi. Bu ularning yig‘ilishi yoki manba kodini tahlil qilish uchun bajariladigan fayllarni qismlarga ajratish yoki dekompilyatsiya qilishni o‘z ichiga olishi mumkin. Shubhali yoki tushunarsiz kodlar, kodlangan URL yoki IP manzillari, shifrlash tartiblari va zararli harakatning boshqa ko‘rsatkichlari qidiriladi [3].

String tahlili: fayldan satrlarni ajratib olinadi va ularni fayl manzillari, ro‘yxatga olish kitobi kalitlari, API chaqiruvlari va buyruq va boshqaruv server manzillari kabi ma’lum zararli

namunalar uchun tahlil qilinadi. Shubhali xatti-harakatlarni yashirish uchun ishlatilishi mumkin bo‘lgan kodlangan yoki shifrlangan satrlarga e’tibor beriladi.

Statik fayl strukturasini tahlil qilish: fayl tuzilishini tahlil qilinadi, masalan, uning bo‘limlari, importi, eksporti va manba ma’lumotlari kabi tuzilishlar tahlil qilinadi. Buzg‘unchilik yoki zararli niyatni ko‘rsatishi mumkin bo‘lgan oddiy fayl tuzilmalaridan anomaliyalar yoki og‘ishlar qidiriladi.



2 - rasm. Detect it Easy dasturi yordamida aniqlangan file ma’lumotlari

Fayl imzosi tahlili: Fayl imzosi yoki xesh qiymatini tahdid razvedkasi ma’lumotlar bazalarida ma’lum bo‘lgan zararli dastur imzolari bilan solishtiriladi. Bu oldindan aniqlangan zararli dasturlarni va ma’lum bo‘lgan zararli fayllarni aniqlashga yordam beradi.

Xulq-atvor tahlili (ixtiyoriy): Statik tahlil zararli dasturning kodi va tuzilishini o‘rganishga qaratilgan bo‘lsa, xatti-harakatlar tahlili zararli dasturning boshqariladigan muhitda harakatlarini kuzatishni o‘z ichiga oladi. Bu odatda dinamik tahlil deb hisoblansa-da, xulq-atvor tahlilining ba’zi jihatlarini statik tahlil natijalaridan xulosa qilish mumkin [4].

Hujjatlar va hisobotlar: Aniqlangan ma’lumotlar, shu jumladan har qanday shubhali yoki zararli ko‘rsatkichlar, qo‘llanilgan tahlil metodologiyalar hamda yumshatish yoki qo‘shimcha tekshirish bo‘yicha tavsiyalar hujjatlashtiriladi. Tahlil natijalarini jamlagan batafsil hisobot tayyorlanadi va uni tegishli manfaatdor tomonlar yoki kiberxavfsizlik guruhlariga yuboriladi.

Ushbu bosqichlarni bajarish orqali zararli dasturlarning xususiyatlarini, xatti-harakatlarini va tizimlar yoki tarmoqlarga potentsial ta’sirini aniqlash uchun to‘liq statik tahlilni o‘tkazishimiz mumkin. Statik tahlil zararli dasturlarni tahlil qilishda muhim birinchi qadam bo‘lib xizmat qiladi va tashkilotlarga o‘zgaruvchan tahdidlarga qarshi kiberxavfsizlik himoyasini kuchaytirishga yordam beradi.

1-jadval

Statik tahlil vositalari

Statik tahlil vositalari nomi	Tavsif
PeView	Ushbu vosita Windows bajariladigan fayllarning to‘liq sarlavhasi ma’lumotlarini taqdim etadi. Har bir bajariladigan fayl turli xil ma’lumotlardan, jumladan ma’lumotlardan, kodlardan, faylning metama’lumotlaridan iborat. Zararli dasturlarni tahlil qilishda PE (Portable Executable) sarlavhasi zararli ma’lumotlari va zararli dasturlarni tasniflash uchun ishlatiladi.
PEid	Hozirgi vaqtda zararli dastur ishlab chiquvchisi zararli dasturlarning haqiqiy kodini yashirish uchun tahlilga qarshi vositalardan

	foydalanadi. Paketlangan zararli dasturlarni aniqlash uchun PEid dan foydalanish mumkin. Ushbu dasturiy ta’minot zararli dasturni aniqlash uchun ishlatiladi, agar "ha" bo‘lsa, unda paketlash vositasidan (masalan, UPX, NSPACK va boshqalar) foydalanadi.
PsFile	Ushbu yordamchi dastur tizimda ochilgan fayllar haqidagi ma’lumotlarni ko‘rsatadi. Kompyuter tizimining masofadan turib boshqarilishini tahlil qilish juda foydali. Mahalliy kompyuterda ochilgan fayllar haqidagi ma’lumotlarni masofaviy kompyuter orqali berish imkoniyati mavjud.
IOC Finder	XOQ (Kompromis ko‘rsatkichi). Ushbu vosita buzilgan tizimlar haqida ma’lumot beradi. U MS Word yoki HTML formatida ma’lum xostning tizimi va qurilmadan foydalanishi haqida ma’lumot beruvchi hisobotni ishlab chiqadi. Ushbu hisobot tizim xavfsizligi ko‘rsatkichlarini bilish uchun tahlil qilinadi.

Dinamik tahlil

Zararli dasturlarning dinamik tahlili zararli dasturiy ta’minotning harakatlarini va tizimga potentsial ta’sirini tushunish uchun boshqariladigan muhitda, odatda sandbox yoki virtual mashinada zararli dasturning harakatini kuzatishni o‘z ichiga oladi [4]. Zararli dasturlarni dinamik tahlil qilish bilan bog‘liq qadamlarning umumiy ko‘rinishi:

O‘rnatish muhiti: Zararli dastur xost tizimiga ta'sir qilmasdan xavfsiz tarzda bajarilishi mumkin bo‘lgan virtual mashina yoki sandbox kabi boshqariladigan muhit yaratiladi. Zararli dastur tarqalishining oldini olish uchun atrof-muhit tarmoqdan va maxfiy ma’lumotlardan ajratilganligiga ishonch hosil qilinadi.

Zararli dasturni ishga tushirish: Zararli dastur namunasini boshqariladigan muhitda ishga tushiriladi va real vaqt rejimida uning harakatini kuzatib borishimiz mumkin bo‘ladi. Bu zararli dasturni qo‘lda bajarish yoki avtomatlashtirilgan tahlil vositalaridan foydalanishni o‘z ichiga olishi mumkin.[5]

Xulq-atvor monitoringi: Zararli dastur bajarilayotganda uning xatti-harakatlari kuzatiladi va yozib olinadi. Fayl tizimini o‘zgartirish, ro‘yxatga olish kitobini o‘zgartirish, tarmoq aloqasi, jarayonni yaratish va imtiyozlarni oshirish yoki aniqlashdan qochish kabi harakatlarga e’tibor beriladi.

Tarmoq trafigini tahlil qilish: tashqi serverlar yoki buyruq va boshqaruv (C2) infratuzilmasi bilan aloqani aniqlash uchun zararli dastur tomonidan yaratilgan tarmoq trafigi kuzatib boriladi. Zararli dasturning aloqa usullarini tushunish uchun tarmoq protokollarini, domen nomlarini, IP manzillarini va ma’lumotlar yuklamalari tahlil qilinadi [5].

Xotira tahlili: zararli dastur artefaktlarini aniqlash uchun zararlangan tizimning xotira qoldiqlarini yoki oniy tasvirlarini oling va tahlil qilinadi. Xotira bo‘linmalaridan tegishli ma’lumotlarni ajratib olish va tahlil qilish uchun xotira kriminalistikasi vositalaridan foydalaniladi.

Kodni kiritish tahlili: Zararli dastur mavjudligini yashirish yoki qonuniy jarayonlarda zararli kodni ishga tushirish uchun kodni kiritish usullaridan foydalanishi aniqlanadi. Kod kiritish belgilarini aniqlash va uning tizim barqarorligi va xavfsizligiga ta'sirini tushunish uchun jarayon xotirasi va tizim chaqiruvlari tahlil qilinadi.

Zararli dasturiy ta’minotning dinamik imzolari: kuzatilgan xatti-harakatlar va tarmoq trafigi namunalari asosida dinamik zararli dastur imzolari yaratiladi. Ushbu imzolar boshqa tizimlar yoki tarmoqlarda real vaqtda shu kabi zararli dasturlarni aniqlash va bloklash uchun ishlatilishi mumkin.

Hujjatlar va hisobotlar: Kuzatilgan xatti-harakatlar, tarmoq ko‘rsatkichlari va zararli dastur tomonidan qo‘llaniladigan tahlilga qarshi usullar hujjatlashtiriladi. Dinamik tahlil natijalarini jamlagan batafsil hisobot tayyorlanadi va uni tegishli manfaatdor tomonlar yoki kiberxavfsizlik guruhlariga yuboriladi.

Dinamik tahlil zararli dasturlarning xatti-harakatlari va imkoniyatlari haqida qimmatli tushunchalarni beradi, bu esa tashkilotlarga uning tizimlar va tarmoqlarga ta'sirini tushunishga va samarali yumshatish strategiyalarini ishlab chiqishga imkon beradi. Ushbu qadamlarni bajarish orqali kiberxavfsizlik bo‘yicha mutaxassislar tahdidlarni aniqlash va ularga javob berish imkoniyatlarini oshirish uchun keng qamrovli dinamik tahlilni o‘tkazishlari mumkin.

2-jadval

Dinamik tahlil vositalari

Dinamik tahlil vositalari nomi	*Tavsif*
Process Explorer	Process Explorer - bu tizim monitori va vazifalarni boshqarish vositasi. U Windows vazifa menejeri kabi ishlaydi tizimda ishlaydigan jarayonlar haqida batafsil ma’lumot beradi.
ProcMon	ProcMon (jarayon monitori) ishlaydigan jarayonlar tomonidan bajariladigan harakatlarni yozib oladi. U har birini qamrab oladi fayl tizimlari operatsiyalari, ro‘yxatga olish kitobini o‘zgartirish, xotira ishlashi va tarmoq faoliyatining tizim chaqiruvlaribu o‘z ichiga oladi.
Wireshark, Tshark	Wireshark va Tshark tarmoq trafigini tahlil qilish uchun ishlatiladi. Ushbu vositalar funktsional imkoniyatlarga ega tizimdan tashqi dunyoga har bir kiruvchi va chiquvchi paketni ushlash imkonini beradi. Har xil turlari URL manzillari, port manzili va ma’lumotlar oqimi kabi tarmoq xususiyati qo‘lga kiritiladi, ular zararli dastur fayllarini tasniflash uchun qo‘shimcha o‘rganiladi .
TCPview	Bu Windows tarmoq dasturi bo‘lib, u barcha UDP va TCP so‘nggi nuqtalari haqidagi ma’lumotlarni ko‘rsatadigan tizim.
Regshot	Regshot vositasi bajarilgan namuna tomonidan ro‘yxatga olish kitobiga kiritilgan o‘zgarishlarni qayd qilish uchun ishlatiladi. Oldin va keyin zararli dastur namunasining bajarilishi, Oyna registrining holati saqlanadi. Ikkala shtat ham bajarilgan namunaviy fayl tomonidan qanday o‘zgarishlar amalga oshirilishini bilish uchun solishtirganda

Xulosa

Xulosa qilib shuni aytish mumkinki, maqolada keltirilgan statik va dinamik yondashuvlarni birlashtirgan holda, gibrid usul har bir texnikaning kuchli tomonlarini qo‘llash va ularning individual zaif tomonlarini yumshatishga qaratilgan. Bu keng qamrovli tahdidlarni, shu jumladan ma’lum va ilgari ko‘rilmagan zararli dasturlarni aniqlashga qodir bo‘lgan yanada mustahkam va moslashuvchan zararli dasturlarni aniqlash tizimiga olib keladi.

Foydalanilgan adabiyotlar

1. *Дилшода Курбаналиева*, 2023. “Tarmoq xujumlarini aniqlash vositalari tahlili”. Ж: Информатика и инженерные технологии.
2. Suhrobjon Bozorov, Nozima Akhmedova, Dilshoda Qurbonaliyeva and Kader Gultekin 2024. “Survey on honeypot: detection, countermeasures and future with ML”, AIP Conference Proceedings (ISSN:0094-243X; E-ISSN:1551-7616).
3. W. Han, J. Xue, Y. Wang, Z. Kong, MalDAE: Detecting and explaining malware based on correlation and fusion of static and dynamic charactristics, Comput. Secur. 83 (2019) 208-233, http://dx.doi.org/10.1016/j.cose.2019.02.007.
4. A. Damodaran, F.D. Troia, C.A. Visaggio, T.H. Austin, M. Stamp, A comparison of static, dynamic, and hybrid analysis for malware detection, J. Comput. Virol. Hacking Tech. 13 (1) (2017) 1-24, http://dx.doi.org/10.1007/s11416-015-0261-z.
5. AV-TEST, Malware statistics and trends report, AV-TEST, 2020, https://www.avtest.org/en/statistics/malware.
6. U.M.Yarlakabov Didactic Ways of Forming Students' Technical Thinking.- Eastern European Scientific Journal, 2018 - journale.auris-verlag.de

7. Sharipov Sanjar. Vocational orientation through the development of mathematical competences in the students of technical higher education institutions. CURRENT RESEARCH JOURNAL OF PEDAGOGICS. 3. No. 06 (2022). 58-64. https://doi.org/10.37547/pedagogics-crjp-03-06-10

8. Nadirova-Kazan, H. (2023, November). EXPLORING THE CONTENT OF MEDIA LITERACY: A COMPREHENSIVE REVIEW. In International Scientific and Current Research Conferences (pp. 107-110).

9. Mahkamov, S., Aynakulov, T., & Baratov, J. (2024). ANDROIDDA MODEL VIEW PRESENTER (MVP) ARXITEKTURASI. International Journal of scientific and Applied Research, 1(3), 199-202.

10. Ikrom Kulanov, Sneha Latha, Azizbek Uzakboyev, Shakhzoda Burkhanova. Effect of gyrotactic microorganisms on electrically conducting carreau nanofluid flow along an exponentially stretching surface in the presence of chemical reaction. Problems in the textile and light industry in the context of integration of science and industry and ways to solve them: ptlicisiws-2.4–5 may 2023.Namangan, Uzbekistan.AIP Conf. Proc. 3045, 030066 (2024). https://doi.org/10.1063/5.0197498

11. Sanjar Sobirovich Sharipov. IMPLEMENTATION OF SPECIAL AND GENERAL PROFESSIONAL INTEGRATION AS A PEDAGOGICAL PROBLEM Scientific Bulletin of Namangan State University.2020. 2-8. 364-370-p.