ZARARLI DASTURLAR TURLARI VA ULARNING ISHLASH MEXANIZMLARI: TAHLIL VA TASNIF

Ziyodullayev Ramziddin

Qarshi davlat texnika universiteti
Buxgalteriya yo'nalishi talabasi
DOI: 10.61587/mmit.tiue.uz.v1i1.413

Annotatsiya. Ushbu maqolada zararli dasturlar (malware) ning asosiy turlari, ularning ishlash mexanizmlari va tarqalish usullari ilmiy jihatdan tahlil qilingan. Viruslar, qurtlar (worm), troyan dasturlari, ransomware, spyware, adware, rootkit va botnet kabi zararli dastur turkumlari batafsil ko'rib chiqilgan. Har bir tur uchun texnik ishlash tamoyillari, tarqalish vektorlari, aniqlanish usullari va zamonaviy xavfsizlik mexanizmlari yoritilgan. Shuningdek, kiberhujumlarning global iqtisodiy zarari, Mirai, WannaCry, Stuxnet kabi real dunyo misollarida tahlil o'tkazilgan. Maqola axborot xavfsizligi sohasida ishlayotgan mutaxassislar, tadqiqotchilar va talabalar uchun mo'ljallangan bo'lib, zararli dasturlarning evolyutsiyasi va ularga qarshi kurashishning dolzarb usullarini qamrab olgan.

Kalit so'zlar: *zararli dasturlar, malware, virus, troyan, ransomware, spyware, rootkit, botnet, kibertahdid, axborot xavfsizligi, kiber hujum, tarqalish mexanizmi, antivirus, kriptovirus, social engineering.*

TYPES OF MALWARE AND THEIR OPERATING MECHANISMS: ANALYSIS AND CLASSIFICATION

Ziyodullayev Ramziddin

Karshi State Technical University
Student of Accounting

Abstract. This article provides a scientific analysis of the main types of malicious software (malware), their operating mechanisms, and methods of propagation. Categories such as viruses, worms, Trojan programs, ransomware, spyware, adware, rootkits, and botnets are examined in detail. For each type, the technical principles of operation, propagation vectors, detection methods, and modern security mechanisms are described. The global economic damage caused by cyberattacks is also analyzed through real-world examples such as Mirai, WannaCry, and Stuxnet. The article is intended for specialists, researchers, and students working in the field of information security and covers the evolution of malware and current methods of countering it.

Keywords: *malicious software, malware, virus, Trojan, ransomware, spyware, rootkit, botnet, cyber threat, information security, cyberattack, propagation mechanism, antivirus, cryptovirus, social engineering.*

KIRISH

Axborot texnologiyalarining jadal rivojlanishi bilan birga, raqamli muhitdagi tahdidlar ham misli ko'rilmagan darajada kuchaymoqda. Zararli dasturlar, ya'ni malware (inglizcha: malicious software) — bu foydalanuvchi ruxsatisiz tizimga kirib, ma'lumotlarni o'g'irlash, tizimni buzish, josuslik qilish yoki moliyaviy zarar yetkazish maqsadida yaratilgan dasturiy mahsulotlar majmuasidir (Symantec Corporation, 2019). Kiberjinoyatchilik sanoati bugungi kunda global iqtisodga yiliga 8 trillion AQSh dollaridan ortiq zarar yetkazmoqda (Cybersecurity Ventures, 2023).

Zararli dasturlarning tarixi 1971 yilga, ya'ni ARPANET tarmog'ida paydo bo'lgan 'Creeper' dasturiga borib taqaladi (Cohen, 1987). Keyinchalik 1988 yilda Robert Morris tomonidan yozilgan 'Morris Worm' birinchi keng tarqalgan tarmoq qurti sifatida tarixga kirdi va taxminan 6,000 dan ortiq kompyuterni ishdan chiqardi. Bugungi kunda esa AV-TEST institutining ma'lumotlariga ko'ra, har kuni 450,000 dan ortiq yangi zararli dastur namunasi aniqlanmoqda (AV-TEST Institute, 2024).

Ushbu maqolaning maqsadi — zararli dasturlarning asosiy turlarini tizimlashtirish, ularning texnik ishlash mexanizmlarini tahlil qilish va zamonaviy kibertahdidlarga qarshi kurashishning ilmiy asoslarini yoritishdan iborat. Tadqiqot metodologiyasi sifatida tizimli tahlil, taqqoslash va tasnif usullaridan foydalanilgan.

Zamonaviy axborot xavfsizligi adabiyotida zararli dasturlarni tasniflashning bir nechta yondashuvi mavjud. Kaspersky Lab tadqiqotchilarining tasniflashiga ko'ra, zararli dasturlar asosan o'z-o'zini tarqatish qobiliyati, maqsad va ishlash mexanizmi bo'yicha guruhlarga bo'linadi (Kaspersky Lab, 2022). Anderson (2020) esa zararli dasturlarni uch asosiy kategoriyaga ajratadi: infeksion kodlar (virus, qurt), yashirin kodlar (troyan, rootkit) va maqsadli kodlar (spyware, ransomware, adware).

NIST (National Institute of Standards and Technology) ning SP 800-83 standarti malwareni quyidagicha tasnif qiladi: viruslar va qurtlar (o'z-o'zini ko'paytiruvchi), troyanlar (aldamchi dasturlar), spyware va adware (ma'lumot to'plovchi), ransomware (tovlamachilik), rootkit (yashirincha kiradigan), botnet (masofadan boshqariladigan) va hybrid threats (kombinatsiyalangan tahdidlar) (NIST, 2013). Ushbu tasnif zamonaviy tadqiqotlarda keng qo'llaniladi va maqolaning asosiy tuzilmasini belgilab beradi.

Kompyuter virusi — bu boshqa dasturlarga yoki fayllarni infektsiya qiluvchi va o'z nusxasini ko'paytira oladigan dasturiy koddir. Virusning asosiy belgisi — u faol holda ishga tushirilgunga qadar tarqalmaydi, ya'ni 'host' fayl talab qilinadi (Szor, 2005). Fred Cohen 1983 yilda kompyuter virusini ilmiy jihatdan birinchi marta ta'riflagan va uni 'o'zini boshqa dasturlarga yuqtirib, ularni zaraklab, ta'sir doirasini kengaytiradigan dastur' sifatida tavsiflagan (Cohen, 1987).

Viruslar ishlash mexanizmi bo'yicha bir nechta turga bo'linadi. Birinchidan, faylni infeksiya qiluvchi viruslar (File Infector Viruses) — .exe va .com kengaytmali bajariladigan fayllarga birikib, har safar ishga tushirilganda o'zini boshqa fayllarga ko'chirib oladi. Masalan, CIH (Chernobyl) virusi 1998 yilda dunyo bo'ylab 60 million kompyuterga zarar yetkazgan (Symantec, 2001). Ikkinchidan, yuklash sektori viruslari (Boot Sector Viruses) — qattiq disk yoki flesh kartaning MBR (Master Boot Record) sektorini infeksiya qilib, kompyuter yoqilganda birinchi ishga tushadi. Uchinchidan, makro viruslar — Microsoft Word va Excel hujjatlarining makro tili yordamida tarqaladi; Melissa virusi (1999) ana shunday virus bo'lib, elektron pochta orqali 1 million dan ortiq kompyuterni zaraklab, 80 million dollar zarar yetkazgan (FBI, 2002). To'rtinchidan, polimorfik va metamorfik viruslar — har tarqalganida o'z kodini o'zgartiradi, bu esa ularni antivirus dasturlar uchun aniqlab olishni nihoyatda qiyinlashtiradi.

Tarmoq qurti (worm) — virusdan farqli o'laroq, 'host' dasturga muhtoj bo'lmagan va mustaqil ravishda tarmoq orqali tarqala oladigan zararli dasturdir. Qurtlar tarmoq zaifliklaridan, elektron pochta ilovalaridan, messenjer dasturlaridan yoki almashtirilgan disklar orqali tarqaladi (Nazario, 2004).

Morris Worm (1988) — tarixdagi birinchi keng tarqalgan qurt sifatida mashhur. U UNIX tizimlarining sendmail, fingerd va rsh/rexec xizmatlaridagi zaifliklardan foydalangan. Stuxnet (2010) esa kiberjangning eng murakkab namunasidir: SCADA sanoat tizimlarini nishon qilib, Eron yadroviy dasturiga jiddiy zarar yetkazgan. Tadqiqotchilar Stuxnet-ning 500 kilobyte hajmli kodini tahlil qilib, 4 ta zero-day zaiflikdan foydalanganini aniqladilar (Langner, 2011). Mirai Botnet (2016) esa IoT qurilmalarini (router, kamera, printer) infeksiya qilib, tarixdagi eng kuchli DDoS hujumlaridan birini amalga oshirdi — Dyn DNS provayderiga 1.2 Tbps tezlikdagi hujum (Antonakakis et al., 2017). WannaCry (2017) esa Windows tizimlaridagi EternalBlue zaifligidan foydalanib, 150 mamlakatda 230,000 kompyuterni infeksiya qildi va 4 milliard dollarlik zarar yetkazdi (UK National Cyber Security Centre, 2018).

Troyan oti (Trojan horse) — o'zini zararsiz yoki foydali dastur sifatida ko'rsatib, aslida zararli harakatlar amalga oshiradigan dasturdir. Yunon mifologiyasidagi Troya oti afsonasiga ishora qilib nomlangan bu dasturlar foydalanuvchilarni aldashga asoslanadi (McGraw & Morrisett, 2000). Troyanlar o'z-o'zini ko'paytirmaydi, lekin kiber jinoyatchilarning qo'lidagi eng kuchli qurollardan biri hisoblanadi.

Troyanlarning asosiy turlari va ishlash mexanizmlari quyidagicha: RAT (Remote Access Trojan) — masofaviy kirish troyanlar kiberjinoyatchiga infeksiyalangan kompyuterga to'liq kirish imkonini beradi. BlackShades RAT 2012-2014 yillarda 100 dan ortiq mamlakatda tarqalib, 700 mingdan ortiq qurilmani nazorat ostiga olgan (US Department of Justice, 2014). Banking Trojanlar (bank troyanlar) bank hisob ma'lumotlarini o'g'irlashga ixtisoslashgan. Zeus (Zbot) troyan 2007 yilda paydo bo'lib, 70 million dollardan ortiq mablag'ni o'g'irlaganligini FBI tasdiqlagan (FBI, 2010). Downloader/Dropper troyanlar birinchi bosqichda sodda ko'rinib, so'ngra internetdan boshqa zararli dasturlarni yuklab oladi. Formjacking troyanlar (keylogger) esa klaviatura tugmachalarini yozib borib, parol va kredit karta raqamlarini to'playdi.

Troyanlar ko'pincha social engineering metodlari orqali tarqaladi: soxta elektron pochta xabarlari (phishing), buzilgan veb-saytlar (drive-by download), pirat dastur va o'yinlar orqali yuklanadi. Verizon ma'lumotlariga ko'ra, axborot xavfsizligi hodisalarining 82% inin inson omili (social engineering) tashkil qiladi (Verizon DBIR, 2022).

Ransomware — foydalanuvchining ma'lumotlarini shifrlash yoki tizimga kirishni bloklash orqali to'lov talab qiladigan zararli dastur turi bo'lib, bugungi kunda eng daromadli kiber jinoyat shakliga aylangan. Birinchi ransomware — AIDS Trojan (PC Cyborg) 1989 yilda Joseph Popp tomonidan disketa orqali tarqatilgan (Young & Yung, 1996).

Zamonaviy ransomware ishlash mexanizmi bir necha bosqichdan iborat: birinchi bosqichda — tarqalish (delivery) phishing, zaif RDP portlari yoki ekspluatatsiya orqali tizimga kiriladi. Ikkinchi bosqichda — tizimga joylashish (persistence) Windows Registry yoki Task Scheduler orqali tizim qayta ishga tushganda ham faol bo'lishi ta'minlanadi. Uchinchi bosqichda — razvedka (reconnaissance) muhim faylllar (hujjatlar, rasmlar, ma'lumotlar bazasi) aniqlanadi. To'rtinchi bosqichda — shifrlash (encryption) AES-256 yoki RSA-2048 algoritmlar bilan fayllar shifrlanadi va kalit faqat to'lovdan so'ng beriladi. Beshinchi bosqichda — to'lov talabi (ransom demand) odatda Bitcoin yoki Monero kriptovalyutasida to'lov talab qilinadi (Bhardwaj et al., 2016).

WannaCry (2017) va NotPetya (2017) global ransomware hujumlari alohida ahamiyat kasb etadi. NotPetya Ukraina kompaniyalarini nishon qilib, global shipping giganti Maersk va farmatsevtika ulkani Merck-ga ham zarar yetkazdi, jami zarar 10 milliard dollardan oshdi (Greenberg, 2018). CNA Financial korporatsiyasi 2021 yilda Phoenix CryptoLocker ransomware dan qutulish uchun 40 million dollar to'lagan — bu tarixdagi eng katta ransomware to'lovi hisoblanadi (Bloomberg, 2021). FBI ma'lumotlariga ko'ra, 2023 yilda ransomware hujumlaridan jami zarar 1.1 milliard dollarni tashkil etdi (FBI IC3, 2024).

Spyware — foydalanuvchi bilimisiz uning harakatlarini kuzatuvchi, ma'lumotlarini to'plovchi va uchinchi shaxslarga uzatuvchi zararli dastur. Spyware toifasiga keyloggerlar, screen capturer (ekran tasviri oluvchi), audio/video yozuvchilar, brauzer tarixini o'g'irlovchilar va system monitor dasturlari kiradi (Egele et al., 2008).

Pegasus spyware — NSO Group (Isroil) tomonidan yaratilgan va hukumat razvedka xizmatlari uchun sotilgan yuqori texnologiyali spyware bo'lib, iPhone va Android qurilmalarining zero-click zaifliklaridan foydalanadi (Marczak & Scott-Railton, 2016). Citizen Lab tadqiqotlari natijasida Pegasus 45 mamlakatda jurnalistlar, faollar va siyosatchilarni josuslik qilish uchun ishlatilganligi isbotlangan (Citizen Lab, 2018). Emotet — dastlab banking troyan sifatida boshlangan bo'lsa-da, keyinchalik spyware va boshqa zararli dasturlarning

taqsimlovchisiga aylangan; Europol uni 'dunyoning eng xavfli zararli dasturi' deb ta'riflagan (Europol, 2021).

Adware — reklama ko'rsatish orqali daromad olishga mo'ljallangan, lekin ko'pincha foydalanuvchi ruxsatisiz o'rnatiladigan dastur turi. Garchi adware to'g'ridan-to'g'ri ma'lumot o'g'irlamasa ham, brauzer sozlamalarini o'zgartirish, qidiruvni qayta yo'naltirish va qo'shimcha zararli dastur o'rnatish orqali xavf tug'diradi. FTC (Federal Trade Commission) ma'lumotlariga ko'ra, 2004 yilda kompyuterlarning 80% idan ortig'i turli darajada adware bilan infeksiyalangan edi (FTC, 2004).

Rootkit — operatsion tizim darajasida yashirincha faoliyat yurituvchi va o'z vujudini antivirus va foydalanuvchidan yashiradigan zararli dasturlar toifasi. Rootkit termini UNIX tizimlarida 'root' (administrator) huquqlari va 'kit' (vositalar to'plami) so'zlaridan hosil bo'lgan (Hoglund & Butler, 2006). Rootkitlar ishlash darajasiga ko'ra to'rtta asosiy turga bo'linadi: User-mode rootkitlar — foydalanuvchi makonida ishlaydi va API funksiyalarini o'zgartiradi; Kernel-mode rootkitlar — OS yadrosiga kirib, eng yuqori darajadagi yashirishni ta'minlaydi; Bootkit — BIOS yoki MBR darajasida ishlaydi va OS yuklanishidan oldin faol bo'ladi; Hypervisor rootkitlar — virtual mashina darajasida ishlaydi.

Sony BMG (2005) skandali rootkit tarixidagi eng mashhur holatlardan biridir: Sony musiqa kompaniyasi CD disklarida foydalanuvchilarning kompyuterlariga muallif huquqlarini himoya qilish bahonasida rootkit o'rnatib qo'ygan, ammo bu rootkit boshqa zararli dasturlar uchun ham eshik ochib bergan. Natijada Sony 500,000 dan ortiq kompyuter ta'sirlanib, kompaniya katta jarimaga tortilgan (EFF, 2005).

Botnet — kiberjinoyatchilar tomonidan masofadan boshqariladigan infeksiyalangan kompyuterlar tarmog'i (bot — robot, net — tarmoq). Botnet arxitekturasi ikki xil bo'ladi: markazlashtirilgan C&C (Command and Control) serverli model va p2p (peer-to-peer) tarqatilgan model. Botnetlar DDoS hujumlari, spam tarqatish, kriptovalyuta qazib olish (cryptojacking), ma'lumot o'g'irlash va ransomware tarqatish uchun ishlatiladi. Zeus botnet o'z faoliyati davomida 13 million qurilmani o'z ichiga olgan (Symantec, 2010). Mariposa botnet 2010 yilda Ispaniya politsiyasi tomonidan tugatilgan bo'lib, u 190 mamlakatda 12.7 million kompyuterni boshqargan (FBI, 2010).

APT (Advanced Persistent Threat — ilg'or doimiy tahdid) — davlat yoki yirik tashkilot tomonidan moliyalashtiriladigan, uzoq muddatli va nishonlangan kiberhujumlar sinfini anglatadi. APT hujumlari oddiy zararli dasturlardan farqli o'laroq, bir necha oy yoki yil davomida nishon tizimda yashirincha faoliyat yuritadi (Mandiant, 2013).

APT29 (Cozy Bear) — Rossiya davlati bilan bog'liq, 2020 yilda SolarWinds Orion platformasi orqali supply chain hujumi amalga oshirib, AQSh hukumat idoralarining 18,000 dan ortiq tarmog'iga kirgan (CISA, 2021). Bu hujum 'supply chain attack' deb atalib, legit dasturiy ta'minotni yangilash jarayonida zararli kod kiritishga asoslangan. Lazarus Group — Shimoliy Koreya davlati bilan bog'liq hujum guruhi bo'lib, Bangladesh Markaziy Bankidan 81 million dollar o'g'irlagan (2016) va WannaCry ransomware hujumiga aloqador deb gumonlanmoqda (US-CERT, 2017). Fileless malware — zamonaviy tendensiya bo'lib, bu turdagi zararli dasturlar qattiq diskka hech qanday fayl yozmaydi, balki tizimning xotirasida va qonuniy jarayonlarda (PowerShell, WMI) ishlaydi, bu esa ularni an'anaviy antivirus bilan aniqlashni deyarli imkonsiz qiladi (Luk et al., 2020).

Zararli dasturlarga qarshi kurashishda kompleks yondashuv talab etiladi va bu ko'p qatlamli (defense-in-depth) model deb ataladi (NIST, 2018). Texnik himoya vositalari qatoriga quyidagilar kiradi: antivirus va EDR (Endpoint Detection and Response) tizimlar — imzo asosidagi (signature-based) va xulq-atvor asosidagi (behavior-based) tahlil usullari bilan ishlaydi; Next-Generation Antivirus (NGAV) — sun'iy intellekt va machine learning algoritmlar yordamida noma'lum tahdidlarni ham aniqlab beradi; Sandboxing — shubhali

fayllarni izolyatsiyalangan muhitda bajarib tekshirish; Network Traffic Analysis (NTA) — tarmoq trafikini real vaqtda tahlil qilish; va Zero Trust Architecture — hech kimga va hech narsaga avtomatik ishonmaslik printsipi.

Profilaktik choralar ham hal qiluvchi ahamiyatga ega: dasturiy ta'minotni muntazam yangilash, kuchli parollar va ko'p faktorli autentifikatsiya (MFA), ma'lumotlarni muntazam zaxiralash (backup), xodimlarni axborot xavfsizligi bo'yicha o'qitish va fishing simulyatsiyalari. Ponemon Institute tadqiqotiga ko'ra, xodimlarni o'qitish kiber hujum xavfini 45-70% gacha kamaytiradi (Ponemon Institute, 2022). MITRE ATT&CK framework — hujumchilarning taktika, texnika va protseduralarini (TTPs) tizimlashtirgan global ma'lumotlar bazasi bo'lib, kibertahdidlarni tahlil qilish va ularga qarshi choralar ishlab chiqishda keng qo'llaniladi (MITRE Corporation, 2023).

Ushbu maqolada zararli dasturlarning asosiy turlari — viruslar, qurtlar, troyanlar, ransomware, spyware, adware, rootkit va botnetlar — ilmiy jihatdan tahlil qilindi. Har bir tur uchun texnik ishlash mexanizmlari, real dunyo misollarida ta'sirli natijalari va himoya usullari ko'rib chiqildi. Tadqiqot natijasida quyidagi xulosalar shakllandi:

Birinchidan, zararli dasturlar evolyutsiyasi davom etmoqda: sodda faylni infeksiya qiluvchi viruslardan APT hujumlari va fileless malwaregacha bo'lgan rivojlanish yo'li kiberxavfsizlik sohasida doimiy ilmiy-tadqiqot ishlarini talab qiladi. Ikkinchidan, gibrid tahdidlar kuchaymoqda: zamonaviy zararli dasturlar ko'pincha bir nechta texnikani birlashtirib, masalan ransomware + data exfiltration + botnet funksiyalarini o'zida mujassamlashtiradi. Uchinchidan, inson omili asosiy zaif bo'g'in bo'lib qolmoqda: texnik vositalar qanchalik rivojlanmasin, social engineering va fishing orqali hujumlar samaradorligini yo'qotmayapti. To'rtinchidan, kompleks yondashuv zarur: bitta texnik vosita bilan to'liq himoyani ta'minlab bo'lmaydi, zamonaviy kibertahdidlarga qarshi ko'p qatlamli mudofaa tizimi va xodimlarni o'qitish kombinatsiyasi talab etiladi.

Kibertahdidlarga qarshi kurashish — bu faqat IT mutaxassislarining muammosi emas, balki davlat siyosati, huquqiy tartibga solish va jamiyat madaniyati darajasida hal etilishi lozim bo'lgan global muammodir. Kelgusida sun'iy intellekt asosidagi zararli dasturlar va deepfake texnologiyalariga asoslangan social engineering hujumlari yanada ko'proq tadqiqot va amaliy ehtiyotkorlik choralarini talab etadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Anderson, R. (2020). Security Engineering: A Guide to Building Dependable Distributed Systems (3rd ed.). Wiley.
2. Antonakakis, M., April, T., Bailey, M., et al. (2017). Understanding the Mirai Botnet. In Proceedings of the 26th USENIX Security Symposium (pp. 1093–1110).
3. AV-TEST Institute. (2024). Security Report 2023/2024. https://www.av-test.org/en/statistics/malware/
4. Bhardwaj, A., Avasthi, V., Sastry, H., & Subrahmanyam, G. V. B. (2016). Ransomware Digital Extortion: A Rising New Age Threat. Indian Journal of Science and Technology, 9(14), 1–5.
5. Bloomberg. (2021, May 20). CNA Financial Paid $40 Million in Ransom After March Cyberattack. Bloomberg News.
6. Citizen Lab. (2018). Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. The Citizen Lab, University of Toronto.
7. CISA. (2021). Alert (AA20-352A): Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations. US Cybersecurity and Infrastructure Security Agency.
8. Cohen, F. B. (1987). Computer viruses: Theory and experiments. Computers & Security, 6(1), 22–35.

9. Cybersecurity Ventures. (2023). Cybercrime To Cost The World $8 Trillion Annually In 2023. Cybersecurity Ventures.
10. Egele, M., Kruegel, C., Kirda, E., Yin, H., & Song, D. (2008). Dynamic spyware analysis. Proceedings of the 2007 USENIX Annual Technical Conference, 233–246.
11. Electronic Frontier Foundation (EFF). (2005). Sony Settles Rootkit Case. EFF Press Release.