INNOVATIVE WORLD
Ilmiy tadqiqotlar markazi

YANGI RENESSANS

ILMIY JURNALI

2026/4

+998335668868
www.innoworld.net

YANGI RENESSANS

ILMIY JURNALI
TO'PLAMI

3 - JILD, 4 - SON
2026

www.innoworld.net

O'ZBEKISTON-2026

Botnetlar va DDoS hujumlarida ularning roli
Роль ботнетов в DDoS-атаках
The Role of Botnets in DDoS Attacks

Sobirjonov Behzodbek Qahramonovich
Farg‘ona davlat universiteti Axborot texnologiyalari kafedrasi o’qituvchisi
behzodbekqahramonovich@gmail.com
Xabibulloyeva Muxlisa Xamidullo qizi
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalari yo‘nalishi
2-kurs talabasi
humayro21m@gmail.com

Annotatsiya

Ushbu ishda botnetlarning tuzilishi, ishlash prinsipi va DDoS hujumlaridagi o‘rni tahlil qilinadi. Botnet — bu zararli dasturlar orqali boshqariladigan ko‘plab qurilmalar tarmog‘i bo‘lib, ular yordamida keng ko‘lamli kiberhujumlar amalga oshiriladi. Ishda DDoS hujumlarining mohiyati, ularning turlari hamda botnetlar orqali qanday tashkil etilishi yoritilgan.

Shuningdek, kiberxavfsizlik nuqtai nazaridan bunday hujumlarning oldini olish usullari, aniqlash mexanizmlari va himoya choralariga alohida e’tibor qaratilgan. Mazkur mavzu kiberxavfsizlik sohasining muhim yo‘nalishlaridan biri bo‘lib, zamonaviy axborot tizimlarini himoya qilishda dolzarb ahamiyat kasb etadi.

Аннотация

В данной работе рассматриваются структура ботнетов, принципы их функционирования и их роль в DDoS-атаках. Ботнет представляет собой сеть устройств, управляемых вредоносным программным обеспечением, которая используется для проведения масштабных кибератак. В работе освещаются сущность DDoS-атак, их виды, а также способы их организации с использованием ботнетов.

Также особое внимание уделено методам обнаружения и предотвращения подобных атак, а также мерам защиты с точки зрения кибербезопасности. Данная тема является важным направлением в области кибербезопасности и имеет актуальное значение для защиты современных информационных систем.

Abstract

This paper examines the structure of botnets, their operating principles, and their role in DDoS attacks. A botnet is a network of devices controlled by malicious software, which is used to carry out large-scale cyberattacks. The study highlights the nature of DDoS attacks, their types, and how they are organized using botnets.

Special attention is also given to detection and prevention methods, as well as protective measures from a cybersecurity perspective. This topic is an important area within cybersecurity and is highly relevant for protecting modern information systems.

Kalit so‘zlar: botnet, DDoS hujum, zararli dastur, tarmoq xavfsizligi, kiberhujum, trafik toshqinlari, autentifikatsiya, himoya mexanizmlari.

Ключевые слова: ботнет, DDoS-атака, вредоносное ПО, сетевая безопасность, кибератака, сетевой трафик, аутентификация, механизмы защиты.

Keywords: botnet, DDoS attack, malware, network security, cyberattack, traffic flooding, authentication, protection mechanisms.

Kirish

Zamonaviy axborot texnologiyalarining jadal rivojlanishi natijasida internet tarmoqlariga bo‘lgan ehtiyoj va bog‘liqlik tobora ortib bormoqda. Bugungi kunda turli onlayn xizmatlar, bank tizimlari, elektron hukumat platformalari hamda ijtimoiy tarmoqlar inson hayotining ajralmas qismiga aylangan. Ushbu tizimlarning uzluksiz va barqaror ishlashi muhim ahamiyat kasb etadi. Shu bilan birga, axborot tizimlariga nisbatan amalga oshirilayotgan kiberhujumlar soni ham keskin oshib bormoqda.

Kiberxavfsizlik sohasida eng keng tarqalgan va xavfli tahdidlardan biri bu DDoS (Distributed Denial of Service) hujumlaridir. Ushbu hujumlarning asosiy maqsadi — server yoki tarmoq resurslarini ortiqcha so‘rovlar bilan yuklab, xizmat ko‘rsatishni izdan chiqarishdir. Natijada foydalanuvchilar tizimdan foydalana olmaydi, bu esa katta iqtisodiy va axborot yo‘qotishlariga olib keladi.

DDoS hujumlarini amalga oshirishda botnetlar muhim rol o‘ynaydi. Botnet — bu zararli dasturlar yordamida boshqariladigan ko‘plab kompyuter va qurilmalar tarmog‘i bo‘lib, ular markazlashgan tarzda boshqariladi. Ushbu qurilmalar “zombi qurilmalar” sifatida ishlatiladi va bir vaqtning o‘zida maqsadli tizimga katta hajmdagi trafik yuboradi. Ko‘pincha bunday qurilmalar egasi bu jarayondan bexabar bo‘ladi.

Mazkur ishda botnetlarning tuzilishi, ishlash mexanizmi va ularning DDoS hujumlaridagi o‘rni batafsil tahlil qilinadi. Shuningdek, DDoS hujumlarining asosiy turlari, ularni aniqlash va oldini olish usullari ham ko‘rib chiqiladi. Ushbu mavzuni o‘rganish zamonaviy axborot tizimlarini himoya qilish, xavfsizlikni ta’minlash va kiberhujumlarning oldini olishda muhim ahamiyatga ega.

Botnet (inglizcha “bot” — robot va “network” — tarmoq) bu zararli dastur bilan zararlangan va masofadan boshqariladigan qurilmalar tarmog‘idir. Ushbu qurilmalar kompyuterlar, serverlar, mobil qurilmalar yoki IoT texnologiyalariga tegishli qurilmalar bo‘lishi mumkin. Botnet tarkibiga kirgan har bir qurilma “zombi qurilma” sifatida ishlaydi va u markaziy boshqaruv tizimi orqali nazorat qilinadi. Odatda bunday boshqaruv C&C (Command and Control) serverlari orqali amalga oshiriladi. Qurilmalar zararli dasturlar, masalan viruslar, trojanlar yoki boshqa zararli kodlar orqali zararlanadi va foydalanuvchi bundan bexabar holda o‘z qurilmasini hujumchi ixtiyoriga topshirib qo‘yadi.

Botnetlarning ishlash prinsipi bir necha bosqichdan iborat bo‘ladi. Avval qurilmaga zararli dastur o‘rnatiladi, bu esa ko‘pincha fishing hujumlari, zararli

fayllar yoki ishonchsiz veb-saytlar orqali amalga oshiriladi. Keyinchalik zararlangan qurilma boshqaruv serveriga ulanadi va undan buyruqlar qabul qila boshlaydi. Shu orqali hujumchi bir vaqtning o‘zida minglab yoki hatto millionlab qurilmalarni boshqarish imkoniyatiga ega bo‘ladi. Zamonaviy botnetlar markazlashgan yoki markazlashmagan, ya’ni P2P (peer-to-peer) texnologiyasi asosida ishlashi mumkin, bu esa ularni aniqlash va yo‘q qilishni ancha murakkablashtiradi.

DDoS (Distributed Denial of Service) hujumlari esa tarmoq yoki server resurslarini haddan tashqari yuklab, uning normal ishlashini izdan chiqarishga qaratilgan kiberhujumlardir. Bunday hujumlar natijasida tizim foydalanuvchilarga xizmat ko‘rsata olmay qoladi yoki juda sekin ishlay boshlaydi. DDoS hujumlari odatda bir nechta turga bo‘linadi: volumetrik hujumlar katta hajmdagi trafik yuborish orqali tarmoqni band qiladi, protokol darajasidagi hujumlar server resurslarini egallab oladi, ilova darajasidagi hujumlar esa bevosita veb-xizmatlarga qaratilgan bo‘ladi. Ushbu hujumlarning asosiy xavfi shundaki, ular qisqa vaqt ichida katta zarar yetkazishi va xizmatlarni to‘liq ishdan chiqarishi mumkin.

Botnetlar DDoS hujumlarining amalga oshirilishida asosiy vosita sifatida xizmat qiladi. Chunki bitta qurilma orqali katta hajmdagi trafik yuborish deyarli imkonsiz, ammo minglab zararlangan qurilmalar yordamida bu juda oson amalga oshiriladi. Hujumchi boshqaruv serveri orqali botnetga buyruq yuboradi va barcha qurilmalar bir vaqtning o‘zida maqsadli serverga so‘rov yubora boshlaydi. Natijada server ortiqcha yuklama tufayli ishlamay qoladi yoki xizmat ko‘rsatish sifati keskin pasayadi. Amaliyotda Mirai kabi mashhur botnetlar aynan IoT qurilmalaridan foydalanib, juda kuchli DDoS hujumlarini amalga oshirganligi bilan tanilgan.

Kiberxavfsizlik nuqtai nazaridan DDoS hujumlarini aniqlash va oldini olish juda muhim hisoblanadi. Buning uchun tarmoq trafiklarini doimiy monitoring qilish, noodatiy faoliyatni aniqlash, firewall va IDS/IPS tizimlaridan foydalanish zarur. Shuningdek, yuklamani bir nechta serverlarga taqsimlash (load balancing), kontent yetkazib berish tarmoqlari (CDN) dan foydalanish va zararli IP manzillarni bloklash orqali bunday hujumlarning ta’sirini kamaytirish mumkin. Shu bilan birga, oddiy foydalanuvchilar ham o‘z qurilmalarini muntazam yangilab borish, antivirus dasturlaridan foydalanish orqali botnetlarga qo‘shilib qolish xavfini kamaytirishlari mumkin.

Xulosa

Xulosa qilib aytganda, zamonaviy axborot texnologiyalari rivojlanishi bilan bir qatorda kiberxavfsizlik tahdidlari ham sezilarli darajada ortib bormoqda. Ayniqsa, DDoS hujumlari internet xizmatlari va axborot tizimlari uchun eng xavfli hujum turlaridan biri hisoblanadi. Ushbu hujumlarning samarali amalga oshirilishida botnetlar asosiy vosita sifatida muhim rol o‘ynaydi. Zararli dasturlar

orqali boshqariladigan ko‘plab qurilmalar tarmog‘i bir vaqtning o‘zida katta hajmdagi trafik hosil qilib, server va tarmoqlarni ishdan chiqarishga qodir.

Tadqiqot davomida botnetlarning tuzilishi, ishlash mexanizmi hamda DDoS hujumlaridagi o‘rni tahlil qilindi. Shuningdek, DDoS hujumlarining asosiy turlari va ularning axborot tizimlariga ko‘rsatadigan salbiy ta’siri ko‘rib chiqildi. Aniqlanishicha, bunday hujumlar nafaqat texnik, balki iqtisodiy zarar ham yetkazishi mumkin.

Shu bois, DDoS hujumlariga qarshi samarali kurashish uchun zamonaviy himoya vositalaridan foydalanish, tarmoq monitoringini yo‘lga qo‘yish, xavfsizlik siyosatini kuchaytirish va foydalanuvchilarning axborot xavfsizligi bo‘yicha bilimlarini oshirish zarur. Faqat kompleks yondashuv orqali bunday kiberxavflarning oldini olish va axborot tizimlarining barqaror ishlashini ta’minlash mumkin.

Foydalanilgan adabiyotlar

1. Stallings, W. — *Network Security Essentials: Applications and Standards*. Pearson Education, 2017.
2. Kurose, J. F., Ross, K. W. — *Computer Networking: A Top-Down Approach*. Pearson, 2021.
3. Scarfone, K., Hoffman, P. — *Guidelines on Firewalls and Firewall Policy*. NIST Special Publication, 2009.
4. Behl, A., Behl, K. — *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, 2017.
5. Zargar, S. T., Joshi, J., Tipper, D. — “A Survey of Defense Mechanisms Against DDoS Flooding Attacks”, *IEEE Communications Surveys & Tutorials*, 2013.