BOTNETLAR VA DDOS HUJUMLARIDA ULARNING ROLI

РОЛЬ БОТНЕТОВ В DDOS-АТАКАХ

THE ROLE OF BOTNETS IN DDOS ATTACKS

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Tursunova Ra’noxon Ismoiljon qizi
FarDu Axborot tizimlari va tehnologiyalari yo‘nalishi 2-bosqich talabasi
tursunovaranoxon214@gmail.com
To‘lqinboyeva Odinaxon Dilshodbek qizi
FarDu Axborot tizimlari va tehnologiyalari yo‘nalishi 2-bosqich talabasi
odinatolqinboyeva85@gmail.com

Annotatsiya. Ushbu maqolada botnetlar tushunchasi, ularning tuzilishi va zamonaviy kiberxavfsizlik tizimlariga tahdidi tahlil qilinadi. Ayniqsa, botnetlarning DDoS (Distributed Denial of Service) hujumlaridagi o‘rni va ularning ishlash mexanizmi chuqur o‘rganiladi. Maqolada botnetlarni yaratish usullari, ularni boshqarish (Command and Control — C&C) tizimlari, hamda DDoS hujumlarining asosiy turlari yoritiladi. Shuningdek, bunday hujumlardan himoyalanish usullari va zamonaviy xavfsizlik choralariga alohida e’tibor qaratilgan. Tadqiqot natijalari asosida botnetlarga qarshi samarali kurashish va tarmoqlarni himoyalash bo‘yicha amaliy tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: botnet, DDoS hujum, kiberxavfsizlik, zararli dastur, C&C server, tarmoq xavfsizligi, trafik, hujum, himoya mexanizmlari, internet xavfsizligi.

Аннотация. В данной статье рассматривается понятие ботнетов, их структура и угроза для современных систем кибербезопасности. Особое внимание уделяется роли ботнетов в DDoS-атаках и механизму их функционирования. Анализируются методы создания ботнетов, системы управления (Command and Control — C&C), а также основные типы DDoS-атак. Кроме того, освещаются методы защиты от подобных атак. На основе исследования предложены практические рекомендации по защите сетей и противодействию ботнетам.

Ключевые слова: ботнет, DDoS-атака, кибербезопасность, вредоносное ПО, C&C сервер, сетевая безопасность, трафик, атака, защита.

Abstract. This article examines the concept of botnets, their structure, and their threat to modern cybersecurity systems. Special attention is given to the role of botnets in Distributed Denial of Service (DDoS) attacks and their operational mechanisms. The study analyzes methods of botnet creation, Command and Control (C&C) systems, and the main types of DDoS attacks. Additionally, protection methods against such attacks are discussed. Based on

the research, practical recommendations are provided to improve network security and counter botnet-based attacks.

Keywords: botnet, DDoS attack, cybersecurity, malware, C&C server, network security, traffic, attack, protection mechanisms.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida kiberxavfsizlik masalalari tobora muhim ahamiyat kasb etmoqda. Internet tarmoqlarining kengayishi, raqamli xizmatlarning ortishi hamda turli qurilmalar, jumladan IoT (Internet of Things) tizimlarining ommalashuvi kiberjinoyatchilik uchun yangi imkoniyatlar yaratmoqda. Ayniqsa, botnetlar va ular yordamida amalga oshiriladigan DDoS (Distributed Denial of Service) hujumlari bugungi kunda eng xavfli tahdidlardan biri sifatida qaralmoqda. Botnetlar zararli dasturlar orqali boshqariladigan va hujumchi tomonidan masofadan turib nazorat qilinadigan qurilmalar tarmog‘idir. Bunday qurilmalar ko‘pincha foydalanuvchi bilmagan holda zararlanadi va “zombi kompyuterlar” sifatida ishlaydi.

Botnetlar odatda zararli dasturlarni tarqatish, phishing hujumlari yoki tizimdagi zaifliklardan foydalanish orqali shakllantiriladi. Har bir bot maxsus boshqaruv tizimi — Command and Control (C&C) server orqali boshqariladi. Ushbu server orqali hujumchi barcha zararlangan qurilmalarga buyruq yuboradi va ularni ma’lum vazifalarni bajarishga majbur qiladi. Botnetlar boshqaruv mexanizmiga ko‘ra markazlashgan va tarqatilgan turlarga bo‘linadi. Markazlashgan tizimlarda barcha buyruqlar bitta server orqali uzatilsa, tarqatilgan tizimlarda botlar o‘zaro aloqa qilib ishlaydi, bu esa ularni aniqlash va bartaraf etishni murakkablashtiradi.

Botnetlarning eng keng tarqalgan qo‘llanilish sohalaridan biri bu DDoS hujumlarini amalga oshirishdir. DDoS hujumlari server yoki tarmoqqa juda katta hajmdagi so‘rovlar yuborish orqali uning ishlashini izdan chiqarishga qaratilgan. Bunday hujumlar natijasida server resurslari band bo‘lib qoladi va haqiqiy foydalanuvchilar xizmatlardan foydalana olmaydi. DDoS hujumlari bir nechta turlarga bo‘linadi, jumladan volumetrik hujumlar, protokol darajasidagi hujumlar va ilova darajasidagi hujumlar. Volumetrik hujumlarda asosiy maqsad tarmoqni ortiqcha trafik bilan to‘ldirish bo‘lsa, protokol darajasidagi hujumlarda server resurslarini band qilishga e’tibor qaratiladi. Ilova darajasidagi hujumlar esa bevosita web xizmatlarga qaratilgan bo‘lib, ular nisbatan murakkab va aniqlash qiyin bo‘ladi.

Botnetlar orqali amalga oshiriladigan DDoS hujumlarining asosiy ustunligi shundaki, ular juda katta miqdordagi qurilmalarni bir vaqtning o‘zida ishga soladi. Natijada minglab yoki millionlab so‘rovlar bir vaqtda yuboriladi va bu serverning ishlashini to‘liq to‘xtatib qo‘yishi mumkin. Bundan tashqari, hujum manbasini aniqlash ham qiyinlashadi, chunki trafik turli geografik hududlardan kelib tushadi. Shu sababli botnetlarga asoslangan DDoS hujumlari zamonaviy kiberxavfsizlik tizimlari uchun jiddiy muammo hisoblanadi.

Bunday tahdidlarga qarshi samarali kurashish uchun kompleks xavfsizlik choralarini qo‘llash zarur. Avvalo, tarmoqlarni himoya qilishda firewall, IDS/IPS tizimlari va trafik monitoringi vositalaridan foydalanish muhim ahamiyatga ega. Shuningdek, CDN

xizmatlaridan foydalanish orqali yuklamani taqsimlash va serverni ortiqcha bosimdan himoya qilish mumkin. Rate limiting texnologiyasi yordamida bir foydalanuvchidan kelayotgan so‘rovlar sonini cheklash ham samarali usullardan biri hisoblanadi. Bundan tashqari, zararli IP manzillarni aniqlash va bloklash orqali hujumlarning oldini olish mumkin. Tizim xavfsizligini ta’minlashda antivirus dasturlarni muntazam yangilab borish, zaifliklarni bartaraf etish va foydalanuvchi huquqlarini to‘g‘ri boshqarish ham muhim rol o‘ynaydi. Tizim xavfsizligini doimiy ravishda audit qilish ham muhim hisoblanadi.

Tahlillar shuni ko‘rsatadiki, botnetlar yordamida amalga oshiriladigan DDoS hujumlari zamonaviy axborot tizimlariga katta zarar yetkazishi mumkin. Ayniqsa, IoT qurilmalar asosida shakllangan botnetlar juda katta hajmdagi hujumlarni amalga oshirish imkonini beradi. Shu sababli xavfsizlik choralarini muntazam ravishda takomillashtirib borish va yangi texnologiyalarni joriy etish zarur. Xulosa qilib aytganda, botnetlar va DDoS hujumlari zamonaviy kiberxavfsizlikning eng dolzarb muammolaridan biri bo‘lib qolmoqda. Ularning oldini olish uchun nafaqat texnik choralar, balki foydalanuvchilarning axborot xavfsizligi bo‘yicha bilimini oshirish ham muhim ahamiyatga ega. Kelajakda sun’iy intellekt asosidagi xavfsizlik tizimlari va avtomatlashtirilgan monitoring vositalari yordamida bunday tahdidlarni aniqlash va bartaraf etish yanada samarali bo‘lishi kutilmoqda.

Foydalanilgan adabiyotlar

1. Stallings, W. Network Security Essentials. – Pearson, 2022.
2. Kurose, J., Ross, K. Computer Networking. – Pearson, 2021.
3. Microsoft Security Documentation – https://learn.microsoft.com
4. ENISA Cybersecurity Reports – https://www.enisa.europa.eu
5. O’Reilly – Cybersecurity and Network Defense, 2021
6. Symantec Threat Reports, 2023
7. Kaspersky Security Bulletin, 2024
8. Cisco Annual Cybersecurity Report, 2023