BOTNETLAR VA DDOS HUJUMLARIDA ULARNING ROLI

Behzod Sobirjonov Qahramonivich
FarDu Axborot tehnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Usipaliyeva Madinaxon Mohirali qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi 2-bosqich talabasi
m40437770@gmail.com
Telefon raqam:91-144-99-06
https://doi.org/10.5281/zenodo.19968748

ANNOTATSIYA

Ushbu maqolada botnetlar va DDoS hujumlarida ularning roli, ishlash mexanizmlari hamda zamonaviy kiberxavfsizlikka ta’siri tadqiq etiladi. Maqolada kiberjinoyatchilar tomonidan zararlangan qurilmalarni masofadan boshqarish usullari, botnet tarmoqlarining tuzilishi va DDoS hujumlarini amalga oshirishdagi ahamiyati tahlil qilingan.Maqolada kiberxavfsizlikning dolzarb tahdidlaridan biri bo‘lgan botnet va DDoS tushunchalari, ularning ishlash prinsiplari hamda o‘zaro bog‘liqligi yoritiladi.

Kalit so‘zlar: Kiberxavfsizlik, Botnet, DDoS hujumi, Zararli dastur, Tarmoq xavfsizligi, Kiberhujum, Himoya strategiyalari.

АННОТАЦИЯ

В данной статье исследуются ботнеты и их роль в DDoS-атаках, механизмы их работы, а также влияние на современную кибербезопасность. В статье проанализированы методы удалённого управления заражёнными устройствами со стороны киберпреступников, структура ботнет-сетей и их значение при осуществлении DDoS-атак. Рассматриваются ботнеты и DDoS как одни из наиболее актуальных угроз кибербезопасности, а также раскрываются принципы их функционирования и взаимосвязь.

Ключевые слова: Кибербезопасность, Ботнет, DDoS-атака, Вредоносное ПО, Сетевая безопасность, Кибератака, Стратегии защиты.

ANNOTATION

This article examines botnets and their role in DDoS attacks, their operating mechanisms, and their impact on modern cybersecurity. The article analyzes the methods used by cybercriminals to remotely control infected devices, the structure of botnet networks, and their importance in carrying out DDoS attacks. It also discusses botnets and DDoS as some of the most significant cybersecurity threats, explaining their operating principles and interconnection.

Keywords: Cybersecurity, Botnet, DDoS Attack, Malware, Network Security, Cyberattack, Protection Strategies.

Zamonaviy kiberxavfsizlik tizimlari texnik jihatdan yuqori darajada himoyalangan bo‘lsa-da, kiberjinoyatchilar hanuzgacha internetga ulangan himoyasiz qurilmalar va tarmoq infratuzilmasidan foydalanishda davom etmoqda. Botnetlar va DDoS hujumlari aynan shu zaifliklardan foydalanib, serverlar faoliyatini izdan chiqarish, onlayn xizmatlarni to‘xtatish hamda katta miqdorda iqtisodiy zarar yetkazishni maqsad qiladi.

Botnet: Yashirin Boshqariluvchi Qurilmalar Tarmog‘i.Botnet — bu zararli dastur bilan zararlangan va masofadan turib boshqariladigan ko‘plab qurilmalar majmuasidir. Ushbu

qurilmalar kompyuterlar, mobil telefonlar, serverlar, videokameralar yoki aqlli IoT qurilmalari bo‘lishi mumkin.

Mexanizmi:Kiberjinoyatchilar virus yoki trojan dasturlari yordamida qurilmalarni zararlaydi va ularni maxsus boshqaruv markaziga bog‘laydi. Har bir zararlangan qurilma “bot” yoki “zombi qurilma” deb ataladi.

Asosiy imkoniyatlari:

1. Egasi bilmagan holda ishlaydi.
2. Buyruqlarni masofadan qabul qiladi.
3. Bir vaqtning o‘zida minglab hujumlarda qatnashadi.
4. Katta trafik oqimini hosil qiladi.

DDoS: Taqsimlangan Xizmatni Rad Etish Hujumi.DDoS (Distributed Denial of Service) — ko‘plab qurilmalar orqali server, sayt yoki tarmoqqa bir vaqtda juda ko‘p so‘rov yuborilib, uning normal ishlashini to‘xtatishga qaratilgan hujum turidir.

Ishlash prinsipi: Botnet tarkibidagi minglab botlar bir vaqtda bitta nishonga murojaat qiladi. Server ortiqcha yuklama sababli haqiqiy foydalanuvchilarga xizmat ko‘rsata olmay qoladi.

Oqibatlari:

1. Sayt yoki ilova ishlamay qoladi.
2. Mijozlar xizmatdan foydalana olmaydi.
3. Moliyaviy zarar yuzaga keladi.
4. Kompaniya obro‘siga putur yetadi.

Botnetlarning DDoS Hujumlaridagi Roli

Botnet DDoS hujumlarining eng asosiy vositasi hisoblanadi. Bitta qurilma katta zarar yetkaza olmasa-da, minglab zararlangan qurilmalar birlashganda ulkan hujum quvvatini hosil qiladi.

Hujum bosqichlari:

1. Qurilmalarni zararli dastur bilan yuqtirish.
2. Ularni markaziy boshqaruv serveriga ulash.
3. Nishonni aniqlash.
4. Barcha botlarga bir vaqtda buyruq yuborish.
5. Nishon serverni trafik bilan band qilish.

Zamonaviy Botnet Strategiyalari

IoT Botnetlar: Kamera, router va aqlli qurilmalarni egallaydi.

Ransom DDoS: Hujum bilan tahdid qilib, pul talab qilish.

Hybrid Attack: DDoS bilan birga fishing yoki malware hujumlarini qo‘llash.

Cloud Botnet: Bulutli serverlardan foydalanib hujumni kuchaytirish.

Botnet va DDoS hujumlariga qarshi quyidagi choralar samarali hisoblanadi:

Kuchli firewall va IDS/IPS tizimlaridan foydalanish. Tarmoq trafikini doimiy monitoring qilish. Qurilmalar dasturiy ta’minotini yangilab borish. Kuchli parollar va MFA qo‘llash. Anti-DDoS xizmatlaridan foydalanish. IoT qurilmalarni alohida himoalangan tarmoqqa ulash.

Raqamli makonda xavfsizlik faqat serverlarni himoya qilish bilan cheklanmaydi, balki tarmoqqa ulangan har bir qurilmani nazorat qilishni ham talab etadi. Botnetlar va DDoS hujumlari zamonaviy kiberxavfsizlikka jiddiy tahdid bo‘lib qolmoqda. Shu sababli

foydalanuvchilar va tashkilotlar o‘z tizimlarini muntazam himoyalab borishlari zarur. Har bir himoyasiz qurilma kelajakdagi yirik kiberhujumning bir qismiga aylanishi mumkin.

Adabiyotlar, References, Литературы:

1. Axmedov Q.X. Kiberxavfsizlik asoslari va axborotni himoyalash usullari. Toshkent: O‘zbekiston Respublikasi Oliy ta’lim nashriyoti, 2024.
2. Karimov B.R. Kompyuter tarmoqlari xavfsizligi va zamonaviy tahdidlar. Toshkent: Fan va texnologiya, 2023.
3. Rasulov M.A. Axborot xavfsizligida botnet va zararli dasturlar tahlili. Toshkent, 2024.
4. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. Kiberxavfsizlik bo‘yicha milliy tavsiyalar va qo‘llanmalar. Toshkent, 2025.
5. Ismoilov D.N. DDoS hujumlari va tarmoq infratuzilmasini himoyalash. Toshkent: Yangi asr avlodi, 2024.