ZONE TRANSFER (AXFR) HUJUMLARI VA ULARNING OLDINI OLISH

Behzod Sobirjonov
FarDU Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
+998905268738
Jabborova Oygul Baxtiyor qizi
Farg‘ona davlat universiteti Axborot tizimlari va texnologiyalari yo‘nalishi
II kurs talabasi
oygul2804@gmail.com
Telefon raqam:91-282-80-78
https://doi.org/10.5281/zenodo.19880421

Annotatsiya. Raqamli infratuzilmaning asosi hisoblangan DNS (Domain Name System) tizimi tarmoq xavfsizligida muhim o‘rin tutadi. DNS zonalarini uzatish (AXFR) mexanizmi asosiy va ikkilamchi DNS serverlari o‘rtasida ma’lumotlarni sinxronizatsiya qilish uchun xizmat qilsa-da, noto‘g‘ri konfiguratsiya qilingan holatlarda u kiberhujumchilar uchun qimmatli ma’lumotlar manbaiga aylanadi. Ushbu maqolada AXFR hujumlarining mohiyati, hujumchilar tomonidan ma’lumot yig‘ish usullari va ushbu turdagi xavflarni bartaraf etish bo‘yicha samarali himoya choralari tahlil qilinadi.

Kalit so‘zlar: DNS, AXFR, Zone Transfer, Kiberxavfsizlik, DNS noto‘g‘ri konfiguratsiyasi, Tarmoq razvedkasi, BIND, Xavfsizlik choralari, TSIG.

Аннотация

Система DNS (Domain Name System), являющаяся основой цифровой инфраструктуры, играет важную роль в сетевой безопасности. Хотя механизм передачи зон DNS (AXFR) служит для синхронизации данных между основным и вторичным DNS-серверами, при неправильной конфигурации он становится ценным источником информации для киберпреступников. В данной статье анализируется сущность атак AXFR, методы сбора информации злоумышленниками и эффективные меры защиты по предотвращению данного типа угроз.

Ключевые слова: DNS, AXFR, Передача зоны, Кибербезопасность, Неправильная конфигурация DNS, Сетевая разведка, BIND, Меры безопасности, TSIG.

Annotation

The Domain Name System (DNS), the backbone of digital infrastructure, plays a critical role in network security. While the DNS Zone Transfer (AXFR) mechanism is designed to synchronize data between primary and secondary DNS servers, misconfigurations can turn it into a valuable information source for cyber attackers. This article examines the nature of AXFR attacks, the methods used by attackers for information gathering (reconnaissance), and effective security measures to mitigate these risks.

Keywords: DNS, AXFR, Zone Transfer, Cybersecurity, DNS Misconfiguration, Network Reconnaissance, BIND, Security Measures, TSIG.

Zone transfer (AXFR) — bu DNS serverlar o‘rtasida ma’lumotlar bazasini to‘liq ko‘chirish mexanizmi bo‘lib, odatda asosiy (primary) va ikkilamchi (secondary) DNS serverlar o‘rtasida sinxronlash uchun ishlatiladi. Ammo noto‘g‘ri sozlangan DNS serverlar ushbu funksiyani har qanday tashqi foydalanuvchiga ochiq qoldirsa, bu katta xavfsizlik muammosiga aylanishi mumkin. AXFR hujumi aynan shu zaiflikdan foydalanib, butun domen zonasi haqidagi

ma’lumotlarni noqonuniy qo‘lga kiritishga qaratilgan. Bunday hujum orqali tajovuzkor domen ichidagi barcha subdomenlar, server nomlari, IP manzillar, pochta serverlari va boshqa muhim infratuzilma elementlari haqida to‘liq tasavvurga ega bo‘ladi. Bu ma’lumotlar keyingi bosqichdagi hujumlar — masalan, phishing, brute-force, yoki tizimlarga to‘g‘ridan-to‘g‘ri kirish urinishlari uchun asos bo‘lib xizmat qiladi. Shuning uchun AXFR hujumi ko‘pincha razvedka (reconnaissance) bosqichining muhim qismi hisoblanadi.

Muammo shundaki, ko‘plab tizim administratorlari DNS sozlamalarini to‘g‘ri cheklamaydi yoki eski konfiguratsiyalarni yangilamasdan qoldiradi. Natijada DNS serverlar har qanday so‘rovga zone transfer orqali javob berishi mumkin bo‘ladi. Bu esa butun tarmoq tuzilmasini oshkor qiladi. Ayniqsa, ichki tizimlarga oid yozuvlar (internal records) ham tashqi foydalanuvchilarga ko‘rinib qolsa, xavf yanada ortadi.AXFR hujumlarining oldini olish uchun birinchi navbatda DNS server konfiguratsiyasini qat’iy nazorat qilish zarur. Zone transfer faqat ishonchli ikkilamchi serverlar bilan cheklanishi kerak. Buni IP manzillar orqali ruxsat berish (allow-transfer) mexanizmi bilan amalga oshirish mumkin. Bundan tashqari, DNS serverlarni muntazam ravishda audit qilish, loglarni tahlil qilish va shubhali faoliyatni aniqlash muhim hisoblanadi. Yana bir muhim chorasi — DNSSEC kabi xavfsizlik kengaytmalaridan foydalanishdir. Bu texnologiya ma’lumotlarning yaxlitligini ta’minlaydi va soxta javoblar yuborilishining oldini oladi. Shuningdek, firewall va IDS/IPS tizimlari orqali DNS trafigini nazorat qilish ham foydali bo‘ladi. Xulosa qilib aytganda, AXFR hujumlari oddiy ko‘rinishiga qaramay, katta xavf tug‘diradi, chunki ular tizim haqidagi muhim ma’lumotlarni oshkor qiladi. To‘g‘ri sozlangan va himoyalangan DNS infratuzilmasi esa bunday hujumlarning oldini olishda asosiy rol o‘ynaydi.

Xulosa

Zone Transfer (AXFR) mexanizmi tarmoq barqarorligi uchun zarur bo'lsa-da, uni nazoratsiz qoldirish kiberhujumchilarga tashkilotning raqamli xaritasini "podnosda" taqdim etish bilan barobardir. WHOIS va RDAP kabi tashqi xizmatlar domen haqida umumiy ma'lumot bersa, AXFR noto'g'ri sozlansa, ichki tizimlarning barcha nozik nuqtalarini ochib beradi. Shu sababli, DNS serverlarini to'g'ri konfiguratsiya qilish, TSIG kalitlarini joriy etish va kirish huquqlarini cheklash zamonaviy tarmoq xavfsizligining ajralmas qismidir. Xavfsiz DNS infratuzilmasi nafaqat ma'lumotlar butunligini, balki butun tashkilot kiber-immunitetini ta'minlaydi.

Adabiyotlar, References, Литературы:

1. RFC 5936 — DNS Zone Transfer Protocol (AXFR) bo'yicha rasmiy texnik standartlar va xavfsizlik bo'yicha tavsiyalar.
2. DNS Security: Defending the Domain Name System — DNS protokoli hujumlari va himoya usullari haqidagi fundamental qo'llanma.
3. CISA (Cybersecurity & Infrastructure Security Agency) Guidelines — DNS infratuzilmasini himoya qilish bo'yicha kiberxavfsizlik ko'rsatmalari.
4. BIND 9 Administrator Reference Manual — DNS serverlarini xavfsiz sozlash bo'yicha amaliy qo'llanma.