EVIL TWIN (SOXTA ACSESS POINT)HUJUMLARI

Sobirjonov Begzod
FarDu Axborot tehnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Sobirova Dildoraxon Bahodirjon qizi
FarDu Axborot tizimlari va tehnologiyalari yo‘nalishi 2-bosqich talabasii
sobirova2007dildora@gmail.com

Annotatsiya. *Mazkur maqolada simsiz tarmoqlarda uchraydigan Evil Twin (soxta access point) hujumlari va ularning kiberxavfsizlikka ta’siri tahlil qilinadi. Ushbu hujum turi orqali foydalanuvchilarning shaxsiy ma’lumotlarini qo‘lga kiritish mexanizmlari ko‘rib chiqiladi. Shuningdek, Evil Twin hujumlarining ishlash prinsipi, xavf darajasi hamda ulardan himoyalanish usullari yoritiladi.*

Kalit so‘zlar: *Evil Twin, soxta access point, Wi-Fi xavfsizligi, kiberhujum, ma’lumotlar xavfsizligi, sniffing, MITM, tarmoq xavfsizligi.*

Аннотация. *В данной статье рассматриваются атаки типа Evil Twin (поддельная точка доступа) и их влияние на кибербезопасность. Анализируются методы перехвата пользовательских данных с помощью подобных атак. Также освещаются принципы работы, уровень угрозы и способы защиты от атак Evil Twin.*

Ключевые слова: *Evil Twin, поддельная точка доступа, безопасность Wi-Fi, кибератака, защита информации, MITM, сетевые угрозы.*

Annotation. *This article analyzes Evil Twin (fake access point) attacks and their impact on cybersecurity. It discusses the mechanisms of data interception through such attacks, as well as their working principles, threat levels, and protection methods.*

Keywords: *Evil Twin, fake access point, Wi-Fi security, cyber attack, data protection, MITM, network security.*

Kirish

Hozirgi kunda simsiz tarmoqlardan foydalanish keng tarqalgan bo‘lib, Wi-Fi texnologiyalari kundalik hayotning ajralmas qismiga aylangan. Biroq, ushbu qulaylik bilan bir qatorda turli xil kiberxavfsizlik tahdidlari ham ortib bormoqda. Shunday tahdidlardan biri — Evil Twin (soxta access point) hujumidir.

Evil Twin hujumi foydalanuvchilarni aldash orqali ularning shaxsiy va maxfiy ma’lumotlarini qo‘lga kiritishga qaratilgan. Ushbu hujum turi ayniqsa ochiq Wi-Fi tarmoqlarda keng tarqalgan bo‘lib, foydalanuvchilar uchun katta xavf tug‘diradi. Shu

sababli mazkur hujumni o‘rganish va undan himoyalanish usullarini ishlab chiqish dolzarb masalalardan biridir.

Asosiy qism

Evil Twin hujumi — bu hujumchi tomonidan haqiqiy Wi-Fi tarmog‘iga juda o‘xshash soxta access point yaratish orqali amalga oshiriladigan kiberhujum turidir. Foydalanuvchilar ko‘pincha tarmoq nomiga (SSID) e’tibor bermagan holda unga ulanadi va natijada hujumchining tuzog‘iga tushadi.

Birinchidan, hujumchi mavjud Wi-Fi tarmog‘ini aniqlaydi va uning nomidan foydalanib soxta tarmoq yaratadi. Ushbu tarmoq odatda kuchli signal bilan ta’minlanadi, bu esa foydalanuvchilarni aynan shu tarmoqqa ulanishga undaydi.

Ikkinchidan, foydalanuvchi soxta tarmoqqa ulangach, uning barcha internet trafigi hujumchi orqali o‘tadi. Bu jarayonda hujumchi “Man-in-the-Middle” (MITM) texnikasidan foydalanib, foydalanuvchi ma’lumotlarini kuzatishi va yozib olishi mumkin.

Uchinchidan, hujumchi foydalanuvchini soxta login sahifalariga yo‘naltirishi mumkin. Masalan, ijtimoiy tarmoqlar yoki bank sahifalariga o‘xshash interfeys orqali foydalanuvchi login va parollarini kiritadi, natijada ushbu ma’lumotlar hujumchi qo‘liga o‘tadi.

Evil Twin hujumlari ayniqsa quyidagi joylarda keng tarqalgan:

- kafe va restoranlar
- aeroport va vokzallar
- mehmonxonalar
- savdo markazlari
- ochiq Wi-Fi hududlari

Ushbu hujumning asosiy xavfi shundaki, foydalanuvchi hujum sodir bo‘layotganini sezmasligi mumkin. Natijada shaxsiy ma’lumotlar, bank rekvizitlari va boshqa muhim axborotlar o‘g‘irlanadi.

Himoyalanish usullari

Evil Twin hujumlaridan himoyalanish uchun quyidagi choralarni ko‘rish tavsiya etiladi:

- Faqat ishonchli va parol bilan himoyalangan Wi-Fi tarmoqlardan foydalanish
- VPN xizmatlaridan foydalanish
- HTTPS protokoliga ega saytlarni tekshirish
- Avtomatik Wi-Fi ulanish funksiyasini o‘chirish
- Ikki bosqichli autentifikatsiyani yoqish
- Shubhali tarmoqlardan uzoq turish
- Antivirus va xavfsizlik dasturlaridan foydalanish

Xulosa. Xulosa qilib aytganda, Evil Twin hujumlari zamonaviy kiberxavfsizlik muammolaridan biri bo‘lib, foydalanuvchilarning shaxsiy ma’lumotlariga jiddiy xavf

tug‘diradi. Ushbu hujumlar oddiy usullar bilan amalga oshirilishiga qaramay, katta zarar yetkazishi mumkin.

Shu sababli foydalanuvchilar Wi-Fi tarmoqlardan foydalanishda ehtiyotkor bo‘lishlari, shuningdek zamonaviy himoya vositalaridan foydalanishlari zarur. Kelajakda simsiz texnologiyalar rivojlanishi bilan bunday hujumlarga qarshi yanada samarali himoya mexanizmlarini ishlab chiqish muhim ahamiyat kasb etadi.

FOYDALANILGAN ADABIYOTLAR

1. Kiberxavfsizlik asoslari / R. Alimuhamedov, A. Abdullayev. – Toshkent: O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi nashriyoti, 2021.
2. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti professor-o‘qituvchilari tomonidan tayyorlangan **“Axborot xavfsizligi asoslari”** o‘quv qo‘llanma. – Toshkent, 2020.
3. O‘zbekiston Respublikasi Raqamli texnologiyalar vazirligi. **Axborot xavfsizligi bo‘yicha uslubiy qo‘llanmalar va tavsiyalar**. – Toshkent, 2022.
4. UZCERT – Kompyuter hodisalariga tezkor javob berish xizmati rasmiy sayti materiallari va tahliliy maqolalari. – https://uzcert.uz
5. O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi. **Kiberxavfsizlik fanidan o‘quv-uslubiy majmua**. – Toshkent, 2023.