EVIL TWIN (SOXTA ACCESS POINT) HUJUMLARI

Sobirjonov Behzod. Q
FarDu Axborot texnologiyalari kafedrasi o‘qituvchisi
behzodbekqahramonovich@gmail.com
Obidjonova Shalola Baxtiyorjon qizi
FarDu Axborot tizimlari va texnologiyalari yo‘nalishi
2-kurs talabasi shalolaobidjonova@gmail.com
https://doi.org/10.5281/zenodo.19887122

Annotatsiya. Ushbu maqolada “Evil Twin” (soxta kirish nuqtasi) hujumlari, ularning ishlash prinsipi, tarmoqlarda yuzaga kelish mexanizmi hamda axborot xavfsizligiga ta’siri tahlil qilinadi. Shuningdek, foydalanuvchilarning shaxsiy ma’lumotlarini himoya qilishda yuzaga keladigan asosiy xavf omillari ko‘rib chiqiladi. Maqolada soxta Wi-Fi tarmoqlarini aniqlash usullari va ulardan himoyalanish bo‘yicha zamonaviy yondashuvlar ham yoritiladi.

Kalit so‘zlar: Evil Twin, soxta Wi-Fi, axborot xavfsizligi, tarmoq hujumlari, simsiz tarmoqlar, kiberxavfsizlik, ma’lumotlarni himoya qilish.

Аннотация : В данной статье рассматриваются атаки типа “Evil Twin” (поддельная точка доступа), их принцип работы, механизм возникновения в сетях и влияние на информационную безопасность. Также анализируются основные риски утечки персональных данных пользователей. В статье описываются методы обнаружения поддельных Wi-Fi сетей и современные подходы к защите от таких атак.

Ключевые слова: Evil Twin, поддельный Wi-Fi, информационная безопасность, сетевые атаки, беспроводные сети, кибербезопасность, защита данных.

Annotation: This article examines Evil Twin (fake access point) attacks, their working principles, network implementation mechanisms, and impact on information security. It also analyzes the main risks of personal data leakage. The paper discusses methods for detecting fake Wi-Fi networks and modern approaches to protecting against such attacks.

Keywords: Evil Twin, fake Wi-Fi, information security, network attacks, wireless networks, cybersecurity, data protection

Kirish

Hozirgi kunda axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi natijasida simsiz tarmoqlar, xususan Wi-Fi texnologiyalari keng qo‘llanilmoqda. Ushbu texnologiyalar foydalanuvchilarga internetga tez va qulay ulanish imkonini yaratishi bilan birga, kiberxavfsizlik sohasida yangi turdagi tahdidlarning paydo bo‘lishiga ham sabab bo‘lmoqda. Shunday tahdidlardan biri “Evil Twin” (soxta kirish nuqtasi) hujumlaridir. Bu hujum turida tajovuzkor haqiqiy Wi-Fi tarmog‘iga o‘xshash nom, parametrlar va ba’zan bir xil sozlamalarga ega bo‘lgan soxta kirish nuqtasini yaratadi. Natijada foydalanuvchilar ushbu soxta tarmoqqa ishonch bilan ulanib, o‘zlarining shaxsiy va maxfiy ma’lumotlarini xavf ostiga qo‘yadilar. Evil Twin hujumlari asosan ochiq yoki himoyasi sust bo‘lgan simsiz tarmoqlarda, jumladan jamoat joylaridagi Wi-Fi nuqtalarida keng tarqalgan bo‘lib, bu holat foydalanuvchilarning login, parol, bank ma’lumotlari va boshqa muhim axborotlarining o‘g‘irlanishiga olib kelishi mumkin. Mazkur maqolada Evil Twin hujumlarining ishlash prinsipi, ularni amalga oshirish mexanizmlari hamda ulardan himoyalanish usullari ilmiy jihatdan tahlil qilinadi. Shuningdek, simsiz tarmoqlarda axborot xavfsizligini ta’minlash bo‘yicha zamonaviy yondashuvlar ham ko‘rib chiqiladi.

Asosiy qism

Axborot xavfsizligi bo‘yicha adabiyotlarda ta’kidlanishicha, simsiz tarmoqlarda hujumlarning asosiy zaifliklaridan biri foydalanuvchining tarmoqqa ulanish jarayonida autentifikatsiya mexanizmining yetarlicha tekshirilmasligidir (Stallings, 2022). Evil Twin hujumi aynan ushbu zaiflikdan foydalanadi. Evil Twin hujumida tajovuzkor haqiqiy Wi-Fi kirish nuqtasiga (Access Point) o‘xshash soxta kirish nuqtasini yaratadi. Bu soxta nuqta odatda bir xil SSID (tarmoq nomi) va ba’zan o‘xshash MAC manzil bilan sozlanadi. Foydalanuvchi qurilmasi avtomatik ravishda signal kuchi yuqoriroq bo‘lgan tarmoqqa ulanadi, natijada u haqiqiy emas, balki soxta tarmoqqa ulanib qoladi. Kurose va Ross (2021) asarlarida qayd etilishicha, simsiz tarmoqlarda “roaming” mexanizmi foydalanuvchi qurilmasini eng kuchli signalga ega tarmoqqa avtomatik ulaydi. Aynan shu holat Evil Twin hujumlarining muvaffaqiyatli amalga oshishiga imkon yaratadi**.**

Xulosa

Ushbu maqolada simsiz tarmoqlarda uchraydigan “Evil Twin” (soxta kirish nuqtasi) hujumlarining mohiyati, ishlash prinsipi, amalga oshirilish bosqichlari hamda ularning axborot xavfsizligiga ta’siri ilmiy jihatdan tahlil qilindi. Tahlillar shuni ko‘rsatadiki, ushbu hujum turi asosan foydalanuvchilarning simsiz tarmoqlarga avtomatik ulanishi va autentifikatsiya jarayonidagi zaifliklardan foydalanishga asoslanadi. Evil Twin hujumlari natijasida foydalanuvchilarning shaxsiy ma’lumotlari, login va parollari, shuningdek moliyaviy axborotlari xavf ostida qolishi mumkin. Ayniqsa, ochiq va shifrlanmagan Wi-Fi tarmoqlari ushbu turdagi hujumlar uchun qulay muhit yaratadi. Maqolada keltirilgan ma’lumotlar asosida shuni ta’kidlash mumkinki, Evil Twin hujumlarining oldini olish uchun zamonaviy shifrlash protokollaridan (WPA2/WPA3) foydalanish, VPN texnologiyasini qo‘llash hamda foydalanuvchilarning kiberxavfsizlik bo‘yicha bilimlarini oshirish muhim ahamiyat kasb etadi. Umuman olganda, simsiz tarmoqlarda axborot xavfsizligini ta’minlash kompleks yondashuvni talab etadi va bu jarayonda texnik himoya vositalari bilan bir qatorda foydalanuvchi xabardorligi ham muhim o‘rin tutadi.

Adabiyotlar, References, Литературы:

1. T. X. Alimuhamedov. “Axborot xavfsizligi asoslari”. Toshkent: O‘zbekiston Respublikasi Oliy va o‘rta maxsus ta’lim vazirligi nashriyoti, 2020.
2. A. A. Karimov. “Kompyuter tarmoqlari”. Toshkent: “Fan va texnologiya” nashriyoti, 2019.
3. Sh. S. Qodirov. “Axborot-kommunikatsiya texnologiyalari va xavfsizlik”. Toshkent: “O‘zbekiston” nashriyoti, 2021.
4. M. R. Xolmatov. “Kiberxavfsizlik asoslari”. Toshkent: Toshkent axborot texnologiyalari universiteti nashriyoti, 2022.
5. O‘zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. “Axborot xavfsizligi bo‘yicha o‘quv qo‘llanma”, 2023.