FISHING VA (SOCIAL ENGINEERING) IJTIMOIY MUHANDISLIKKA QARSHI KURASHISH TATU FARG‘ONA FILIALI

Umarov Abdumuxtor, Ro‘zaliyev Abdumalikjon, Qodirov Ahmadxon

ANNOTATSIYA

Fishing va (social engineering) ijtimoiy muhandislik kiber-xavf turlari kuzatilishi, aniqlanishi, va ularni oldini olishning strategiyalarini o‘rganishga qaratilgan maqola. Bu mavzu, kiber-xavf so‘rovnomalari orqali o‘z shaxsiy ma’lumotlaringizni himoyalashning ahamiyatini bildiradi va foydalanuvchilarga kiber-jarayonlar va kiber-hujumlar orqali xavfni kamaytirish uchun kerakli ko‘nikmalar va bilimlarni beradi.

Kalit So‘zlar. Fishing, social engineering, kiber-xavf, kuzatish, himoya, ma’lumot himoyasi, foydalanuvchi tartibi, xavfni oldini olish, shaxsiy ma’lumotlar, kiber-xavf turlari.

Ijtimoiy muhandislik hujumlari o‘z maqsadini tajovuzkor xohlagan narsani qilishga undash uchun aldash, majburlash va shunga o‘xshash usullardan foydalanadi. Tajovuzkor o‘zini hamkasbi, obro‘li shaxs, ishonchli sotuvchi yoki maqsad ishonadigan va yordam berishni xohlaydigan boshqa odam sifatida ko‘rsatishi mumkin. Shu bilan bir qatorda, tajovuzkor, agar nishon ularning xohish-istaklarini bajarmasa, maxfiy yoki zararli ma’lumotlarni oshkor qilish bilan tahdid qilishi yoki nishonga yordam berish uchun pora taklif qilishi mumkin.

Ijtimoiy muhandislik hujumlari turli yo‘llar bilan amalga oshirilishi mumkin. Ular kompyuterlarni jalb qilishi, telefondan foydalanishi yoki shaxsan yuz berishi mumkin. Misol uchun, o‘zini pochta tashuvchisi sifatida ko‘rsatish yoki kimdirdan eshikni ushlab turishni so‘rash xavfsiz hududga jismoniy kirish uchun mo‘ljallangan ijtimoiy muhandislik hujumlarining klassik namunasidir.

Fishing nima? Fishing hujumlari tajovuzkorning taklifini bajarish uchun maqsadni olish uchun zararli xabarlardan foydalanadi. Ko‘pincha, bu xabarlar o‘rnatilgan havola yoki zararli tarkibga ega biriktirilgan fayl bilan birga keladi. Agar foydalanuvchi havolani bossa yoki faylni ochsa, ular maxfiy ma’lumotlarni o‘g‘irlaydigan yoki kompyuteriga zararli dasturlarni o‘rnatadigan veb-sahifaga o‘tishi mumkin.

Biroq, barcha fishing hujumlari ushbu zararli havola yoki faylni talab qilmaydi. Ba’zilar foydalanuvchini aldash uchun mo‘ljallangan. Masalan, ishbilarmonlik elektron pochtasi (BEC) hujumlari ko‘pincha kompaniya uchun bajarilganligi taxmin qilingan xizmatlar uchun soxta hisob-fakturalarni o‘z ichiga oladi. Bu hisob-

fakturalarda zararli dasturlar mavjud emas, lekin agar qabul qiluvchi hisob-fakturaga ishonib to‘lasa, pul tajovuzkorga o‘tadi. Fishing odatda elektron pochta xabarlari bilan bog‘lanadi, ammo bu hujumlarni amalga oshirish uchun har qanday xabar almashish platformasidan foydalanish mumkin. Matnli xabarlar orqali fishing smishing (SMS fishing uchun) deb nomlanadi va ijtimoiy tarmoqlar, korporativ hamkorlik platformalari va shunga o‘xshash echimlar fishing hujumlarini amalga oshirish uchun ham ishlatilishi mumkin.

Ijtimoiy muhandislik va fishing. Ijtimoiy muhandislik va fishing o‘zaro bog‘liq tushunchalardir. Aslida, fishing ijtimoiy muhandislik hujumining o‘ziga xos turidir.

Ijtimoiy muhandislik tajovuzkor o‘z maqsadini tajovuzkorning taklifini bajarishga undash uchun foydalanadigan usullarni anglatadi. Fishing hujumi sodir bo‘lgan taqdirda, tajovuzkor qabul qiluvchiga havolalar, zararli qo‘shimchalar yoki boshqa turdagi aldamchi, jozibali yoki tahdid qiluvchi kontentni yuborish uchun xabar almashish platformasining ba’zi shakllaridan foydalanadi.

Fishing hujumlari ijtimoiy muhandislikning eng keng tarqalgan turi va bir nechta o‘zgarishlar, jumladan, nayzali fishing va kit ovidir. Biroq, ijtimoiy muhandislik hujumlarining boshqa shakllari ham mavjud, jumladan:

Piggybacking/Tailgating: Bu jismoniy ijtimoiy muhandislik hujumi bo‘lib, tajovuzkor qonuniy xodimni aldash orqali xavfsiz hududga kirish huquqiga ega bo‘ladi.

Pharming: Pharming hujumlari DNS o‘g‘irlash yoki boshqa usullar orqali qonuniy URL manzillarini tajovuzkor tomonidan boshqariladigan saytga yo‘naltiradi.

Pretexing: Pretexting tajovuzkor o‘zini boshqa birovga o‘xshatsa va bir qator potentsial hujumlarda qo‘llaniladigan usuldir.

Baiting: Ushbu hujumda tajovuzkor nozik ma’lumotlarni yoki boshqa harakatlarni taqdim etish evaziga nishonga qimmatli narsani va’da qiladi.

Ijtimoiy muhandislik hujumlarini qanday oldini olish mumkin

Tashkilotlar ijtimoiy muhandislik hujumlariga qarshi keng qamrovli himoya vositalarini amalga oshirishi mumkin, jumladan:

Xodimlarni tayyorlash: Ijtimoiy muhandislik hujumlari odatda yolg‘on va hiyla-nayrangga tayanadi. Xodimlarni ushbu hujumlarni tan olish va to‘g‘ri javob berishga o‘rgatish muvaffaqiyatli hujum xavfini kamaytiradi.

Elektron pochta xavfsizligi: Fishing ijtimoiy muhandislik hujumlarining eng keng tarqalgan shakllaridan biridir. Elektron pochta xavfsizligi yechimlari zararli xatlarni xodimning pochta qutisiga yetib borishidan oldin aniqlashi va bloklashi mumkin.

Hisob xavfsizligi: Fishing kabi ijtimoiy muhandislik hujumlari ko‘pincha foydalanuvchilarning hisoblari uchun kirish ma’lumotlarini o‘g‘irlash uchun mo‘ljallangan. Ko‘p faktorli autentifikatsiya, tarmoqqa ishonchsiz kirish va shunga

o‘xshash echimlardan foydalanish tajovuzkorning ushbu hisoblarga kirishi xavfini va agar ular muvaffaqiyatli bo‘lsa, etkazilishi mumkin bo‘lgan zararni kamaytirishi mumkin.

Yakuniy nuqta xavfsizligi: Ijtimoiy muhandislik hujumlari ko‘pincha korporativ tizimlarda zararli dasturlarni joylashtirish uchun ishlatiladi. Oxirgi nuqta xavfsizlik tizimlari ushbu zararli dastur infektsiyalarining oldini oladi va biznes uchun tahdidni yo‘q qiladi.

Veb xavfsizligi: Fishing xabarlaridagi zararli havolalar foydalanuvchilarni ma’lumotlarni o‘g‘irlaydigan yoki zararli dasturlarni etkazib beradigan zararli veb-saytlarga yo‘naltirishi mumkin. Brauzer ichidagi xavfsizlik zararli kontentni aniqlashi va foydalanuvchi qurilmasiga kirishini bloklashi mumkin.

Ma’lumotlarni yo‘qotishning oldini olish (DLP): Ijtimoiy muhandislik hujumlari ko‘pincha nozik ma’lumotlarni o‘g‘irlash uchun mo‘ljallangan. DLP yechimlari ruxsatsiz shaxslarga maxfiy ma’lumotlar oqimini aniqlashi va ma’lumotlar sizib chiqishini bloklashi mumkin.

Vazifalarni ajratish: BEC va boshqa ijtimoiy muhandislik hujumlari foydalanuvchini zararli harakatlar qilish uchun, aldash uchun mo‘ljallangan bo‘lishi mumkin. Hisob-fakturalarni to‘lash kabi muhim jarayonlarni turli xodimlarga tegishli bir necha bosqichlarga ajratish tajovuzkorni bir nechta maqsadlarni aldashga majbur qiladi va bu ularning muvaffaqiyat ehtimolini kamaytiradi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI: (REFERENCES)

1. Muxtarov, F., Umarov, A., & Ro‘zaliyev, A. (2023). AXBOROT TIZIMLARIDA XAVFSIZLIK TAHDIDLARINING TASNIFI.
2. Muxtorov, F. M. (2022, July). AXBOROT XAVFSIZLIGI XAVFLARINI TAHLIL QILISH UCHUN IERARXIK AKTIVLARNI BAHOLASH USULI. In INTERNATIONAL CONFERENCES (Vol. 1, No. 4, pp. 76-80).
3. Umarov, A. M. O. G. L. (2021). AXBOROT XAVFSIZLIGI XAVFINI BAHOLASH. Scientific progress, 2(8), 293-300.
4. AXBOROT XAVFSIZLIGIDA BIOMETRIK HIMOYA USULLARI, RA Vahobjon o‘g, UA Maxammad o‘g‘li, R Adaxanov - Proceedings of International Educators Conference, 2022
5. AXBOROTNI XIMOYALASH TIZIMINI ISHLAB CHIQISH, MF Muxammadovich, UA Maxammad o‘g‘li - Proceedings of International Educators Conference, 2022
6. BIOMETRIK BARMOQ IZI ORQALI AXBOROTLAR XAVFSIZLIGI, R Adaxanov - INTERNATIONAL CONFERENCES, 2022

7. Polvonov, A. (2023). CISCO PACKET TRACER uskunalar va aloqa kabellari. Engineering problems and innovations.
8. Qodirov AA. NEYRON TARMOQLARINI O‘RGANISHDA “TENSORFLOW” IMKONIYATLARIDAN FOYDALANISH. Scientific progress. 2021;2(8):287-92
9. Muhammadjon o‘g‘li, O. D., Olimjon o‘g‘li, A. I., & Marifjonovich, S. D. (2022). AHOLI SOG ‘LIG ‘INI SAQLASHDA TIBBIY TEXNIKALARNING O ‘RNI VA AHAMIYATI. Новости образования: исследование в XXI веке, 1(5), 1044-1046.6