Emro Science and Education
International open-access scientific journal
Journal homepage: https://journal.emro.uz

OPEN ACCESS

CONFERENCE PAPER OPEN ACCESS

Vol. 1 No. 1 (2023) · "Axborot oqimlari va intellektual tizimlarning ijtimoiy, iqtisodiy va texnik-texnol... DOI: 10.5281/zenodo.24319155

materiallar to'plami

ENG KENG TARQALGAN VEB-XAVFSIZLIK TAHDIDLARI - FISHING, RANSOMWARE.

Solijonov Madaminbek Botirjon o'g'li, Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali magistranti

Annotatsiya: Ushbu maqolada zamonaviy kiberhujumlar, ularning turlari haqida ma'lumotlar berilgan. Phishing, ransomware, kabi hujumlarning asosiy xususiyatlari va ta'siri tavsiflanadi. Shuningdek, maqolada kiberhujumlarning axborot tizimlariga ta'siri, ulardan himoyalanish bo'yicha choralar va tavsiyalar beriladi. Oddiy foydalanuvchi yoki tashkilot tizimlardagi zaifliklarni kamaytirishi va jiddiy zararni oldini olishi uchun qanday himoya usullaridan foydalanish mumkinligini bilib olishi mumkin. Ushbu maqola axborot xavfsizligi mutaxassislari, xavfsizlik menejerlari va o'zini kiber tahdidlardan qanday himoya qilish haqida ko'proq ma'lumot olishni xohlaydiganlar uchun foydali bo'lishi mumkin.

Kalit so'zlar: fishing, ransomware, smishing, kiberhujum, zararli dasturlar, shifrlash, deshifrlash.

Hozirgi jadal rivojlanib borayotgan zamonda, kundalik hayotimiz, sanoat, ishlab chiqarish va hizmat ko'rsatish sohalari ham birdek taraqqiy etib bormoqda. Bu esa axborot almashish jarayonini tezlashtirishni talab etadi, buning echimi sifatida web tizimlardan keng foydalanilmoqda. Web tizimlarning o'ta qisqa fursatda juda tez rivojlanishi esa turli qarashlar, farazlar hamda maqsadlarni keltirib chiqardi. Sohaning rivojlanishi bilan birga web tizimlarda ham turlicha xavsizlik muammolari yuzaga kela boshladi. Turli jinoyatchilik va firbgarliklarning ham raqamli ko'rinishlari paydo bo'ldi.

Texnologik innovatsiyalarning rivojlanishi o'sishda davom etar ekan, kiberjinoyatchilar yanada aqlli bo'lib bormoqda va bu butun dunyo bo'ylab veb-hujumlarning tezligini sezilarli darajada tezlashtirdi[1].

Eng keng tarqalgan veb-xavfsizlik tahdidlari - bu fishing, to'lov dasturi, Strukturaviy so'rovlar tili (SQL) in'ektsiyasi, saytlararo skript (XSS), tarqatilgan xizmat ko'rsatishni rad etish (DDoS) hujumlari, viruslar, qurtlar va josuslik dasturlari hisoblanadi.

Fishing hujumlari o'z nomi bilan baliq ovini eslatadigan jarayondir. Huddi baliq haqiqiy o'lja deb, qarmoqdagi xo'rakni tanlagani kabi foydalanuvchilar ham haqiyqiy tarmoqqa juda o'xshash bo'lgan qalbaki tarmoq qurboniga aylanishadi.

Phishing – foydalanuvchilarning maxfiy ma'lumotlarini olish uchun ularni aldashga asoslangan kiberhujumlarning bir turi hisoblanadi. Ko'pincha, bu kiberhujum banklar, ijtimoiy tarmoqlar yoki foydalanuvchi ishonadigan boshqa tashkilotlar nomidan rasmiy ko'rinishdagi elektron pochta xabarlarini yuborish orqali amalga oshiriladi. Ushbu elektron pochta xabarlari asl nusxaga o'xshash, lekin parollar, bank

Published: 10.11.2023

Cite this article: Solijonov Madaminbek Botirjon o'g'li (2023). Eng keng tarqalgan veb-xavfsizlik tahdidlari - fishing, ransomware. Emro Science and Education, 1(1). https://doi.org/10.5281/zenodo.24319155

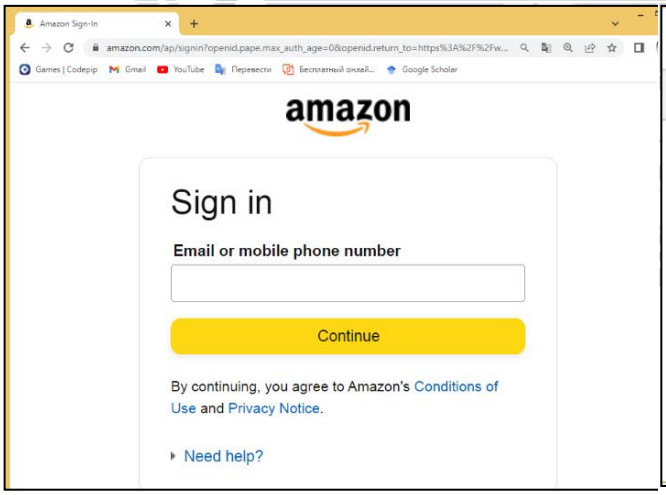
© 2023 The Author(s). Published by Emro Science and Education. This is an open access article.

karta raqamlari, manzillar va boshqa ma’lumotlar kabi shaxsiy foydalanuvchi ma’lumotlarini to‘playdigan saytlarga soxta havolalarni o‘z ichiga oladi[2].

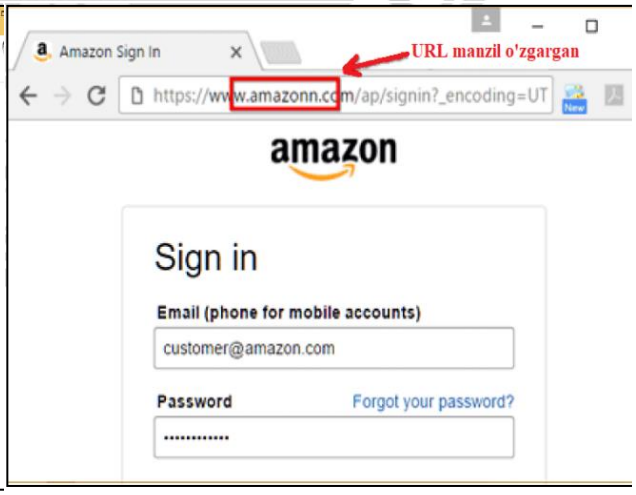
Fishing odatda elektron pochta xabarlari bilan bog‘lanadi, ammo bu hujumlarni amalga oshirish uchun har qanday xabar almashish platformasidan foydalanish mumkin. Matnli xabarlar orqali fishing smishing (SMS fishing uchun) deb nomlanadi va ijtimoiy tarmoqlar, korporativ hamkorlik platformalari va shunga o‘xshash echimlar fishing hujumlarini amalga oshirish uchun ham ishlatilishi mumkin[3].

Elektron pochta xabarlarida keng tarqalgan fishing amaliyoti foydalanuvchilardan hisob ma'lumotlarini yangilashni so'rashdir. Biroq, foydalanuvchilar kursorni havola ustiga olib borishsa, bu tashkilotning haqiqiy veb-saytiga emas, balki fishing tuzog'i saytiga olib keladi. Quyidagi rasmlarda fishingni yaxshiroq tushunish uchun misol ko‘rib chiqamiz. Dastlab haqiqiy amazon.com saytining ko‘rinishiga e’tibor qarating (1-rasm). Keyin esa fishing hujum uchun qurol vazifasini o‘tagan qalbaki “amazonn.com” saytini ko‘rishingiz mumkin (2-rasm). Texnik jihatdan bilimsiz yoki tajribasiz foydalanuvchi farqni sezmaydi va o‘zining shaxsiy ma’lumotlarini oshkor qilib qo‘yadi. Endi uning shaxsiy sahifasidan jinoyatchilar istagan maqsadlarida foydalanishlari mumkin. Achinarlisi, odatda bu kabi saytlarda bank kartalari ham ulangan bo‘ladi.

Fishingning turlari ko‘p bo‘lgani kabi undan himoyalanishning ham turli usul va himoyalanish bosqichlari mavjud. Masalan, elektron pochta xavfsizligi echimlari zararli xatlarni sizning pochta qutingizga etib borishidan oldin aniqlashi va bloklashi mumkin. Ko‘p bosqichli 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. Brauzer ichidagi xavfsizlik zararli kontentni aniqlashi va foydalanuvchi qurilmasiga kirishini bloklashi mumkin.



1 – rasm. Haqiqiy amazon.com sayti



2 – rasm. Soxta amazon.com sayti

materiallar to‘plami

Zararli dasturlarning eng mashhur va ommabop turlaridan yana biri bu ransomwaredir. So‘zma-so‘z tarjima qilinganda ransomware-to‘lov dasturi degan ma’noni bildiradi. Aslida esa zararli dastur bo‘lgan ransomware – bu kiberhujumlarning bir turi bo‘lib, unda kiberjinoyatchi foydalanuvchining fayllarini shifrlaydi va ularni ochish uchun to‘lov talab qiladi.

Kompyuterni zararlash jarayoni foydalanuvchi zararli fayl yoki virusli havolani ochganda boshlanadi. Keyin ransomware muhim fayllarga kirishni bloklaydi. Agar foydalanuvchi fayllarni shifrlash jarayonida virusni olib tashlashga harakat qilsa yoki shunchaki kompyuterni qayta ishga tushirsa, tizim butunlay ishdan chiqadi[2].

Ma’lumotlarni shifrlash ularni uzatish va saqlash vaqtida maxfiyligini ta'minlash uchun ishlatiladi. Afsuski, jinoyatchilar jabrlanuvchining ma'lumotlarini shifrlash va jabrlanuvchi to'lovni to'lagandan keyingina o'z ma'lumotlarini chiqarish hujumlari uchun shifrlashni qo'llagan.

1989-yilda Jozef Popp tomonidan ransomwarening birinchi namoyishi qurbonlarning qattiq disklarini o'g'irlash va to'lovni talab qilish uchun simmetrik kalitli shifrlashdan foydalangan. Simmetrik kalitli shifrlash - bu shifrlash va dekodlash uchun bir xil kalitdan foydalanadigan yagona kalitli tizim bo'lib, uning o'ziga xos zaif tomoni bor, chunki shifrlash (parchalash) kaliti ransomware bilan birga joylashtirilgan bo‘ladi.

Ransomware - bu onlayn jinoiy faoliyat orqali foyda topiladigan biznes. Jinoyatchilar oson daromad olishga intilishadi, shuning uchun to'lov usuli (monetizatsiya) muhim ahamiyatga ega. Yuqorida aytib o'tilgan, Jozef Poppning birinchi to'lov talabi pochta qutisi orqali bo'lgan, bu ishonchli emas, chunki politsiya jismoniy joylashuvni kuzatishi va to‘lov sodir bo'lganda jinoyatchini qo‘lga olishi mumkin.

2005-yilda jinoyatchilar nosimmetrik shifrlashdan foydalangan ransomware hujumini (Gpcoder) boshladilar, bu esa Gpcoder ransomwareini tahlil qilish va qarshi chora ko'rish orqali qisqa vaqtda bartaraf etildi. Keyin 2006-yilda jinoyatchilar assimetrik shifrlash deb nomlangan yanada mustahkamroq shifrlash usulini qo'llashdi. Asimmetrik shifrlashda matematik bog'langan ikkita shifrlash kaliti (ochiq va shaxsiy kalitlar) qo'llaniladi. Ochiq kalit ma'lumotlarni shifrlash uchun ishlatiladi va ma'lumotlarni deshifrlash uchun foydalanilmaydi va shuning uchun ochiq kalit maxfiy kalit haqida hech qanday ma'lumotni sezdirmasdan uzatilishi mumkin. Maxfiy kalit faqat ma'lumotlarni dekodlash uchun ishlatiladi va to'lov to'lanmaguncha yashirin saqlanadi[4].

Ko‘pincha, kiberjinoyatchilar identifikatsiya qilish va jinoiy javobgarlikka tortish jarayonini murakkablashtirish uchun kriptovalyutada to‘lovni talab qilishadi. Biroq, to‘lov to‘lanishiga qaramay, ma’lumotlarni tiklash kamdan-kam hollarda sodir bo‘ladi. Ransomware nihoyatda makkor va zararli dastur bo‘lib, odatda fishing elektron pochta xabarlari orqali tarqalsa ham, u biznesdagi zaifliklar va orqa eshiklardan ham foydalanadi.

materiallar to‘plami

Fishing hamda ransomware qurboni bo‘lmaslikning birinchi sharti etarli malakaga ega bo‘lishdir. Xodimlarni ushbu hujumlarni taniy olish va to‘g‘ri javob berishga o‘rgatish muvaffaqiyatli hujum xavfini kamaytiradi. Shuningdek shubhali fayllar yoki havolalarni ochmaslik ham muhim, ayniqsa ularni jo‘natuvchisi noma’lum bo‘lganda. Kiberhujum sodir bo‘lgan taqdirda, darhol virus tarqalishini to‘xtatish va zararni kamaytirishga yordam beruvchi axborot xavfsizligi mutaxassislariga murojaat qilish zarur.

Adabiyotlar:

1. Solijonov Madaminbek Botirjon o‘g‘li. A study of security issues in web systems. Finland, Helsinki international scientific online conference "Sustainability of education socio-economic science theory", Part 11 october 7th Colletions of scientific works, Helsinki 2023.
2. G‘ulomov Sherzod Rajaboyevich, Normirzayev Farrux Abdurahimovich. Zamonaviy kiberhujumlar va ularga qarshi himoya choralari. Raqamli Transformatsiya va Sun’iy Intellekt ilmiy jurnali, Sep 20, 2023.
3. Umarov Abdumuxtor, Ro‘zaliyev Abdumalikjon, Qodirov Ahmadxon. Fishing va (social engineering) ijtimoiy muhandislikka qarshi kurashish. Educational Research in Universal Sciences, volume 2 | special issue 12 | 2023.
4. Philip O'Kane, Sakir Sezer, Domhnall Carlin. Evolution of ransomware. doi: 10.1049/iet-net.2017.0207, The Institution of Engineering and Technology 2018

materiallar to‘plami

TADBIRKORLIK VA KICHIK BIZNES BOSHQARUVINI RAQAMLASHTIRISHNI TAKOMILLASHTIRISH

Andijon mashinasozlik institute, “Axborot texnologiyalari” kafedrasi assistenti
Yuldashev Mirzohid Maxmudjonovich

Annotatsiya: Maqolada tadbirkorlik korxonalarini boshqarishda qo‘llaniladigan strategiyalarning metodlari yoritib o‘tilgan. Shuningdek, tadbirkorlik faoliyatida strategiyalarni shakllantirish usullari, ularning afzallik tomonlari bayon etilgan. Sohada strategiyani shakllantirish uchun tegishli tavsiyalar ishlab chiqilgan.

Kalit so‘zlar: Innovatsion marketing , kichik biznes , kichik biznes subyektlari , bozor , tovar , marketing , korxona , reklama , firma , samaradorlik , raqamli iqtisodiyot , xususiy sektor , mobil va raqamli texnologiyalar , raqamli biznes .

Kirish Mamlakatimizning tadbirkorlik, ishbilarmonlik muhitidagi keskin o‘zgarishlar raqobat, axborot texnologiyalari, biznesni globallashuvi va boshqa ko‘plab omillarning rivojlanishi bilan bog‘liq bo‘lib, bu boshqaruv strategiyasining ahamiyatini orttirib bormoqda. Bu tadbirkorlik faoliyatidagi beqaror sharoitlarning o‘sib borishi bilan firmalarning menejment strategiyasiga e’tiborini kuchaytirmoqda. Strategik boshqaruvtadbirkorlik faoliyatining menejment, marketing, iqtisodiyot, moliyaviy qirralari va axborot texnologiyasini birlashtiruvchi integratsion boshqaruvdir. Strategik boshqaruv doimo rivojlanib boradi. Tadbirkorlik faoliyatini rivojlantirishda strategik boshqaruvning yangi usul va uslublarini ishlab chiqish katta ahamiyatga egadir. Uni shakllantirish tamoyillariga asoslanib, ijtimoiy-iqtisodiy rivojlanish strategiyalari ishlab chiqiladi. Tadbirkorlik faoliyatidagi quyidagi omillar boshqaruv strategiyasining shakllantirishni dolzarbligini ifodalaydi: - XX asrning ikkinchi yarmida korxona ichki va tashqi muhitidagi o‘zgarishlar oqibatida vazifalar soni muttasil oshib bordi. Ularning ko‘pchiligi tubdan yangi bo‘lib, XX asrning birinchi yarmida orttirilgan tajriba asosida hal etib bo‘lmas edi; - bazifalarning ko‘pligi milliy iqtisodiyotlar faoliyatining geografik ko‘lamini kengaytirish bilan birga boshqaruv muammolarining yanada murakkablashuviga olib keldi; - XX asrning birinchi yarmida orttirilgan boshqaruv ko‘nikma va malakalari yuzaga kelgan muammolarni hal qilish shartlariga kamroq mos kelib, yuqori boshqaruv bo‘g‘inining roli ortib bordi; - tashqi muhitning beqarorligi kuchaydi, bu esa keskin strategik o‘zgarishlar ehtimolliligini oldindan bashorat qilib bo‘lmasligini oshirdi.

“2022 – 2026 – yillarga mo‘ljallangan Yangi O‘zbekistonning taraqqiyot strategiyasi ”da 29 – maqsadi sifatida Tadbirkorlik faoliyatini tashkil qilish va doimiy daromad manbalarini shakllantirish uchun sharoitlar yaratish , xususiy sektorning Yalpi ichki mahsulotdagi ulushini 80 foizga va eksportdagi ulushini 60 foizga etkazish belgilangan. Raqamli iqtisodiyot sharoitida faol tadbirkorlikni shakllantirish va rivojlantirishda kichik biznes va tadbirkorlikda marketing faoliyatini tashkil etish muhim ahamiyatga egadir . So‘ngi yillarda raqamli iqtisodiyot tez suratlarda o‘sib bormoqda. Raqamli iqtisodiyotning o‘sishi raqamli va mobil texnologiyalar bilan bevosita bog‘liq bo‘lgan texnologiyalar rivojlanishining hozirgi bosqichida va bozorlarning hozirgi holati sharoitida raqamli iqtisodiyotni maqsad sifatida emas, balki iqtisodiy faoliyat samaradorligini oshirish vositasi sifatida ko‘rib chiqish kerak.