Kiberdələduzluq : Özünüzü necə qorumalısınız?

Maliyyə Monitorinqi Xidməti öhdəlik daşıyan şəxslər tərəfindən təqdim edilən şübhəli hesabatlar əsasında son bir il ərzində ölkəmizdə baş verən və insanların maddi zərərə uğramasına səbəb olan müxtəlif kiberdələduzluq halları barədə məlumatları təhlil etmişdir.

Prezentasiyada əsas kiberdələduzluq üsulları və onların törədilməsinə dair misallar, habelə onlardan qorunmaq üçün tövsiyələr təqdim edilir.

Fişinq

Fişinq (*ing.* *Phishing*) balıq ovunu xatırladan dələduzluğun bir növüdür.

Dələduzlar (fişerlər) istifadəçiləri aldadaraq onların kredit kartı, parol, bank hesabı və digər şəxsi məlumatlarını ələ keçirirlər.

Adətən, bu cür dələduzluq bank, onlayn mağaza və ya digər təşkilatların veb-saytlarını təqlid edən saxta saytların yaradılması və ya istifadəçilərə rəsmi qurumların adından saxta e-poçtlar göndərilməsi ilə həyata keçirilir.

! Unutmayın ki, banklar, dövlət qurumları və böyük şirkətlər sizdən heç vaxt e-poçt və ya SMS vasitəsilə gizli məlumatlarınızı (şifrə, kart nömrəsi və s.) tələb etmir.

Misal 1: Saxta zənglər

Əsasən vətəndaşlara xidmət göstərən maliyyə institutları və təşkilatların adından saxta telefon zəngləri vasitəsilə həyata keçirilir.

Dələduzlar özlərini bank və ya digər səlahiyyətli qurumun əməkdaşı kimi təqdim edərək, müxtəlif bəhanələrlə (guya hədiyyə qazandıqları, hesablarına yanlış ödəniş daxil olduğu, hesablarının kibertəhlükə altında olduğu və s.) vətəndaşların fərdi mobil bankçılıq məlumatlarını, ödəniş kartı rekvizitlərini və digər şəxsi hesab məlumatlarını əldə etməyə çalışırlar. Əldə olunan bu məlumatlardan istifadə etməklə dələduzlar vəsaitləri zərərçəkmişin hesablarından öz nəzarət etdikləri hesablara yönləndirirlər.

Misal 2: Elan saytlarında alqı-satqı

Əsasən ikinci əl malların, əmlakın və ya avtomobillərin alqı-satqısının aparıldığı onlayn veb səhifələr üzərindən həyata keçirilir. Dələduzlar özünü alıcı kimi təqdim edərək, elan yerləşdirən şəxslərlə əlaqə saxlayır (əksər hallarda zənglər xarici mobil operatorlardan daxil olur) və müvafiq malı almaqda maraqlı olduqlarını bildirirlər. Onlar satıcıya ilkin ödəniş etməyə razı olduqlarını deyərək, ödənişin həyata keçirilməsi üçün satıcının bank kartı məlumatlarını — kart nömrəsini, son istifadə tarixini və kartın arxa tərəfindəki 3 rəqəmli təhlükəsizlik kodunu (CVV) tələb edirlər. Satıcının kart məlumatlarını əldə etdikdən sonra dələduzlar həmin hesabdan vəsaitləri öz nəzarətlərində olan hesablara köçürürlər.

Bu cinayətin digər geniş yayılmış forması isə dələduzların elanlarda malları real dəyərindən xeyli aşağı qiymətə təklif etməsi ilə bağlıdır. Belə hallarda onlar əmlaka maraq göstərən şəxslərin çox olduğunu bildirir və ilkin ödənişi (beh) ilk edən şəxsə malın satılacağını deyirlər. Beləliklə, alıcı tərəfindən köçürülən ilkin vəsait dələduzlar tərəfindən ələ keçirilir.

Misal 3: İşə düzəltmə adı ilə onlayn dələduzluq

Əsasən elan veb səhifələri və ya sosial şəbəkələr üzərindən törədilir. Belə ki, dələduzlar müxtəlif iş elanları platformalarında özlərini insan resursları üzrə ixtisaslaşmış şirkət kimi təqdim edərək iş axtaran şəxslərə “komissiya” qarşılığında iş təklif edirlər.

Bu cür elanlar əsasında dələduzlar əvvəlcə vətəndaşlardan şəxsi məlumatlarının və CV-lərinin düzgün şəkildə doldurulması üçün komissiya ödənişi tələb edir, daha sonra isə həmin şəxsin guya artıq işə qəbul olunduğunu bildirərək əlavə ödəniş (işə qəbul haqqı və ya sənədləşmə xərci adı altında) tələb edirlər.

İş axtaran şəxsi inandırmaq məqsədilə dələduzlar saxta şirkət adından zəng edir, bəzi hallarda isə saxta elektron poçt və ya onlayn görüşlər vasitəsilə rəsmi prosedur görüntüsü yaradır və qarşı tərəfdən məlumatlarını onlayn təqdim etməsini istəyirlər. Şəxs işə qəbul edildiyinə inandıqdan sonra isə tələb olunan vəsaitlər dələduzların nəzarətində olan hesablara köçürülür.

Tövsiyələr

✓ Ödəniş kartlarının tam məlumatlarını, xüsusilə də CVV kodunu heç bir halda paylaşmayın

✓ Şübhəli linklərə klikləməyin

✓ Asan və yüksək gəlirli iş elanlarını nəzərdən keçirməyin, elan yerləşdirmiş şirkətlər barədə açıq mənbələrdə olan məlumatları araşdırın

✓ Adlarından istifadə edilən qurumların rəsmi əlaqə nömrələri ilə əlaqə saxlayıb daxil olan zəngin həqiqiliyini təsdiqləyin

✓ Saytın dizaynına nəzər yetirin, adətən Fishing saytlarının dizayn detalları az da olsa oriqinal saytlardan fərqlənir

✓ Şəxsi məlumatları yalnız etibarlı saytlarda daxil edin

Deepfake

Deepfake – süni intellektlə yaradılmış saxta video, audio və ya şəkillərdir.

Bu texnologiya, adətən, insan üzünü və ya səsin başqa bir insanla əvəz etmək üçün istifadə olunur.

Sosial şəbəkələrdə profiliniz açıqdırsa, səsinizin olduğu istənilən video və ya audio yazısı hər kəs tərəfindən asanlıqla əldə edilə bilər. Bu isə dələduzlar üçün material toplamağa şərait yaradır.
Bütün sosial media platformalarında (məsələn, Instagram, Facebook, TikTok) hesabınızın gizlilik parametrlərini yoxlayın. Kontentinizin yalnız dostlarınız və ya izləmək üçün icazə verdiyiniz şəxslər tərəfindən görünməsini təmin edin.

Misal 4: Tanıdığınız şəxslərin adından istifadə

“Deepfake” funksionallıqları vasitəsilə dələduzlar insanlara onların qohumları, dostları, tanışları adından zəng edirlər. Bu yolla, müxtəlif bəhanələrdən istifadə etməklə (məsələn, təcili maliyyə ehtiyacı, qəza, hüquqi məsələ və s.) dələduzlar zərərçəkmişləri inandıraraq onların hesablarındakı vəsaitləri öz nəzarətlərində olan hesablara köçürülməsinə nail olurlar.

Bu texnologiyalar həm telefon zəngləri, həm də sosial mesajlaşma platformaları (məsələn: WhatsApp, Messenger, Telegram və s.) vasitəsilə istifadə oluna bildiyindən, dələduzlar tərəfindən insanları manipulyasiya etmək üçün geniş şəkildə tətbiq olunur.

Misal 5: Virtual tanışlıq

Dələduzlar real və ya “Deepfake” və ya “Voice Cloning” kimi süni intellekt texnologiyalarından istifadə etməklə cazibədar, diqqətçəkici və bəzən məşhur şəxslərin adından saxta profillər yaradır və tanışlıq saytlarında qeydiyyatdan keçmiş şəxslərlə əlaqə qurur.

Dələduzlar bu yolla tanış olduqları şəxslərdə etimad formalaşdırır, daha sonra isə müxtəlif üsullarla onlardan şəxsi və həssas məlumatlar (məsələn: foto, video, səs yazısı və s.) əldə edirlər. Ardınca dələduzlar həmin məlumatların sosial şəbəkələrdə yayılması ilə hədə-qorxu gələrək vətəndaşdan pul tələb edirlər.

Misal 6: Saxta saytlar və linklər

Dələduzlar mal və (ya) xidmət təqdim edən müxtəlif ödənişlərin həyata keçirildiyi platformalara vizual baxımdan oxşar, adında adətən 1-2 simvol fərqi olan saxta (klonlaşdırılmış) veb səhifələr yaradırlar. Bir çox hallarda istifadəçilər müxtəlif axtarış platformalarında (məsələn: Google, Yandex və s.) sorğu edərkən və ya internet saytlarında yerləşdirilmiş saxta reklam bannerlərinə klikləməklə saxta veb səhifələrə yönləndirilirlər.

Bu səhifələr, dizayn və funksionallıq baxımından rəsmi platformalara çox oxşadığı üçün vətəndaşlar onları real səhifələrdən fərqləndirməkdə çətinlik çəkirlər. Bundan başqa, zərərçəkənlər veb ünvanın adında olan kiçik fərqlərə (məsələn: bir hərf fərqi, əlavə simvol və s.) diqqət yetirmədiklərindən, həmin səhifə vasitəsilə etdikləri ödənişlər birbaşa dələduzlara məxsus hesablara köçürülür.

Misal 7: Şirkətlərə qarşı dələduzluq

Müxtəlif şirkətlərin və ya şəxslərin elektron poçt ünvanlarına vizual baxımdan oxşar (adətən 1-2 simvol fərqi ilə) saxta elektron poçt ünvanlarının yaradılması və bu ünvanlardan istifadə edilməklə onların adından çıxış edilməsidir. Bu yolla dələduzlar saxta invoyslar və bank rekvizitləri təqdim edərək, hüquqi şəxslərin maliyyə vəsaitlərinin öz hesablarına köçürülərək ələ keçirilməsinə nail olurlar.

Tövsiyələr

✓ Ucuz elanlara aldanmayın və beh ödəməyin

✓ Maddi yardın xahiş edən şəxslərlə digər əlaqə nömrələri vasitəsilə əlaqə saxlayıb daxil olan zəngin həqiqiliyini təsdiqləyin

Ünvan sətrində linkə fikir verin – sadəcə bir simvol saxta saytı həqiqidən fərqləndirməyə imkan verə bilər

✓ Sosial şəbəkələrdə səsinizin açıq şəkildə eşidildiyi videoları paylaşmayın

✓ Tanımadığınız şəxslərlə həssas məlumatlarınızı paylaşmayın

✓ Biznes tərəfdaşınız tərəfindən elektron poçt vasitəsilə yenilənmiş bank rekvizitləri təqdim edilərkən, poçt ünvanının yazılışına fikir verin, ödəniş etməzdən öncə tərəfdaşınız ilə digər kommunikasiya alətləri vasitəsilə əlaqə yaradın

Hər zaman maliyyə savadlılığınızın artırılması üzərində çalışın

Xəbər saytları və sosial şəbəkələrdə baş verən dələduzluq halları barədə xəbərləri oxuyun

Rəsmi dövlət qurumlarının, maliyyə sektoru iştirakçılarının xəbərdarlıqlarını nəzərə almağa çalışın

DƏLƏDUZLARIN QURBANI OLMAYIN!