DOI: https://doi.org/10.36719/2789-6919/20/179-182

Tacir Alıyev
Azərbaycan Texniki Universiteti
magistrant
aliyevtacir041@gmail.com

SOSİAL MÜHƏNDİSLİK HÜCUMLARI

Xülasə

Bəzi mənbələrə əsasənlanaraq, biz kiberdələduzluq sahəsini fəal inkişaf etmiş kimi təsvir edirik. Bir çox mənbələrə əsaslanaraq bu sahədə olan bəzi məqamlara nəzər yetirək. Həmçinin məqalədə Amerikanın Purplesec analitik şirkətinin sosioloji araşdırmaları və tədqiqatları da yer alır. Sosial mühəndislik kompyuter informasiya sahəsində cinayətlərin törədilməsi metodu kimi baxılır. Hər bir sahənin növləri və üsulları olduğu kimi sosial mühəndislik sahəsinində bir neçə üsulları vardır. Sosial mühəndislik təcrübəsinin xüsusən səkkiz texnikası (metodları): fişinq, səsli saxtakarlıq, uydurmaq, hiyləgər, qəsbçi, həvəsləndirici bəxşiş, aldatmaq, əks sosial mühəndislik vurğulanır və təsvir olunur. Ümumiyyətlə çalışıb hakerlərin bu üsullarından uzaq durmaq lazımdır.

Açar sözlər: *sosial mühəndislik, kibercinayətkarlıq, sosial mühəndislik texnikaları, kiber fırıldaqçı, sosial mühəndislik üsulları, informasiya təhlükəsizliyi*

Tajir Aliyev
Azerbaijan Technical University
master sudent
aliyevtacir041@gmail.com

Social engineering attacks

Abstract

Based on some sources, we describe the field of cyber fraud as actively developing. Let’s look at some points in this area based on many sorces. The article also includes sociological studies and research by the American analyst company Purplesec. Social engineering is viewed as a method of committing crimes in the field of computer information. Just as every field has its types and methods, there are several methods in the field of social engineering. Eight techniques (methods) of social engineering practice in particular are highlighted and described: phishing, voice spoofing, spoofing, trickery, extortion, incentive giving, deception, reverse social engineering. In general, you should try to stay away from these methods of hackers.

Keywords: *social engineering, cybercrime, social engineering techniques, cyber fraudster, social engineering methods, information security*

Giriş

Sosial mühəndislik şəxsi məlumatları, giriş və ya qiymətli əşyaları əldə etmək üçün insan səhvindən istifadə edən bir manipuliyasiya üsuludur. Kibercinayətkarlıqda bu “insanların sındırılması” prosesinə bənzədilir, zərərli proqram infeksiyalarını yaymağa və ya məhdudlaşdırılmış sistemlərə giriş imkanı verməyə sövq edir. Hücumlar onlayn, şəxəsn və digər qarşılıqlı əlaqə yolu ilə baş verə bilər. Sosial mühəndisliyə əsaslanan fırıldaqlar insanların necə düşündüyü və hərəkət etdiyi ətrafında qurulur. Beləliklə, sosial mühəndislik hücumları istifadəçilərin davranışın maipuliyasiya etmək üçün xüsusilə faydalıdır. Təcəvüzkar istifadəçinin hərəkətlərini nəyin motivasiya etdiyini başa düşdükdən sonra istifadəçini aldada və effektiv bir şəkildə manipuliyasiya edə bilər.

Sosial mühəndislik. Bu gün müasir həyatı informasiya-kommunikasiya texnologiyaları olmadan təsəvvür etmək mümkün deyil. Bütün dünya praktiki olaraq informasiya axınları ilə

"örtülüb" və vəzifəsi məlumatın ötürülməsi, toplanması, təhlili və saxlanmasıdır. Hal-hazırda istənilən dövlətin prioritet vəzifəsi vətəndaşlarının informasiya təhlükəsizliyini təmin etməkdir.

Hər il daha çox kibercinayətlər baş verir. Rusiya Daxili İşlər Nazirliyinin statistikasına əsasən, 2017-ci ildə kompüter informasiyası sahəsində 1883 cinayət qeydə alınıb, 2018-ci ildə - 2 min 5002, 2019-cu ildə informasiya və telekommunikasiya texnologiyalarından istifadə etməklə və ya kompüter informasiyası sahəsində törədilmiş 294 min 409 cinayət, məhkəmələrə göndərilmiş cinayyətlər isə 57 min 2213, 2020-ci ilin yanvar-iyul aylarında isə 272 min 737, məhkəmələrə göndərilmiş 47 min 98, qalan 87% isə açıqlanmamış qalır.

Statistik göstəricilərə görə kibercinayətkarlıq sferasının nə qədər sürətlə inkişaf etdiyi aydın hiss olunur ki, cinayət işlərinin məhkəməyə göndərilməsinin göstəriciləri haqqında bunu demək mümkün deyil. Rusiya Daxili İşlər Nazirliyinin statistik verilənlərini təhlil etdikdən sonra, bildirirəm ki, kibercinayətlərlə bağlı cinayətlərin araşdırılması çətindir. Bunun üçün də hüquq-mühafizə orqanlarına kompüter texnologiyaları sahəsində kifayət qədər intellektual potensiala malik kadrlar lazımdır.

Şəxsi məlumat əldə etmək, nəyəsə giriş əldə etmək üçün texniki sındırma üsullarından istifadə etmədən insan psixologiyasını idarə etməyin bacarıqlı üsulu sosial mühəndislik adlanır. Sosial mühəndislik insan zəifliklərinə, maraqlarına, diqqətsizliyinə, sadəlövhlüyünə, qeyri-ciddiliyinə yönəlmişdir (Sozaev, Kunaşev, 2020: 85-88).

90-cı illərdə Məşhur kibercinayətkar Kevin Mitnik, sonradan təhlükəsizlik üzrə məsləhətçiyə çevrildi və "sosial mühəndislik" terminini ilk dəfə populyarlaşdıran şəxs olmuşdur. O hesab edirdi ki, heç bir texniki kod cinayətkarın psixoloji bacarıqları və vərdişləri kimi insanı aldada bilməz (Mitnik, Simon, 2004: 360).

Bu gün sosial mühəndislik (98%) kibercinayətkarların istifadə etdiyi üsullar arasında hələ də populyardır.

Amerikanın "Purplesec" analitik şirkəti dünya İT mütəxəssisləri arasında müsahibələr və sorğular keçirib. Onların 43%-i müxtəlif vaxtlarda sosial mühəndislik hücumlarının hədəfi olduqlarını bildirib. Respondentlərin 60%-i yeni işə qəbul edilənlərin bu cür hücumlara ən çox həssas olduğuna və işlədikləri şirkətləri riskə atdıqlarına inanırlar. Təəssüf ki, işçilərin yalnız 3%-i zərərli e-poçtları şirkət rəhbərliyinə bildirir.

Purplesec həmçinin müəyyən etmişdir ki, şirkətlərdə indiki və ya keçmiş İT mütəxəssislərinin 21%-i sosial mühəndislikdən maliyyə üstünlüyü əldə etmək, qisas almaq, maraqdan ötrü və ya əylənmək üçün istifadə edir.

Ənənəvi olaraq kriminalistikada cinayətin törədilməsi metodu dedikdə "ətraf mühit şəraiti və xassələri və şəxsiyyətin xassələri ilə müvafiq alətlərdən, vasitələrdən, yer və zaman şərtlərindən istifadə ilə əlaqələndirilə bilən müəyyən edilən ictimai təhlükəli əməlin hazırlanması, törədilməsi və gizlədilməsi üzrə hərəkətlər sistemi başa düşülür" (Zuikov, 1970: 31).

Sosial mühəndislik üsulları. Kibercinayətkarların ən çox istifadə etdiyi sosial mühəndislik üsullarına nəzər salaq. Bunlara əsasən aşağıdakılar daxildir:

1. Fişinq (elektron məktubların kütləvi şəkildə e-poçtlara göndərilməsi, mətn mesajları, "sualtı ovlama").

Fişinqlik sosial mühəndisliyin ən məşhur yoludur. IT sahəsində çalışan mütəxəsislərin, insanların 56%-nin fikrincə, məqsədyönlü-fişinq hücumları informasiya təhlükəsizliyi üçün əsas təhlükədir. Purplesec şirkəti dünya üzrə respondentlərin fikirlərini təhlil edib və fişinq hücumları haqqında araşdırma aparıb və belə nəticəyə gəlib ki, 2017-ci ildə respondentlərin 76%-i, 2018-ci ildə isə 83%-i fişinq hücumlarına məruz qalıb.

Zərərli əlavələrin, hansı ki, fişinq hücumları bunlar vasitəsilə həyata keçirilir ən çox yayılmış növləri bunlardır:

"ofis" - 38%;
arxiv - 37%;
PDF faylları - 14%;
icra edilə bilən fayllar - 4%

E-poçt fişinqinin məqsədi mesajı şəxsin güvəndiyi şirkət və ya təşkilat tərəfindən göndərilmiş kimi göstərmək üçün çox sayda insana e-poçt ünvanına spam mesajlar göndərməkdir. Belə e-poçtları indi tanınmış şirkətlərin əvvəlcədən hazırlanmış e-poçt şablonlarını ehtiva edən hazır "fişinq dəstləri" vasitəsilə yaratmaq asandır. Belə spam e-poçtda istifadəçi adlarını və parolları toplamaq üçün hazırlanmış fişinq saytına keçid var. Fişinq saytlarının təxminən 50%-i HTTPS texnologiyasından da istifadə edir (Hadnagy, 2010).

Fişinq SMS mətn mesajları (Smishing) planşet, smartfon və ya smart saatda yayılan bir fişinq növüdür. Belə hücumlarda qurbanlar adətən naməlum göndəricidən qalib olduqları müsabiqə haqqında hər hansı xüsusi təklif şəklində onlara məlumat verən mətn mesajı alırlar. Bu zaman həmin mətndə giriş üçün qeydiyyat verilənlərini toplamaq üçün nəzərdə tutulmuş saxta (güzgü) sayta keçid olur və bu ilk baxışdan orijinal kimi görünür.

2. Vişinq (Vishing) (səs fişinqi) zərərçəkənin şəxsi və maliyyə məlumatlarına giriş əldə etmək üçün telefon şəbəkəsində sosial mühəndislikdən istifadədir. Bu hücum həmçinin kibercinayətkarlar tərəfindən kəşfiyyat məqsədləri üçün təşkilat və ya şirkət haqqında məlumat toplamaq üçün istifadə olunur.

3. Sosial mühəndisliyin az populyar olmayan başqa bir üsulu bəhanədir. Bu, cinayətkarın hərəkətlərinin əvvəlcədən yaxşı yazılmış ssenarisidir, nəticədə 80% hallarda kibercinayətkar üçün zəruri olan informasiyanın qurbandan alınması baş verir. Bu hücumda, telefon zəngi ilə edilə bilər. (Kumar, Chaudhary, Kumar: 2015)

4. "Trojan atı" bir növ zərərli proqramdır. Kompüter troyanları dağıdıcı yükə malikdir. E-poçta gizli zərərli proqramı daxil etmək, qoşmaq Trojan formasıdır. Sosial mühəndisliyin hiyləsi ondan ibarətdir ki, zərərli faylı göndərən e-poçt etibarlı göndəricidən gəlir.

5. Qəsbçi kibercinayətkarlardan satın almaq məqsədilə faylları saxlayan (şifrələyən) zərərli proqramtəminatı növüdür. Qiymətli verilənlərini qaytarmaq (şifrəsini açmaq) istəyən insanlara cinayətkarlar onları almağı təklif edirlər (Abdelhamid, 2020).

6. Qui pro Quo (xidmətə görə xidmət). Bu hücumda kibercinayətkar texniki işçi kimi çıxış edir. Texniki dəstək işçisi kimi olan kibercinayətkar telefonla zərərçəkmişə fərdi kompüterdə proflaktik tədbirlərin görülməsinin vacibliyini bildirir və ya zərərçəkmişdən kompüterdə hər hansı problemin olub-olmadığını soruşur. Sonra cinayətkar texniki problemləri həll edir, daha sonra təcrübəsiz istifadəçiyə cinayət məqsədlərinin həyata keçirilməsi üçün bu kompüterdən məlumatları ona ötürəcək proqramı quraşdırmağı təklif edir.

7. "Yol alması" (Baiting) (ov üçün yem). Bu hücum metodunun əsasında "troya atı"nın əlamətləri dayanır. Yeganə fərq ondadır ki, bu metod hücum üçün fiziki daşıyıcını istifadə edir. Bu hücumda cinayətkarlar məqsədyönlü şəkildə fiziki daşıyıcısını maraqlı şəxslər tərəfindən tez aşkar oluna bilmələri üçün qəsdən ictimai yerlərdə tərk edirlər, qoyurlar. Bundan sonra həmin daşıyıcını aşkar edən şəxs onu kompüterə qoşan kimi informasiyanın kibercinayətkara ötürülməsi baş verir.

8. Tərs sosial mühəndislik. Bu hücumun özünəməxsus cəhəti ondan ibarətdir ki, bu hücumda kibercinayətkarlar elə vəziyyət yaradırlar ki, hər hansı bir problemi həll etmək üçün şəxs özü ona müraciət edir və ona şəxsi və ya digər məlumatlarını təqdim edir.

Yuxarıdakı siyahı hazırda kibercinayətkarlar tərəfindən istifadə edilən sosial mühəndisliyin ən populyar texnikalarını (metodlarını) ehtiva edir, lakin informasiya texnologiyalarının sürətli inkişafını nəzərə alsaq, bu, tam deyil (Salahdine, Kaabouch: 2019).

Nəticə

Bu gün əsas vəzifələrdən biri ilkin səviyyədə hücumları müəyyən etmək üçün fərdi kompüter istifadəçilərini öyrətməkdir. Mesajlarda, e-poçtlarda və telefon danışıqlarında şübhəli açar sözlərin aşkarlanması potensial hücumun vaxtında qarşısını almağa kömək edəcək. Sosial mühəndislik bizim üçün kritik bir təhlükədir, ona görədə özümüzü və cihazlarımızı ondan qorumalıyıq. Bundan əlavə, hakerlər istifadəçinin məlumatsızlığından istifadə etməyə çalışırlar. Texnologiyanın sürəti sayəsində bir çox istehlakçılar və işçilər sürücü ilə yükləmələr kimi müəyyən təhlükələrdən xəbərsizdirlər, həmçinin çox böyük risklər edirlər.

Ədəbiyyat

2. Sozaev, S., Kunaşev, D. (2020). Sosial mühəndislik, onun metodları və onun əks-təsirləri. Beynəlxalq "Vestnik Nauki" jurnalı. 2 (23). Cild 1, s.85-88.
3. Mitnik, K., Simon, V. (2004). Aldatma sənəti. IT şirkəti, 360 s.
4. Zuikov, Q. (1970). Cinayətin Metoduna dair Məhkəmə Tibbi Doktrina: Avtoreferat. dis. Hüquq Elmlər Doktoru, 31 s.
5. Hadnagy, C. (2010). Sosial Mühəndislik: insan hacking sənət. Art Hum. Hacking.
6. Kumar, A., Chaudhary, M., Kumar, N. (2015). "Sosial Mühəndislik Təhdidləri və Agahlıq: Asurvey," Avro. J. Adv. Eng. Texnologiya.
7. Abdelhamid, M. (2020). "Fişinq həssaslığında sağlamlıqla bağlı problemlərin rolu: Sorğu dizaynı araşdırması," J. Med. İnternet Res.
8. Salahdine, F., Kaabouch, N. (2019). Sosial mühəndislik hücumları. Sorğu. Cild 11, N 4.

Göndərildi: 02.02.2023 Qəbul edildi: 14.04.2023