Rəqəmsal İzlərin Aşkar Edilməsində Sosial Mühəndislik Metodlarından İstifadə İmkanları

Orxan Məmmədov
Daxili İşlər Nazirliyinin Polis Akademiyası, Bakı, Azərbaycan
infosec@pa.edu.az

***Xülasə*— Müasir dövrdə kibercinayətlərin, onlayn dələduzluq hallarının, şəxsi məlumatların qanunsuz əldə edilməsi hallarının və sosial şəbəkələr vasitəsilə törədilən hüquqazidd əməllərin sayının artması rəqəmsal izlərin vaxtında aşkarlanmasını hüquq-mühafizə fəaliyyəti üçün mühüm istiqamətə çevirmişdir.. Rəqəmsal izlər təkcə texniki sistemlərdə qalan məlumat qalıqları deyil, həm də istifadəçi davranışı, ünsiyyət forması, sosial əlaqələr və qərarvermə nümunələri ilə bağlı göstəricilərdir. Məqalədə rəqəmsal iz anlayışı təhlil olunur, onların aşkarlanmasında sosial mühəndislik texnikalarının legitim və qanuni istifadə imkanları araşdırılır, rəqəmsal kriminalistika metodları və praktik nümunələr təqdim edilir.**

Açar sözlər*— *rəqəmsal iz; sosial mühəndislik; kibercinayət; rəqəmsal kriminalistika; fişinq; metadata.

I. GİRİŞ

Rəqəmsal transformasiya cəmiyyətin bütün sahələrinə nüfuz etdikcə cinayətkarlıq da yeni formalar qazanmışdır [1]. Əvvəllər fiziki məkanda törədilən bir çox əməllər hazırda elektron poçt, mobil tətbiqlər, sosial media platformaları, bulud xidmətləri və kriptovalyuta ekosistemində baş verir [2]. Cinayətlərin aşkar olunması prosesində ənənəvi sübutlarla yanaşı, rəqəmsal izlərin rolu da son illərdə əhəmiyyətli dərəcədə artmışdır [3].

Lakin təcrübə göstərir ki, bəzi hallarda yalnız texniki ekspertiza kifayət etmir [4]. Cinayətkarlar VPN, anonim e-poçt xidmətləri, saxta hesablar və birdəfəlik nömrələrdən istifadə etməklə izlərini gizlətməyə çalışırlar [5]. Belə hallarda insan davranışı, psixoloji reaksiyalar və ünsiyyət modelləri əlavə məlumat mənbəyinə çevrilir [6]. Məhz bu nöqtədə sosial mühəndislik texnikalarının hüquqi çərçivədə tətbiqi rəqəmsal izlərin aşkarlanmasına yardım edə bilər [7].

Rəqəmsal iz - şəxsin və ya təşkilatların elektron sistemlərdə fəaliyyəti nəticəsində yaranan, saxlanılan və sonradan bərpa edilə bilən məlumatların məcmusudur [4]. Rəqəmsal izlər yaranma mexanizminə görə aktiv və passiv formada təzahür edir. Aktiv izlər istifadəçinin şüurlu fəaliyyəti nəticəsində (mesaj yazmaq, hesab açmaq, fayl göndərmək), passiv izlər isə sistemin avtomatik qeydə aldığı məlumatlar nəticəsində formalaşır [5].

Əsas rəqəmsal iz növləri aşağıdakılardır:

- IP ünvanları və qoşulma tarixçəsi;
- cihaz identifikatorları (IMEI, MAC, seriya nömrəsi);
- geolokasiya və Wi-Fi qoşulma qeydləri;
- brauzer tarixçəsi və kuki (cookie) məlumatları;
- sosial şəbəkə fəaliyyət saatları;
- e-poçt "header" məlumatları;
- silinmiş fayl qalıqları;
- bulud yaddaşının sinxronizasiya qeydləri;
- bank əməliyyatı və OTP təsdiq loqları;
- istifadəçi davranış nümunələri [4, 5].

Rəqəmsal kriminalistika (Digital Forensics) baxımından bu məlumatlar hadisənin vaxtını, istifadə olunan cihazı, şübhəli şəxsin mümkün yerləşmə yerini, əlaqə dairəsini və hərəkət istiqamətini müəyyən etməyə imkan verir [4]. Təcrübədə rəqəmsal izlərin təhlili təkcə texniki məlumatların araşdırılması ilə məhdudlaşmır. Bir çox hallarda istifadəçinin qərarvermə modeli, reaksiyası, ünsiyyət forması və davranış xüsusiyyətləri də əlavə informasiya mənbəyi kimi çıxış edir [5].

Məhz bu mərhələdə insan faktoruna əsaslanan yanaşmalar xüsusi əhəmiyyət qazanır. Çünki kibercinayətlərin mühüm hissəsi texniki zəiflikdən deyil, istifadəçinin aldanması, tələsdirilməsi və ya yanlış istiqamətləndirilməsi nəticəsində baş verir [6]. Rəqəmsal izlərin tam və düzgün qiymətləndirilməsi üçün insan davranışına təsir göstərən üsulların da öyrənilməsi zəruri hesab olunur [6].

Sosial mühəndislik insanın etibar, qorxu, maraq, tələskənlik və ya itaət meyillərindən istifadə etməklə məlumat əldə etmə üsullarının ümumi adıdır. Ən geniş yayılmış formaları fişinq (phishing), vişinq (vishing), smişinq (smishing), saxta kimlikdən istifadə (impersonation) və saxta ssenari qurma (pretexting) hesab olunur [6].

Sözügedən texnikalardan adətən cinayətkarlar istifadə etsələr də, müdafiə və araşdırma məqsədilə onların mexanizmlərinin öyrənilməsi vacibdir [6]. Çünki hücum metodunu anlamadan onun buraxdığı rəqəmsal izi düzgün təhlil etmək mümkün deyil [5].

II. RƏQƏMSAL İZLƏRİN AŞKAR EDİLMƏSİNDƏ SOSİAL MÜHƏNDİSLİK METODLARININ TƏTBİQİ

Bir çox kibercinayətlərdə texniki izlər qəsdən gizlədilsə də, davranış xarakterli izlər saxlanılır [5]. Xüsusilə saxta ssenari qurma (pretexting) hallarında cinayətkar müxtəlif hesab və vasitələrdən istifadə etsə belə, tətbiq etdiyi bəhanə, müraciət forması, təzyiq yaratma üsulu və mesaj məzmunu oxşar qalır [6].

DOI: 10.25045/forensic.gov.2026.44

Bu səbəbdən "pretexting" ssenarilərinin müqayisəli təhlili mühüm əhəmiyyət kəsb edir.

Məsələn, dələduzun müxtəlif sosial media hesablarından vətəndaşlara "kartınız bloklanıb", "hesabınız təhlükədədir", "məlumat təsdiqlənməlidir" və s. məzmunlu mesajlar göndərməsi zamanı istifadə olunan dil üslubu, eyni yazı səhvləri, transliterasiya xüsusiyyətləri, tələsdirmə elementləri və aktivlik saatlarının üst-üstə düşməsi fərqli hesabların eyni şəxs və ya qrup tərəfindən idarə olunmasını göstərən dolayı sübut kimi qiymətləndirilə bilər [6].

Beləliklə, "pretexting" ssenarilərinin müqayisəli təhlili texniki vasitələrlə gizlədilmiş kibercinayət fəaliyyətinin davranış izləri əsasında əlaqələndirilməsinə və şübhəli subyektlərin müəyyən edilməsinə imkan yaradır [5].

Sosial mühəndislik vasitəsilə açıq mənbələrdən əldə olunan məlumatların təhlili şəxsin əlaqə dairəsinin müəyyən edilməsində mühüm rol oynayır [8]. Xüsusilə "Social Network Analysis" metodlarının tətbiqi bu istiqamətdə geniş imkanlar yaradır. Sosial şəbəkə analizi şəxslər, hesablar, telefon nömrələri, elektron poçt ünvanları və digər rəqəmsal identifikatorlar arasında mövcud münasibətlərin struktur şəkildə araşdırılmasına əsaslanır [3].

Təcrübədə saxta lotereya, kredit, investisiya və ya onlayn qazanc vədləri göndərən hesabların araşdırılması zamanı ilk növbədə həmin hesabın dost siyahısı, izləyiciləri, tez-tez qarşılıqlı əlaqədə olduğu istifadəçilər, şərh yazan profillər, eyni məzmunu paylaşan səhifələr və oxşar istifadəçi adları təhlil olunur. Bu məlumatlar ayrı-ayrılıqda qiymətləndirildikdə məhdud informativliyə malik görünsə də, qarşılıqlı əlaqələr əsasında təhlil edildikdə müəyyən şəbəkə strukturu formalaşdırmağa imkan verir.. Belə strukturda hansı hesabların mərkəzi rol oynadığı, hansılarının yalnız görüntü yaratmaq məqsədilə istifadə edildiyi və hansılarının zərərçəkənlərlə birbaşa əlaqəyə girdiyi müəyyən edilə bilər [8].

Məsələn, saxta kredit təklifləri göndərən bir hesabın paylaşımına müntəzəm olaraq eyni şəxslərin "etibarlıdır", "mən istifadə etmişəm", "pulumu aldım" kimi şərhlər yazması həmin profillərin saxta etibar mühiti yaratmaq üçün istifadə olunmasını göstərə bilər. Sonradan bu hesabların başqa dələduzluq səhifələrində də eyni fəaliyyəti göstərməsi onların vahid qrup tərəfindən idarə olunması ehtimalını gücləndirir [5].

Araşdırma zamanı eyni telefon nömrəsi, eyni elektron poçt ünvanı, eyni bank kartı rekviziti və ya eyni mesajlaşma tətbiqi hesabının müxtəlif elanlarda və müxtəlif profillərdə təkrarlanması xüsusi əhəmiyyət daşıyır. Belə təkrar göstəricilər rəqəmsal mühitdə "kəsişmə nöqtələri" hesab olunur. Həmin nöqtələr üzrə qurulan analiz nəticəsində bir-birindən fərqli görünən çoxsaylı hesabların əslində eyni təşkilatlanmış sxemin hissəsi olduğu üzə çıxa bilər [3].

OSINT imkanları sosial şəbəkə analizi ilə birlikdə tətbiq edildikdə nəticə daha səmərəli olur [9]. Açıq profillərdə yerləşdirilmiş fotoşəkillər, geolokasiya nişanları, iş yeri məlumatları, istifadə olunan dil xüsusiyyətləri, paylaşım saatları və əlaqəli platformalardakı aktivlik eyni şəxsin müxtəlif platformalarda istifadə etdiyi hesabları əlaqələndirməyə imkan verir. Məsələn, bir platformada saxta lotereya keçirən profilin istifadə etdiyi şəkil digər platformada fərqli adla qeydiyyatdan keçmiş real hesabda da aşkar edilə bilər [9].

Sosial mühəndislik yanaşmaları burada yalnız aldadıcı məzmunun araşdırılması ilə məhdudlaşmır, həm də cinayətkarın etibar yaratmaq, kütlə toplamaq, psixoloji təsir göstərmək və zərərçəkənləri inandırmaq üçün qurduğu əlaqə mexanizmlərinin təhlilini əhatə edir. Bu mexanizmlərin sosial şəbəkə analizi ilə öyrənilməsi nəticəsində hansı şəxslərin yeni qurbanların cəlb olunmasında rol oynadığı, hansı hesabların saxta rəylər yazdığı, hansı subyektlərin pul vəsaitlərinin qəbulunda istifadə edildiyi müəyyən edilə bilər [8].

Bəzi hallarda şübhəli hesaba qanuni sorğu və ya rəsmi xəbərdarlıq göndərildikdən sonra istifadəçi tərəfindən ani reaksiyalar müşahidə olunur. Belə reaksiyalar çox vaxt araşdırma prosesində əlavə rəqəmsal izlərin yaranmasına səbəb olur. Məsələn, hesabın qısa müddət ərzində silinməsi və ya deaktiv edilməsi məlumatın gizlədilməsi cəhdi kimi qiymətləndirilə bilər. İstifadəçi adının dəyişdirilməsi əvvəlki identifikatorun izini itirmək məqsədi daşıya bilər. Profil şəkli, bioməlumatı və əlaqə vasitələrinin birdən-birə yenilənməsi də diqqətçəkən göstəricilərdən hesab olunur. Bəzi hallarda hesabla əlaqəli cihazların eyni vaxtda oflayn (offline) rejiminə keçməsi istifadəçinin xəbərdar olduğunu göstərə bilər [5].

Mesaj tarixçəsinin silinməsi, paylaşımların aradan qaldırılması və dost siyahısının gizlədilməsi də tipik reaksiyalar sırasındadır. Bu dəyişikliklərin vaxt ardıcıllığı araşdırma üçün xüsusi əhəmiyyət daşıyır. Çünki sorğunun göndərilmə vaxtı ilə istifadəçi reaksiyası arasında uyğunluq səbəb-nəticə əlaqəsini gücləndirə bilər. Nəticə etibarilə, bu cür reaksiyalar şübhəli şəxsin davranış modeli, məlumatlılıq səviyyəsi və sübutları gizlətmə niyyəti barədə mühüm indikator kimi qiymətləndirilir [3].

Rəqəmsal izlərin aşkarlanması zamanı şəxsi həyatın toxunulmazlığı prinsipi əsas hüquqi tələblərdən biri hesab olunur [7]. Elektron mühitdə aparılan hər bir araşdırma şəxslərin konstitusion hüquqlarına hörmət edilməklə həyata keçirilməlidir. Yazışma sirri və rabitə məlumatlarının mühafizəsi xüsusi qorunan hüquqi dəyərlər sırasına daxildir. Elektron məktublara, mesajlaşma məlumatlarına və şəxsi hesablara müdaxilə yalnız qanuni əsaslar mövcud olduqda mümkündür. Məlumatların toplanması zamanı zərurilik və proporsionallıq prinsipləri nəzərə alınmalıdır. Araşdırma məqsədilə əldə edilən məlumatlar yalnız müəyyən edilmiş məqsəd çərçivəsində istifadə olunmalıdır [7].

Sosial mühəndislik texnikalarının hüquq-mühafizə məqsədilə tətbiqi yalnız qanunla nəzərdə tutulmuş hallarda yol verilən vasitə kimi qiymətləndirilə bilər. Belə tədbirlər səlahiyyətli orqan tərəfindən və müəyyən edilmiş prosedur qaydalar çərçivəsində həyata keçirilməlidir. Prosessual nəzarətin mövcudluğu həm vətəndaş hüquqlarının qorunmasına, həm də əldə edilmiş materialların sübut qüvvəsinin təmin edilməsinə xidmət edir [10].

Hüquqi tələblərə əməl olunmaması isə əldə edilmiş məlumatların etibarlılığına və məhkəmədə istifadə imkanlarına mənfi təsir göstərə bilər. Buna görə rəqəmsal izlərin toplanması və istifadəsi zamanı bir sıra əsas tələblərə riayət olunmalıdır. İlk növbədə, tətbiq edilən müdaxilə ilə araşdırılan məqsəd arasında

proporsionallıq qorunmalıdır. Toplanmış məlumatlardan yalnız müəyyən edilmiş məqsəd çərçivəsində istifadə edilməlidir. Eyni zamanda, zəruri olmayan şəxsi məlumatların toplanmasına yol verilməməli, məlumatların minimallaşdırılması prinsipi təmin olunmalıdır. Qanunvericilikdə nəzərdə tutulan hallarda məhkəmə qərarı və ya digər qanuni icazə mexanizmləri əldə edilməlidir. Bundan əlavə, toplanmış məlumatların məxfiliyi və təhlükəsiz saxlanılması da təmin edilməlidir [7].

NƏTİCƏ

Rəqəmsal cinayətlərin araşdırılmasında yalnız texniki izlərə əsaslanmaq kifayət etmir. Cinayətkarlar texniki maskalanma vasitələrindən daha geniş istifadə etdikcə davranış və sosial əlaqə izlərinin əhəmiyyəti artır. Sosial mühəndislik metodlarının öyrənilməsi və onların qanuni çərçivədə analitik məqsədlə tətbiqi rəqəmsal izlərin aşkarlanmasına əlavə imkanlar yaradır.

Azərbaycan təcrübəsi göstərir ki, saxta domenlər, "phishing" kampaniyaları və dövlət qurumlarının adından sui-istifadə halları real təhlükə olaraq qalır. Buna görə rəqəmsal kriminalistika, OSINT, davranış analizi və hüquqi mexanizmlərin birgə tətbiqi gələcək mübarizənin əsas istiqamətlərindən biri hesab olunur.

ƏDƏBİYYAT

[1] CERT Azerbaijan – Fake myGov phishing domains warning, 14.01.2026 - https://cert.gov.az/en/news

[2] CERT.AZ kiber insident müraciəti - https://cert.az/report_cyber

[3] Digital Evidence and Computer Crime – Eoghan Casey. 3rd edition – April, 2011.

[4] https://www.elsevier.com/books/digital-evidence-and-computer-crime/casey/978-0-12-374268-1CERT.AZ – Incident reporting categories and phishing alerts.

[5] Brian Carrier - Digital Forensics methodology studies. https://digital-evidence.org/papers/

[6] ENISA / Europol annual cyber threat reports - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

[7] Social Engineering: The Science of Human Hacking, 2nd Edition - Christopher Hadnagy. July, 2018. https://www.wiley.com/en-us/Social+Engineering%3A+The+Science+of+Human+Hacking%2C+2nd+Edition-p-9781119433385

[8] Budapest Convention on Cybercrime - https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[9] First-ever cyber awareness and phishing simulation portal in Azerbaijan - https://www.smb.gov.az/en/all-news/first-ever-cyber-awareness-and-phishing-simulation-portal-in-azerbaijan

[10] Azerbaijan strengthens cybersecurity defenses amid rising threats - https://www.azernews.az/analysis/238092.html

Possibilities for the Use of Social Engineering Techniques in the Identification of Digital Traces

Orkhan Mammadov

Police Academy of the Ministry of Internal Affairs, Baku, Azerbaijan

infosec@pa.edu.az

Abstract - In the contemporary context, the increasing incidence of cybercrime, online fraud, unauthorized acquisition of personal data, and unlawful activities carried out through social networks has rendered the timely identification of digital traces a priority area of law enforcement practice. Digital traces constitute not only residual data retained within technical systems but also a set of indicators reflecting user behavior, communication patterns, social interactions, and decision-making models. This article provides an analysis of the concept of digital traces, examines the possibilities for the lawful and legitimate application of social engineering techniques in their identification, and discusses digital forensics methods alongside practical examples.

Keywords- digital trace; social engineering; cybercrime; digital forensics; phishing; metadata.