Rəqəmsal Ekspertiza və İnsidentə Cavab Əsasında İnsidentlərin Zaman Xəttinin Rekonstruksiyası Problemləri

Səbinə Tağıyeva[1], Rəvan Abdinov[2]
[1,2]Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti, Bakı, Azərbaycan
[1]*sabina.taghiyeva@cert.gov.az*, [2]*ravan.abdinov@cert.gov.az*

Xülasə **- Müasir kiberinsidentlərdə hücum vektorlarının mürəkkəbliyi səbəbindən yalnız bir mənbəyə əsaslanan təhlil kifayət etmir. Müxtəlif mənbələrdən toplanan elektron sübutların qarşılıqlı korrelyasiyası və analizi insidentin mahiyyətini daha dəqiq müəyyən etməyə imkan verir. Məqalədə zaman xəttinin qurulması, məlumatların normallaşdırılması və hadisələr arasındakı əlaqələrin müəyyən edilməsi izah olunur. Eyni zamanda zaman nişanı uyğunsuzluğu, heterogen məlumat strukturları və kontekst çatışmazlığı kimi çətinliklərə diqqət yetirilir.**

Açar sözlər - rəqəmsal kriminalistika; zaman xətti rekonstruksiyası; elektron sübut; elektron sübutların korrelyasiyası; insident təhlili.

I. GİRİŞ

Müasir kiberinsidentlərin çoxmərhələli strukturu və icra olunma mexanizmləri artıq daha mürəkkəb xarakter aldığı üçün yalnız hücumun baş verdiyi aktivin analiz edilməsi bütöv bir insidentin tam müəyyən edilməsini təmin etmir. Kiberinsidentin həyat dövrünün aydınlaşdırılması isə insidentə cavab verilməsi prosesində mühüm mərhələ olan "Lessons Learned" mərhələsi üçün böyük əhəmiyyət daşıyır. Bu mərhələdə kiberinsidentin nədən və haradan qaynaqlandığı, hansı səbəbdən uğurlu olduğu, hansı boşluqlardan sui-istifadə edildiyi - qısaca insidentin təbiəti aydınlaşdırılır və bir daha baş verməməsi və ya təkrarlandığı halda daha sürətli cavab verilə bilməsi üçün müəyyən tədbirlər görülür. Hücumların çoxmərhələli həyata keçirildiyini nəzərə alsaq, fərqli mənbələrdən rəqəmsal sübutların toplanması və onların analitik interpretasiyası xeyli çətinləşir. Bu halda yalnız müxtəlif aktivlərdən rəqəmsal sübutların toplanması deyil, həmçinin bu texniki izlərin bir-biri ilə qarşılıqlı əlaqəsi və zaman ardıcıllığı əsasında rekonstruksiya edilməsi mühüm əhəmiyyət kəsb edir. Çoxmərhələli şəkildə həyata keçirilmiş kiberinsidentin mahiyyəti yalnız ayrı-ayrı texniki izlərin təhlili ilə aydınlaşdırıla bilməz. Buna görə də toplanılan rəqəmsal sübutların bir-biri ilə məntiqi əlaqəsi aydınlaşdırılmalıdır.

Rəqəmsal ekspertiza və DFIR (Digital Forensics and Incident Response) rolları bu prosesin icrasında bir-birini tamamlayan funksiyalar icra edir. Rəqəmsal ekspertiza zamanı elektron sübutların toplanması, qorunması və təhlili həyata keçirilir. DFIR isə insidentlərin operativ aşkarlanması, araşdırılması və cavab tədbirlərinin həyata keçirilməsini təmin edir. Bu iki yanaşmanın həyata keçirilməsində insidentin zaman xəttinin rekonstruksiyası xüsusi əhəmiyyət qazanır. Məqalədə tez-tez istifadə ediləcək zaman xəttinin rekonstruksiyası dedikdə, çoxmənbəli elektron sübutlar əsasında insidentin gedişatının həm xronoloji, həm də analitik baxımdan yenidən qurulması nəzərdə tutulur.

Kiberinsidentin növündən asılı olaraq son istifadəçi sistemləri, autentifikasiya qeydiyyatları, şəbəkə trafiki, elektron poçt qeydləri və bulud mühitlərdən əldə edilən məlumatlar elektron sübut kimi çıxış edə bilər. Bu halda məlumatlar artıq heterogen xarakter daşıdığı üçün zaman nişanlarının fərqliliyi, kontekst və məlumat həcminin böyük olması kimi problemlərlə qarşılaşılır.

Təqdim olunan işdə çoxmənbəli elektron sübutların korrelyasiyası əsasında insidentlərin zaman xəttinin rekonstruksiyası və bu məlumatların analitik interpretasiyası ilə bağlı nüanslara toxunulur. Xüsusilə, müxtəlif mənbələrdən toplanan texniki izlərin vahid analitik çərçivədə birləşdirilməsi və bu prosesdə yaranan metodoloji çətinliklər tədqiqatın əsas istiqamətlərini təşkil edir.

Kiberinsidentlərin təhlili və rəqəmsal sübutların qiymətləndirilməsi ilə bağlı aparılmış tədqiqatlarda müasir rəqəmsal ekspertiza prosesində hadisələrin zaman ardıcıllığının bərpasının mühüm metodoloji istiqamətlərdən biri olduğu müşahidə olunur. Zaman xəttinin rekonstruksiyası rəqəmsal mühitdə icra edilmiş fəaliyyətlərin elektron izlərinə əsaslanaraq yenidən qurulması ilə nəticələnir və bu cür yanaşmanın tətbiqi insidentin inkişaf mərhələlərini daha yaxşı anlamağa xidmət edir. Müvafiq tədqiqatlarda zaman xəttinin rekonstruksiyası təkcə hadisələrin zaman üzrə sıralanması kimi deyil, həmçinin onların qarşılıqlı əlaqələrinin və insident kontekstində müəyyənləşdirilməsi prosesi kimi izah olunur [1, 2].

Tədqiqatlar göstərir ki, ənənəvi zaman nişanı əsaslı yanaşma bir çox hallarda böyük həcmdə aşağı səviyyəli texniki hadisələri özündə ehtiva edir. Bu kimi hadisələrə fayl sistemində baş verən dəyişikliklər, daxilolma və çıxış cəhdləri, proseslərin icrası, qeyd jurnalındakı dəyişikliklər misal göstərilə bilər. Qeyd edilən məlumatlar təhlilin ilkin prosesində mühüm əhəmiyyət daşısa da, onların çox olması və vahid struktura salınmaması insidentlə bağlı ümumi təsəvvürün yaranmasına imkan vermir [1].

Müasir tədqiqatlarda əsas istiqamətlərdən biri də çoxmənbəli elektron sübutların toplanması məsələsidir. İnsidentin gedişatının daha aydın təsvir edilməsi üçün son istifadəçi sistemlərindən, autentifikasiya jurnallarından, şəbəkə trafikindən, elektron poçt qeydlərindən və bulud mühitlərindən

DOI: 10.25045/forensic.gov.2026.35

əldə edilən müxtəlif xarakter daşıyan elektron sübutların vahid analitik çərçivədə birləşdirilməsi zərurəti yaranır. Bu səbəbdən ədəbiyyatlarda heterogen məlumat mənbələrinin əlaqələndirilməsi, zaman nişanlarının uyğunlaşdırılması və hadisələrarası əlaqələrin müəyyənləşdirilməsi rəqəmsal ekspertizanın aktual problemlərindən biri kimi qeyd edilir [2, 3].

Mövcud araşdırmaları nəzərdən keçirdikdə görə bilərik ki, kiberinsidentlərin effektiv rekonstruksiyası üçün çoxmənbəli elektron sübutların korrelyasiyası, aşağı səviyyəli texniki hadisələrin yüksək səviyyəli ssenarilərə çevrilməsi və zaman xəttinin analitik təhlili kompleks şəkildə nəzərdən keçirilməlidir. Bu problemlər üzrə müəyyən nəzəri və metodoloji əsas formalaşdırılsa da, heterogen məlumatların vahid çərçivə üzrə izahı və analitik nəticəyə transformasiyası hələ də aktual tədqiqat məsələsi olaraq qalmaqda davam edir.

II. DFIR VƏ RƏQƏMSAL EKSPERTİZANIN NƏZƏRİ ÇƏRÇİVƏSİ

DFIR termini iki bir-biri ilə sıx bağlı olan sahəni - rəqəmsal ekspertiza (Digital Forensics) və insidentə cavab (Incident Response) proseslərini özündə birləşdirir. Rəqəmsal ekspertiza elektron sübutların aşkarlanması, toplanması, qorunması, təhlili və hüquqi müstəvidə təqdim edilməsinə qədər olan bütün mərhələləri əhatə edir və bu prosesin əsas komponentlərindən biri də məhz zaman xəttinin təhlili hesab edilir. İnsidentə cavab isə təşkilatın kiberinsidenti aşkarlamaq, onun miqyasını müəyyənləşdirmək və təsirini məhdudlaşdırmaq üçün icra etdiyi tədbirlər məcmusudur. Bu iki sahənin birləşməsi ilə zaman xəttinin rekonstruksiyası insidentin ardıcıllığının aydınlaşdırılmasında və kritik təfərrüatların üzə çıxarılmasında əsas vasitəyə çevrilir [4].

Rəqəmsal ekspertiza prosesi beynəlxalq səviyyədə qəbul edilmiş standartlar vasitəsilə tənzimlənir. Bu sahədə əsas istinad sənədlərindən biri ISO/IEC 27037:2012 standartıdır. Bu standart elektron sübutların identifikasiyası, toplanması, əldə edilməsi və qorunması üzrə beynəlxalq qaydaları müəyyən edir və rəqəmsal sübutun hüquqi qəbul edilə bilməsinin təməlini təşkil edir [5].

Metodoloji baxımdan ən geniş istinad edilən digər sənəd ABŞ Milli Standartlar və Texnologiya İnstitutunun (NIST) nəşr etdiyi "Guide to Integrating Forensic Techniques into Incident Response" (NIST SP 800-86) sənədidir. Bu sənəd rəqəmsal ekspertiza prosesini dörd mərhələdən ibarət analitik çərçivədə təqdim edir: toplama (collection), araşdırma (examination), təhlil (analysis) və hesabat (reporting). NIST SP 800-86 həmçinin çoxsaylı məlumat mənbələrinin - fayl sistemləri, əməliyyat sistemləri qeydiyyatları, şəbəkə trafiki və tətbiqi proqram qeydləri - bir araya gətirilməklə hadisəyə dair daha dərin anlayışın əldə edilməsi yanaşmasını əsaslandırır [6].

Nəzəri yanaşmalar baxımından hadisə rekonstruksiyasının elmi təməllərini ilkin olaraq Eoghan Casey formalaşdırmışdır. Onun təklif etdiyi modeldə təhlilin üç əsas növü fərqləndirilir: zaman əsaslı (temporal), əlaqə əsaslı (relational) və funksional (functional) təhlil. Zaman əsaslı təhlil hadisələrin xronoloji ardıcıllığının qurulmasına, əlaqə əsaslı təhlil obyektlər, subyektlər və yerlər arasındakı əlaqələrin aydınlaşdırılmasına, funksional təhlil isə müəyyən bir hərəkətin texniki baxımdan mümkünlüyünün qiymətləndirilməsinə yönəlmişdir [4]. Bu üçölçülü yanaşma müasir DFIR praktikasında hadisənin yalnız "nə zaman" deyil, həm də "necə" və "niyə" baş verdiyinin aydınlaşdırılması üçün konseptual çərçivə rolunu oynayır.

Brian D. Carrier və Eugene H. Spafford tərəfindən irəli sürülən hadisə əsaslı rəqəmsal ekspertiza modelində hadisə "bir və ya bir neçə obyektin vəziyyətini dəyişən hal" kimi müəyyənləşdirilir. Bu tərif daha sonra Christopher Hargreaves və Jonathan Patterson kimi tədqiqatçılar tərəfindən inkişaf etdirilmiş və aşağı səviyyəli (low-level) hadisələrlə yüksək səviyyəli (high-level), yəni insan üçün başa düşülən hadisələr arasında fərq qoyulması zərurəti əsaslandırılmışdır [2, 7]. Bu konseptual ayrım məhz çoxmənbəli elektron sübutların korrelyasiyası prosesində böyük əhəmiyyət kəsb edir: fayl sistemindəki bir dəyişiklik, qeyd jurnalındakı bir giriş və ya şəbəkə paketi tək başına aşağı səviyyəli hadisədir; lakin bu izlərin birləşdirilməsi nəticəsində "istifadəçi X saat Y-də Z sistemə uzaqdan bağlanıb və A faylını çıxarıb" kimi yüksək səviyyəli ssenarinin formalaşması mümkün olur.

Əməliyyat səviyyəsində DFIR praktikası iki əlavə çərçivə ilə gücləndirilir: Lockheed Martin tərəfindən işlənib hazırlanmış Cyber Kill Chain modeli və MITRE ATT&CK biliklər bazası. Cyber Kill Chain hücumun ardıcıl yüksək səviyyəli mərhələlərini (kəşfiyyat, silahlandırma, çatdırılma, istismar, quraşdırma, idarəetmə və nəzarət, məqsədə üzrə hərəkət) təsvir edirsə, MITRE ATT&CK müşahidə edilmiş taktika, texnika və prosedurları (TTP) struktur şəklində toplayır. Zaman xəttinin rekonstruksiyası zamanı toplanmış aşağı səviyyəli izlərin ATT&CK texnikalarına xəritələnməsi aşkar edilmiş fəaliyyətin hücumçu baxımdan məna kəsb etməsinə və növbəti mərhələlərin proqnozlaşdırılmasına imkan yaradır [8].

III. ZAMAN XƏTTİNİN REKONSTRUKSİYASI VƏ ÇOXMƏNBƏLİ ELEKTRON SÜBUTLARIN KORRELYASIYASI

Hadisələrin zaman ardıcıllığı (timeline) rekonstruksiyası rəqəmsal ekspertizanın ən çətin və əsas metodoloji istiqamətlərindən biridir. Frank Breitinger və həmmüəlliflərinin bu sahədə apardığı sistematik təhlildə göstərildiyi kimi, hadisə rekonstruksiyası ilk növbədə hadisələrin dəqiq ardıcıllığının müəyyən edilməsini nəzərdə tutan zaman üzrə sıralama və korrelyasiya (temporal sequencing and correlation) prosesidir. Lakin bu proses yalnız xronoloji sıralamadan ibarət deyil - müxtəlif zaman xətləri üzrə hadisələrin qarşılıqlı əlaqələri, səbəb-nəticə bağlılıqları və paralel fəaliyyətlər də təhlil edilməlidir. Bundan sonra kontekstual təhlil mərhələsində hadisələr istifadəçi davranışı, sistem konfiqurasiyası və xarici təsirlər nəzərə alınmaqla daha geniş çərçivəyə yerləşdirilir [1].

Çoxmənbəli korrelyasiyanın nəzəri zəmini heterogenlik problemini həll etmək zərurətindən qaynaqlanır. Yoann Chabot və həmkarları bu problemi fərqli mənbələrdən əldə edilən sübutların həm format, həm də semantik baxımdan uyğunsuz olması kimi təsvir edir və bu problemin həlli üçün semantik modelləşdirmə yanaşmasını təklif edirlər. Müəlliflərin SADFC (Semantic Analysis of Digital Forensic Cases) adlandırdığı yanaşma "Ontology for the Representation of Digital Incidents and Investigations" ontologiyası üzərində qurulur və subyekt, obyekt, hadisə və iz (footprint) anlayışları arasındakı əlaqələri formal şəkildə ifadə edir. Bu model aşağı səviyyəli texniki izlərin avtomatik olaraq daha yüksək səviyyəli hadisələrə çevrilməsinə və onlar arasında korrelyasiya qaydalarının tətbiqinə imkan verir [3, 9].

Praktik səviyyədə çoxmənbəli zaman xəttinin qurulması üçün ən geniş yayılmış açıq mənbə vasitələrindən biri Plaso/log2timeline mühərrikidir. Plaso fayl sistemləri, Windows hadisə jurnalları, registr hive, brauzer tarixçəsi, prefetch qeydləri və digər artefaktlardan zaman nişanlarını çıxarıb vahid xronoloji super-zaman xəttini (super timeline) birləşdirmək üçün nəzərdə tutulmuşdur [10]. Bu vasitə və onun üzərində qurulmuş Timesketch kimi kollaborativ platformalar milyonlarla hadisəni filtr etmək, vizuallaşdırmaq və korrelyasiya etmək imkanı verir. Lakin alətlər tərəfindən generasiya edilmiş zaman xətti avtomatik olaraq analitik nəticəyə çevrilmir: analitikin vəzifəsi nüsxə, "səs-küy" (noise) və təkrarlanan qeydləri filtrlədikdən sonra insident üçün əhəmiyyətli olan izləri seçmək və onları məntiqi zəncirdə birləşdirməkdir.

Korrelyasiya prosesinin mühüm elementlərindən biri çarpaz mənbə yoxlamasıdır (cross-source verification). Məsələn, son istifadəçi sistemində hər hansı bir faylın yaradılma zaman nişanı, autentifikasiya serverindəki uğurlu giriş hadisəsi, şəbəkə trafikindəki müvafiq bağlantı və elektron poçt serverindəki mesaj qeydi eyni zaman intervalında müşahidə edildikdə, bu müstəqil mənbələrin üst-üstə düşməsi hadisənin etibarlılığını əhəmiyyətli dərəcədə artırır. Əksinə, bir mənbədə mövcud, digərində isə olmayan iz ya anti-forensik müdaxilənin, ya ölçmə xətasının, ya da mənbənin konfiqurasiya problemlərinin göstəricisi kimi qəbul edilməlidir. Casey bu cür yoxlama prosesini "sübutun gücünün miqyası" (C-Scale) anlayışı ilə əlaqələndirir və hər bir nəticənin arxasında duran sübutun etibarlılıq dərəcəsinin açıq şəkildə qeyd olunmasının vacibliyini vurğulayır [4].

Çoxmənbəli korrelyasiya prosesində istifadə olunan elektron sübut mənbələri əsasən aşağıdakı kateqoriyalara bölünür: (a) son istifadəçi sistemlərindən əldə edilən artefaktlar - MFT qeydləri, registr, prefetch, LNK faylları, Windows hadisə jurnalları; (b) şəbəkə səviyyəli mənbələr - firewall və proksi qeydləri, NetFlow/IPFIX məlumatları, IDS/IPS siqnalları, DNS sorğuları; (c) kimlik və autentifikasiya sistemləri - Active Directory, LDAP, SSO qeydləri; (d) bulud və SaaS platformaları - audit jurnalları, API çağırışları, obyekt saxlama qeydləri; (e) elektron poçt və əməkdaşlıq platformaları. Bu mənbələrin hər biri fərqli zaman dəqiqliyi, fərqli loq formatı və fərqli saxlanma müddətinə malikdir. Buna görə də onların vahid çərçivədə birləşdirilməsi sübut normallaşdırması (evidence normalization) və ontoloji xəritələmə mərhələlərini tələb edir [1, 3, 6].

IV. Analitik İnterpretasiya və Metodoloji Çətinliklər

Analitik interpretasiya çoxmənbəli zaman xəttinin qurulmasından sonra gələn ən həssas mərhələdir. Bu mərhələdə mütəxəssisin əsas vəzifəsi hadisələri təkcə sıralamaq deyil, onların arasındakı səbəb-nəticə əlaqələrini müəyyənləşdirməkdir. Christopher Hargreaves və Jonathan Pattersonun qeyd etdiyi kimi, eyni rəqəmsal vəziyyəti yarada biləcək bir neçə alternativ hadisə ssenarisi mövcud ola bilər və tədqiqatçının vəzifəsi mövcud sübutlarla ən uyğun ssenarini identifikasiya etmək, qalanlarını isə istisna etməkdir [7]. Bu proses hipotezlərin formalaşdırılması və onların sınaqdan keçirilməsi prinsipinə əsaslanır və elmi metodun rəqəmsal araşdırmalara tətbiqinin birbaşa nümunəsidir.

Zaman xəttinin təhlili zamanı rast gəlinən ən ciddi metodoloji problemlərdən biri zaman nişanlarının uyğunsuzluğudur. Bu uyğunsuzluq bir neçə səbəbdən yarana bilər: sistem saatlarının dəqiq sinxronizasiya olunmaması (NTP kənaraçıxmaları), UTC və yerli zaman bölgələri arasındakı fərqlər, yay-qış saat dəyişiklikləri və virtual mühitlərin xüsusi xətaları. Bu problemlərin həlli üçün bütün zaman nişanlarının vahid bir zaman zonasına (bir qayda olaraq UTC-yə) normallaşdırılması və sistem saatı kənaraçıxmalarının ayrıca qeyd olunaraq kompensasiya edilməsi tövsiyə olunur [1].

Daha ciddi problem olan anti-kriminalistik müdaxilələr, xüsusilə zaman nişanlarının saxtalaşdırılması (timestomping) - yəni hücumçular tərəfindən faylların zaman nişanlarının qəsdən dəyişdirilməsi - təhlükəsi müasir kiberinsidentlərdə getdikcə daha çox müşahidə edilir. NTFS fayl sistemində hər fayla məxsus metaverilənlər MFT (Master File Table) daxilində $STANDARD_INFORMATION (SIA) və $FILE_NAME (FNA) atributlarında qeyd edilir. Hər iki atributda əsasən yaradılma zamanı (Creation Time), modifikasiya zamanı (File Content Modified), metadatanın dəyişdirilmə zamanı (Metadata Change), son müraciət zamanı (Last Access Time) öz əksini tapır. Zaman nişanlarının saxtalaşdırılması alətləri adətən SIA dəyərlərini dəyişdirir, lakin FNA dəyərləri sistem tərəfindən yenilənir və müdaxilənin izini özündə saxlayır. Timo Palmbach və Frank Breitingerin araşdırmasına görə, SIA və FNA zaman nişanları arasındakı uyğunsuzluq, həmçinin saniyə altı dəqiqliyin tam sıfır olması zaman nişanlarının saxtalaşdırılması hadisəsinin mühüm göstəriciləri sayılır [11, 12]. Bu kimi halların aşkarlanması üçün mütəxəssis təkcə fayl zaman nişanlarına deyil, eyni zamanda $UsnJrnl və $LogFile jurnallarına, prefetch qeydlərinə və Windows hadisə jurnallarına müraciət etməlidir.

İkinci əsas çətinlik heterogen məlumat strukturları və məlumat həcmidir. Şəbəkə paketləri, tətbiqi proqram qeydləri, registr açarları və bulud audit jurnalları tam fərqli sxemalara və zaman dəqiqliyinə malikdir. Tipik orta ölçülü korporativ sistem günə milyonlarla hadisə qeydi generasiya edir və bütün bu qeydlərin manual təhlili qeyri-mümkündür. Bu problemin həlli üçün iki əsas yanaşma mövcuddur: hədəfli zaman xətti (targeted timeline) - insidentə aid konkret artefaktları seçici şəkildə təhlil etmək, və super-zaman xətti (super timeline) - bütün mövcud izləri bir arada toplayıb filtrasiya və qruplaşdırma vasitəsilə təhlil etmək [10]. Lakin nəzərə alınmalıdır ki heterogen və böyük həcmli məlumatların təhlilində tək yanaşma kifayət etmir. Misal üçün hədəfli zaman xətti yanaşmasının tətbiqi kontekts çatışmazlığına, super-zaman xətti yanaşmasının tətbiqi isə məlumatların birləşdirilməsi nəticəsində "səs-küy" (noisy) qeydləri yaranmasına səbəb ola bilər. İki yanaşmanın kombinasiyası həm operativlik, həm də analitik dərinlik baxımından daha effektiv nəticə verir.

Üçüncü əhəmiyyətli çətinlik kontekst çatışmazlığıdır. Fərdi qeydlər çox vaxt özü-özlüyündə mənasız və ya yanıldıcı görünə bilər. Məsələn, saat 03:00-da baş verən uğurlu SSH girişi təkcə götürüldükdə normal kimi görünə bilər, lakin eyni zamanda xarici ölkə IP ünvanından gəlmişsə, yeni istifadəçi yaratma hadisəsi ilə müşayiət olunursa və sonra yüksək həcmli xarici şəbəkə bağlantısı başlayırsa, artıq bu qeyd "data exfiltration" hücumunun başlanğıc nöqtəsi kimi qiymətləndirilə bilər. Kontekstin bərpası məhz çoxmənbəli korrelyasiyanın ən böyük üstünlüyüdür: fərdi şəkildə aşağı informativ dəyərə malik olub,

"səs-küy" (noise) kimi qiymətləndirilən qeydlər çoxmənbəli elektron sübutlarla birləşdirildikdə mənalı ssenariyə çevrilir.

Nəhayət, tədqiqatçı qərəzi (investigator bias) və hipotez əsaslı təhlilin düzgün tətbiq olunmaması da zaman xəttinin interpretasiyasında ciddi risk mənbəyidir. Mütəxəssis əvvəlcədən formalaşdırdığı bir fərziyyəni təsdiq edən izlərə diqqət verib, onunla ziddiyyət təşkil edən sübutları görməzlikdən gələ bilər. Bu cür qərəzin qarşısını almaq üçün alternativ ssenarilərin sistematik şəkildə formalaşdırılması və hər birinin mövcud sübutlarla müqayisəsi tövsiyə olunur [1, 4].

V. PRAKTİKİ HİSSƏ

Praktiki hissədə heterogen məlumat strukturları, zaman nişanı uyğunsuzluğu kimi problemlərin təsirini qiymətləndirmək məqsədilə nümunə insident ssenarisi əsasında çoxmənbəli analiz həyata keçirilmişdir. Ssenari çərçivəsində sistemə daxil edilmiş icraedilə bilən faylın zaman nişanlarının saxtalaşdırılması simulyasiya edilmiş və müxtəlif artefakt mənbələrindən əldə olunan məlumatlar müqayisəli şəkildə təhlil edilmişdir.

CƏDVƏL I. ZAMAN NIŞANLARININ MANIPULYASIYASI

Mənbə	Artefakt	Hadisə	Zaman nişanı	Qeyd
\	test.exe	Fayl yaradılıb	2022-03-01 09:12:00	Şübhəli
FNA ($FILE_NAME)	test.exe	Fayl yaradılıb	2023-06-15 14:22:10	Uyğunsuz
$UsnJrnl	test.exe	Fayl yaradılıb	2025-01-10 10:15:23	Real
Event Log (4688)	test.exe	Proses başladılıb	2025-01-10 10:16:02	Execution
Prefetch	TEST.EXE	Proqram icra edilib	2025-01-10 10:16:03	Təsdiq

Cədvəl 1-də təqdim olunan məlumatlardan göründüyü kimi, fayl sisteminə aid zaman nişanları ilə digər artefakt mənbələrindən əldə olunan məlumatlar arasında uyğunsuzluq mövcuddur. Xüsusilə, $STANDARD_INFORMATION və $FILE_NAME atributlarında qeydə alınmış tarixlərin daha köhnə olması, $UsnJrnl, prefetch və hadisə jurnallarında qeydə alınmış daha yeni zaman göstəriciləri ilə ziddiyyət təşkil edir. Bu isə zaman nişanlarının manipulyasiyası ehtimalını göstərir və hadisələrin real zaman ardıcıllığının yalnız çoxmənbəli korrelyasiya vasitəsilə müəyyən edilə biləcəyini təsdiq edir.

İlkin mərhələdə yalnız fayl sisteminə aid metaverilənlər (xüsusilə $STANDARD_INFORMATION və $FILE_NAME atributları) əsasında aparılan analiz nəticəsində faylın yaradılma vaxtının köhnə tarixlə uyğunlaşdığı müşahidə olunmuş və bu, ilkin olaraq faylın legitim olması kimi qiymətləndirilmişdir. Lakin sonrakı mərhələdə prefetch qeydləri, Windows hadisə jurnalları və $UsnJrnl məlumatları daxil olmaqla çoxmənbəli korrelyasiya aparıldıqda faylın real yaradılma və icra vaxtlarının daha yeni tarixlərə uyğun gəldiyi müəyyən edilmişdir. Aparılmış təhlil göstərmişdir ki, tək mənbəyə əsaslanan yanaşma yanlış interpretasiyaya səbəb ola bilər. Əksinə, müxtəlif artefakt mənbələrinin inteqrasiyası və vahid zaman xətti üzrə təhlili hadisələrin daha dəqiq rekonstruksiyasına və səbəb-nəticə əlaqələrinin müəyyən edilməsinə imkan verir. Eyni zamanda, praktiki analiz zamanı hədəfli zaman xətti yanaşmasının ilkin mərhələdə əsas hadisələrin operativ identifikasiyası üçün effektiv olduğu, lakin tam kontekstin əldə edilməsi üçün super-zaman xətti yanaşmasının tətbiqinin zəruri olduğu müəyyən edilmişdir.

Bununla belə, super-zaman xətti çərçivəsində yüksək həcmli "səs-küy" qeydlərinin mövcudluğu filtrasiya və prioritetləşdirmə mexanizmlərinin tətbiqini tələb edir. Hədəfli və super-zaman xətti yanaşmalarının praktiki tətbiqi və nəticələrinin müqayisəsi Cədvəl II-də təqdim olunmuşdur.

CƏDVƏL II. ZAMAN XƏTTİ YANAŞMALARININ MÜQAYİSƏSİ

Yanaşma	İstifadə olunan mənbələr	Aşkarlanan hadisələr	Nəticə
Targeted Timeline	Event Log, Prefetch	Proses icrası	Faylın mənşəyi qeyri-müəyyən
Super Timeline	SIA, FNA, USN, Event Log, Prefetch	Tam hadisə zənciri	Timestomping aşkarlanır

Nəticə etibarilə, aparılmış praktiki analiz göstərir ki, heterogen və böyük həcmli məlumatların effektiv təhlili üçün çoxmənbəli korrelyasiya, zaman xəttinin rekonstruksiyası və hipotez əsaslı analitik yanaşmanın kombinasiyası daha etibarlı və əsaslandırılmış nəticələrin əldə olunmasına imkan yaradır.

NƏTİCƏ

Təqdim edilən məqalədə göstərildiyi kimi, müasir kiberinsidentlərin təbiətinin düzgün aydınlaşdırılması yalnız bir mənbədən əldə edilən sübutların təhlili ilə mümkün deyil. Hücumların çoxmərhələli və paylanmış xarakter daşıması son istifadəçi sistemləri, şəbəkə trafiki, autentifikasiya servisləri, bulud mühitləri və elektron poçt sistemlərindən toplanmış heterogen elektron sübutların vahid analitik çərçivədə birləşdirilməsini və korrelyasiyasını tələb edir.

Zaman xəttinin rekonstruksiyası bu prosesin mərkəzində dayanır və təkcə hadisələrin xronoloji ardıcıllığının bərpası kimi deyil, səbəb-nəticə əlaqələrinin, kontekstual şərhin və yüksək səviyyəli ssenarinin formalaşdırılması prosesi kimi qəbul edilməlidir. ISO/IEC 27037, NIST SP 800-86 kimi beynəlxalq standartlar, həmçinin Casey, Chabot, Carrier və digər tədqiqatçıların konseptual işləri bu yanaşmanın metodoloji təməlini təşkil edir.

Eyni zamanda, zaman niçanlarının uyğunsuzluğu, anti-kriminalistik müdaxilələr (xüsusilə timestomping), heterogen məlumat strukturları, məlumat həcminin böyüklüyü və kontekst çatışmazlığı kimi çətinliklər çoxmənbəli korrelyasiya prosesində ciddi problemlər yaradır. Bu çətinliklərin aradan qaldırılması üçün zaman nişanlarının UTC-yə normallaşdırılması, çarpaz mənbə yoxlaması, semantik modelləşdirmə və MITRE ATT&CK kimi strukturlaşdırılmış biliklər bazasının tətbiqi əhəmiyyətli rol oynayır.

Nəticə etibarilə, rəqəmsal insidentlərin effektiv araşdırılması yalnız xronoloji ardıcıllığın qurulması deyil, çoxmənbəli sübutlar əsasında səbəb-nəticə əlaqələrinin aşkar edilməsi, alternativ ssenarilərin sistematik qiymətləndirilməsi və nəticələrin reproduksiya edilə bilən şəkildə sənədləşdirilməsi ilə mümkündür. Bu yanaşma həm insidentin təkrarlanmasının qarşısının alınmasına, həm də gələcək hücumlara daha sürətli və dəqiq cavab verilməsinə xidmət edir.

ƏDƏBİYYAT

[1] F. Breitinger et al., "SoK: Timeline based event reconstruction for digital forensics: Terminology, methodology, and current challenges," Forensic Science International: Digital Investigation, vol. 53, 301932, 2025.

[2] B. D. Carrier and E. H. Spafford, "An event-based digital forensic investigation framework," in Proc. Digital Forensic Research Workshop (DFRWS), 2004.

[3] Y. Chabot, A. Bertaux, C. Nicolle, and T. Kechadi, "An ontology-based approach for the reconstruction and analysis of digital incidents timelines," Digital Investigation, vol. 15, pp. 83–100, 2015.

[4] E. Casey, Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. Amsterdam: Academic Press, 2011.

[5] ISO/IEC 27037:2012, Information technology - Security techniques - Guidelines for identification, collection, acquisition and preservation of digital evidence, International Organization for Standardization, Geneva, 2012.

[6] K. Kent, S. Chevalier, T. Grance, and H. Dang, Guide to Integrating Forensic Techniques into Incident Response, NIST Special Publication 800-86. Gaithersburg, MD: National Institute of Standards and Technology, 2006.

[7] C. Hargreaves and J. Patterson, "An automated timeline reconstruction approach for digital forensic investigations," Digital Investigation, vol. 9, pp. S69–S79, 2012.

[8] The MITRE Corporation, MITRE ATT&CK: Adversary Tactics, Techniques, and Common Knowledge, 2015-2025. https://attack.mitre.org

[9] Y. Chabot, A. Bertaux, C. Nicolle, and T. Kechadi, "A complete formalized knowledge representation model for advanced digital forensics timeline analysis," Digital Investigation, vol. 11, pp. S95-S105, 2014.

[10] K. Guðjónsson, Mastering the Super Timeline With log2timeline, SANS Institute Reading Room, 2010.

[11] D. Palmbach and F. Breitinger, "Artifacts for detecting timestamp manipulation in NTFS on Windows and their reliability," Forensic Science International: Digital Investigation, vol. 32, 300920, 2020.

[12] C. Vanini, R. F. Ramos, and F. Breitinger, "Strategies and challenges of timestamp tampering for improved digital forensic event reconstruction," Forensic Science International: Digital Investigation, 2024.

Challenges in Incident Timeline Reconstruction Based on Digital Forensics and Incident Response.

Sabina Taghiyeva[1], Ravan Abdinov[2]
State Service for Special Communications and Information Security, Baku, Azerbaijan
[1]sabina.taghiyeva@cert.gov.az,[2]ravan.abdinov@cert.gov.az

Abstract - Due to the complexity of attack vectors in modern cyber incidents, analysis based on a single source is no longer sufficient. The correlation and analysis of electronic evidence collected from multiple sources enable a more accurate determination of the nature of an incident. This paper explains the construction of timelines, data normalization, and the identification of relationships between events. It also highlights challenges such as timestamp inconsistencies, heterogeneous data structures, and lack of context.

Keywords - digital forensics; timeline reconstruction; electronic evidence; correlation of electronic evidence; incident analysis.