Müasir Kibertəhdidlərin Analizi və İntellektual Aşkarlaması Metodlarının Analizi

Fərid Hüseynov
Dövlət Təhlükəsizliyi Xidməti, Bakı, Azərbaycan
faridhuseyn14@email.az

***Xülasə*— Məqalədə müasir kiberhücumların aşkarlanması metodları və kibertəhdidlərin analizi yanaşmaları araşdırılmışdır. Tədqiqat müdaxilənin aşkarlanması sistemlərini, anomaliya aşkarlama alqoritmlərini, maşın təliminə əsaslanan aşkarlama modellərini, APT hücumlarının analizini, botnet infrastrukturlarının təhlili və zərərli proqramların davranış analizini əhatə edir. Süni immun sistemlərə əsaslanan metodlar nəzərdən keçirilmiş və müasir şəbəkə mühitlərinə uyğun hibrid aşkarlama yanaşması təklif edilmişdir.**

Açar sözlər*— *kiberhücumların aşkarlanması; anomaliya aşkarlama; maşın təlimi; zərərli proqramların analizi; botnet.

I. GİRİŞ

Rəqəmsal dünyanın sürətlə inkişaf etdiyi bu dövrdə kibertəhdidlər getdikcə mürəkkəbləşir və çoxşaxəli xarakter alır. Şəbəkə infrastrukturlarına yönəlmiş hücumların miqyası və intensivliyi artdıqca, onların vaxtında aşkarlanması və effektiv analizi kritik əhəmiyyət kəsb edir.

Müasir kiberhücumlar sadə port skanından başlayaraq, uzun müddətli əməliyyatları əhatə edən mürəkkəb APT (Advanced Persistent Threat) kampaniyalarına qədər geniş spektr üzrə yerləşir. Bu cür hücumlar yalnız texniki infrastrukturu deyil, həm də insan faktoru, sosial mühəndislik üsulları və zəncirvarı ardıcıl hücum taktikalarından istifadə edir [1].

Bu tədqiqatın əsas məqsədi müasir kiberhücumların aşkarlanması üçün istifadə edilən texnikləri, metodologiyaları və alətləri sistemli şəkildə təhlil etmək, onların üstünlük və məhdudiyyətlərini müəyyən etmək, həmçinin süni intellekt texnologiyalarının bu sahəyə inteqrasiyasının perspektivlərini araşdırmaqdır.

II. ƏDƏBİYYAT İCMALI

Kiberhücumların aşkarlanması sahəsindəki tədqiqatlar bir neçə əsas istiqamətdə inkişaf etmişdir. İmza əsaslı aşkarlama metodları ən qədim yanaşmalardan biridir: bu üsulda məlum hücum nümunələri verilənlər bazasında saxlanılır və şəbəkə trafikinin həmin nümunələrlə müqayisəsi aparılır [2].

Snort və Suricata kimi açıq mənbəli IDS sistemləri bu yanaşmanın ən məşhur nümayəndələridir. Lakin sıfır-gün (zero-day) hücumları qarşısında bu üsulun effektivliyi məhduddur. Anomaliyaya əsaslanan aşkarlama bu çatışmazlığı aradan qaldırmaq üçün inkişaf etdirilmişdir [3].

Son illərdə dərin öyrənmə (deep learning) metodlarının kibertəhlükəsizliyə tətbiqi intensivləşmişdir. LSTM, CNN və Transformer arxitekturalarına əsaslanan modellər şəbəkə trafikinin real-vaxt rejimində analizini mümkün etmişdir [4]. Bununla yanaşı, federated learning texnologiyası məxfilik qorunmasını təmin edərək paylanmış mühitlərdə birgə model öyrənməsinə imkan yaratmışdır.

APT hücumlarının analizi kontekstində MITRE ATT&CK çərçivəsi geniş tətbiq tapmışdır. Bu çərçivə hücum taktika, texnika və prosedurlarını (TTP) sistemləşdirir, müdafiə tədbirlərinin planlaşdırılmasını asanlaşdırır [5].

Botnet infrastrukturlarının kriminalistik tədqiqi sahəsindəki işlər əsasən DNS sinkhole texnologiyası, honeypot sistemləri və şəbəkə qraf analizinə söykənir. Zərərli proqramların statik və dinamik analizi üçün sandbox mühitlərinin istifadəsi standart praktikaya çevrilmişdir [6].

Süni immun sistemlərə əsaslanan yanaşmalar bioloji immunitet prinsiplərini rəqəmsal mühitə adaptasiya edir: özünü tanıma (self-recognition), özünə aid olmayanı aşkarlama (non-self detection) və klonal seçim (clonal selection) alqoritmləri bu sahədə aktiv tədqiq olunur [7].

III. METODOLOGİYA

Bu tədqiqatda kiberhücumların aşkarlanması üçün çoxqatlı hibrid metodologiya təklif edilmişdir. Metodologiya dörd əsas komponentdən ibarətdir (Cədvəl 1):

Anomaliya aşkarlama mərhələsində LSTM (Long Short-Term Memory) şəbəkəsindən istifadə edilmişdir. Model aşağıdakı düsturla ifadə olunan xüsusiyyət vektorunu emal edir:

$$f(t) = \sigma(W\_f \cdot [h\_\{t-1\}, x\_t] + b\_f) \qquad (1)$$

burada W_f çəki matrisi, h_{t-1} əvvəlki gizli vəziyyət, x_t cari giriş vektoru, b_f isə köçürmə (bias) vektorudur. Bu düstur unudulma qapısının (forget gate) hesablanmasını göstərir [8].

CƏDVƏL I. HİBRİD AŞKARLAMA METODOLOGİYASININ KOMPONENTLƏRİ

Komponent	Metod / Texnologiya	Məqsəd
Trafik analizi	Dərin paket inspeksiyası (DPI), NetFlow analizi	Şəbəkə anomaliyalarının aşkarlanması
Anomaliya aşkarlama	LSTM, Isolation Forest, Autoencoder	Qeyri-normal davranış profilləşdirilməsi
İmza əsaslı	Snort qaydaları, YARA imzaları	Məlum hücum nümunələrinin bloklanması
Korrelyasiya mühərriki	SIEM, qraf analizi, TTP xəritəsi	APT kampaniyalarının kəşfi

DOI: 10.25045/forensic.gov.2026.08

IV. EKSPERİMENTAL NƏTİCƏLƏR

Təklif edilən metodologiya NSL-KDD və CICIDS-2018 verilənlər dəstləri üzərində qiymətləndirilmişdir. Hər iki verilənlər toplusunəzarətli (supervised) şəraitdə test edilmiş, nəticələr mövcud metodlarla müqayisə aparılmışdır.

Alınmış nəticələr göstərir ki, hibrid yanaşma 97.3% dəqiqlik göstəricisi ilə digər metodları üstələyir. Yanlış pozitiv nisbəti (FPR) 2.2%-ə endirilib ki, bu da real mühitdə əməliyyat yükünü əhəmiyyətli dərəcədə azaldır. APT hücum simulyasiyasında (CICIDS-2018) isə hibrid model 14 hücum kateqoriyasından 13-nü uğurla aşkarlaya bilmişdir.

CƏDVƏL II. METODLARIN MÜQAYİSƏLİ PERFORMANS GÖSTƏRİCİLƏRİ (NSL-KDD VERİLƏNLƏR TOPLUSU)

Metod	Dəqiqlik (%)	Yanlış Pozitiv (%)	Aşkarlama Dərəcəsi (%)	F1-Xal
İmza əsaslı (Snort)	91.2	8.4	89.7	0.903
Anomaliya (LSTM)	94.6	4.1	95.2	0.948
Hibrid (təklif edilən)	97.3	2.2	97.8	0.975
Müqayisə (Random Forest)	93.1	5.6	92.8	0.929

V. MÜZAKİRƏ

Əldə edilmiş eksperimental nəticələr aşkar şəkildə göstərir ki, ənənəvi imza əsaslı (signature-based) metodlar ilə müasir anomaliya aşkarlama (anomaly detection) üsullarının hibrid modeldə birləşdirilməsi sistemin ümumi effektivliyini və kibertəhdidlərə qarşı dayanıqlılığını əhəmiyyətli dərəcədə artırır. İmza əsaslı yanaşma məlum hücumları sıfır yanlış pozitiv (false positive) riski ilə sürətli şəkildə bloklamağa imkan verdiyi halda, anomaliya aşkarlama modulu sistemin daha əvvəl qarşılaşmadığı "sıfırıncı gün" (Zero-day) hücumlarını identifikasiya etmək boşluğunu doldurur.

Bununla belə, tədqiqat çərçivəsində tətbiq olunan modelin real dünya ssenarilərində tam funksional olması üçün bir sıra kritik problemlər və çağırışlar hələ də həllini gözləyir

Şifrəli Trafik (HTTPS/TLS) Kontekstində Aşkarlama Çətinlikləri: Müasir şəbəkə trafikinin böyük hissəsinin şifrələnməsi zərərli proqramların öz fəaliyyətlərini (məsələn, C2 kommunikasiyasını) gizlətməsinə şərait yaradır. Şəbəkə paketlərin dərin təhlili (Deep Packet Inspection - DPI) həm ciddi resurs tələb edir, həm də məxfilik hüquqlarını pozur. Bu səbəbdən, deşifrə etmədən, yalnız paketin metadata parametrləri (paketlərin gəliş intervalı, ölçü paylanması, TLS konfiqurasiyası) üzərindən maşın təlimi modellərinin təlimi zərurətə çevrilir.

Adversarial ML (Rəqib Maşın Təlimi) Hücumlarına Qarşı Dayanıqlılıq: Təcavüzkarlar aşkarlama modellərini yanıltmaq üçün giriş məlumatına xırda, lakin hədəflənmiş perturbasiyalar (dəyişikliklər) daxil edirlər. Modelin zərərli şəbəkə trafikini zərərsiz" kimi qəbul etməsini təmin edən bu hücumlar (məsələn, evasion attacks) modelin dayanıqlılığını sual altında qoyur və adversarial təlim metodlarının tətbiqini tələb edir.

Real-vaxt rejimində geniş ötürmə zolağının (Bandwidth) idarə edilməsi: əbps və tbps səviyyəsində olan müasir magistral şəbəkələrdə daxil olan hər bir paketin dərin analizi böyük hesablama gecikmələrinə (latency) səbəb olur. Modellərin real-vaxt rejimində işləməsi üçün aparat səviyyəli sürətləndiricilərdən (FPGA/GPU) və ya xüsusi axın verilənləri (stream processing) arxitekturalarından istifadə edilməlidir.

Az Nişanlı (Few-shot/Zero-shot) Hücum Kateqoriya-larında Aşkarlama Dəqiqliyi: Nadir rast gəlinən və ya tamamilə yeni xarakterli hücum növlərinə aid məlumatların (etiketlənmiş nümunələrin) azlığı modelin həmin sinifləri öyrənməsini çətinləşdirir. Bu, balanslaşdırılmamış verilənlər toplusu (imbalanced dataset) problemini yaradır və modelin spesifik hücum sinifləri üzrə dəqiqliyini azaldır.

Gelişmiş Davamlı Təhdidlərin (APT - Advanced Persistent Threats) aşkarlanmasında ən böyük çətinlik onların uzunmüddətli, gizli və mərhələli xarakterindədir. Belə ki, bəzi APT kampaniyaları hədəf şəbəkədə aylarla, hətta illərlə aktiv qala bilir və sistem daxilində normal istifadəçi davranışı nümayiş etdirməyə çalışır. MITRE ATT&CK çərçivəsinə əsaslanan TTP (Tactics, Techniques, and Procedures - Taktika, Texnika və Prosedurlar) xəritəşdirməsi bu problemi qismən həll edərək, fərqli zaman kəsiklərində baş verən xırda anomaliyalar arasında məntiqi əlaqə qurmağa (korrelyasiya) imkan verir. Lakin tam funksional müdafiə üçün yalnız reaktiv deyil, həm də proaktiv kiber kəşfiyyat (threat hunting) proseslərinin avtomatlaşdırılması və insidentlərə avtomatik reaksiya verən SOAR (Security Orchestration, Automation, and Response) sistemlərinin inteqrasiyası tələb olunur.

Botnet şəbəkələrinin və onların idarəetmə mərkəzlərinin (C2) aşkarlanması kontekstində DNS davranışı analizi müstəsna effektivlik nümayiş etdirir. Müdafiə sistemlərindən yayınmaq üçün təcavüzkarlar tərəfindən tez-tez dəyişdirilən IP ünvanları (fast-flux) və ya xüsusi alqoritmlərlə generasiya edilən dinamik domen adları (DGA - Domain Generation Algorithm) statistik metodlar, entropiya analizi və n-gram modelləri vasitəsilə yüksək dəqiqliklə identifikasiya edilə bilir. Bu da botnet yoluxmalarını hələ ilkin mərhələdə – şəbəkə daxili yayılma baş vermədən lokallaşdırmağa şərait yaradır.

Süni İmmun Sistemlərinə (AIS - Artificial Immune Systems) əsaslanan yanaşmaların kibertəhlükəsizlikdəki əsas üstünlüyü onların bioloji immun sistemi kimi yüksək adaptiv və paylanmış xarakter daşımasıdır. Ənənəvi maşın təlimi modelləri yeni verilənləri öyrənərkən köhnə biliklərini itirmək (fəlakətli unutma - catastrophic forgetting) riski ilə üzləşirlər. AIS isə əksinə, yeni hücum nümunələrinə əvvəlki təcrübəsini unudaraq deyil, klonal seçim (clonal selection) və neqativ seçim (negative selection) alqoritmləri vasitəsilə mövcud immun yaddaşına inteqrasiya edərək uyğunlaşır. Bu unikal xüsusiyyət öz kod

strukturunu davamlı olaraq dəyişən polimorf və metamorf zərərli proqramların (malware) aşkarlanmasında xüsusi əhəmiyyət kəsb edir.

Gələcək tədqiqat istiqamətlərinin ən perspektivlilərindən biri sürü kəşfiyyatı (swarm intelligence – məsələn, qarışqa koloniyası və ya zərrəciklər sürüsü alqoritmləri) ilə dərin öyrənmə (deep learning) modellərinin sinerjisinin yaradılmasıdır. Bu yanaşma, paylanmış şəbəkə mühitlərində agentlərin kollektiv zəkası vasitəsilə təhdidlərin daha sürətli lokallaşdırılmasına imkan verəcəkdir. Digər bir inqilabi istiqamət isə kvant hesablama (quantum computing) imkanlarının kibertəhlükəsizliyə inteqrasiyasıdır. Kvant maşın təlimi (QML) alqoritmləri gələcəkdə böyük həcmli şəbəkə məlumatlarını saniyələr ərzində emal edərək aşkarlama sürətini eksponensial olaraq artıra bilər.

NƏTICƏ

Bu tədqiqat işində müasir və mürəkkəb kiberhücumların vaxtında aşkarlanması, habelə dinamik kibertəhdidlərin dərin analizi üçün çoxqatlı, hibrid bir metodologiya təklif edilmiş, arxitekturası qurulmuş və real şəbəkə simulyasiyaları üzərində eksperimental olaraq qiymətləndirilmişdir. Tədqiqatın gedişində əldə edilmiş fundamental elmi və praktiki nəticələr aşağıdakı kəndirlərlə xarakterizə olunur:

Yüksək aşkarlama dəqiqliyi: İmza əsaslı filtrasiya mexanizmləri ilə statistik və maşın təlimi əsaslı anomaliya aşkarlama metodlarının sinergetik inteqrasiyası sayəsində sistem 97.3% ümumi dəqiqlik (accuracy) göstəricisinə nail olmuşdur. Bu nəticə hibrid yanaşmanın tək tətbiq edilən metodlardan daha effektiv olduğunu sübut edir.

Yanlış pozitivlərin radikal azaldılması: Zaman ardıcıllıqlarını və paketlərin kontekstual asılılıqlarını analiz edən uzun-qısamüddətli yaddaş (LSTM - Long Short-Term Memory) əsaslı rekurent neyron şəbəkəsi modeli, şəbəkədəki normal dalğalanmaları hücum kimi qiymətləndirməyən dayanıqlı bir struktur nümayiş etdirmişdir. Nəticədə, yanlış pozitiv nisbəti (False Positive Rate) ənənəvi maşın təlimi metodları ilə müqayisədə 50% azaldılmışdır.

APT-lərin ilkin mərhələdə bloklanması: MITRE ATT&CK beynəlxalq matrisinə əsaslanan TTP (Taktika, Texnika və Prosedur) korrelyasiya mühərriki, bir-biri ilə əlaqəsiz görünən şübhəli fəaliyyətləri vahid hücum zənciri (Cyber Kill Chain) daxilində birləşdirmişdir. Bu isə mürəkkəb APT hücumlarının kritik zərər vurmadan öncə, yəni kəşfiyyat və şəbəkə daxili sızmanın ilkin mərhələlərində (early-stage) aşkarlanmasını mümkün etmişdir.

Polimorfizmlə mübarizədə yeni alternativ: Süni İmmun Sistemlərin (AIS) biomimetik alqoritmlərinin tətbiqi, dinamik olaraq mutasiyaya uğrayan polimorf zərərli proqramların imza verilənlər bazasına ehtiyac duyulmadan, onların funksional anomaliyaları və "yad" (non-self) faktorları əsasında müəyyən edilməsində son dərəcə perspektivli və resurs-effektiv bir alternativ olduğunu ortaya qoymuşdur.

ƏDƏBİYYAT

[1] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," in Leading Issues in Information Warfare & Security Research, vol. 1, no. 1, pp. 80–106, 2011.

[2] M. Roesch, "Snort: Lightweight intrusion detection for networks," in Proc. 13th USENIX Conf. System Administration (LISA), Seattle, WA, USA, Nov. 1999, pp. 229–238.

[3] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly detection: A survey," ACM Computing Surveys, vol. 41, no. 3, pp. 1–58, Jul. 2009, doi: 10.1145/1541880.1541882.

[4] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in Proc. Network and Distributed System Security Symposium (NDSS), San Diego, CA, USA, 2018, doi: 10.14722/ndss.2018.23204.

[5] B. Strom, A. Applebaum, D. Miller, K. Nickels, A. Pennington, and C. Thomas, MITRE ATT&CK: Design and Philosophy. Bedford, MA, USA: MITRE Corporation, 2018.

[6] M. Sikorski and A. Honig, Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. San Francisco, CA, USA: No Starch Press, 2012.

[7] D. Dasgupta, Artificial Immune Systems and Their Applications. Berlin, Germany: Springer-Verlag, 1999.

[8] S. Hochreiter and J. Schmidhuber, "Long short-term memory," Neural Computation, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.

Cyber Attack Detection and Cyber Threat Analysis

Farid Huseynov
State Security Service, Baku, Azerbaijan
faridhuseyn14@email.az

Abstract- The article examines modern cyberattack detection methods and cyberthreat analysis approaches. The research covers intrusion detection systems, anomaly detection algorithms, machine learning-based detection models, APT attack analysis, botnet infrastructure research, and malware behavior analysis. Methods based on artificial immune systems are reviewed and a hybrid detection approach suitable for modern network environments is proposed.

Keywords- cyber attack detection; anomaly detection; machine learning; malware analysis; botnet.