SYNCHROINFO JOURNAL

www.media-publisher.eu/synchroinfo-journal

DETECTING AND COUNTERING MODERN ATTACKS

Dovletaly N. Nuryagdyyev [1], Vitaly B. Kreindelin [2]

[1] The Institute of Telecommunications and Informatics of Turkmenistan, Ashgabat, Turkmenistan;
97dowlet97@gmail.com

[2] Moscow Technical University of Communications and Informatics, Moscow, Russia;
vitkrend@gmail.com

ABSTRACT

The IT community's top priority has become the implementation of monitoring and active defense tools, including IDS, IPS, and integrated IDS platforms. This paper provides a detailed analysis of existing threats, with a particular emphasis on the destructive impact of zero-day attacks, which have become a critical problem for US cybersecurity. It examines the paradigm of network infrastructure protection using IDS/IPS (Intrusion Detection System/Intrusion Prevention System) tools against the backdrop of a qualitative change in cyberthreats. Analyzing modern challenges – from fileless infection methods to targeted APT (Advanced Persistent Threat) campaigns – the authors point to the exhaustion of the potential of standard signature analysis. The paper aims to find ways to improve the effectiveness of network traffic monitoring in the face of constantly evolving attacker tools.

DOI: 10.36724/2664-066X-2026-12-2-2-7

Received: 07.02.2026
Accepted: 10.04.2026

Citation: D.N. Nuryagdyyev, V.B. Kreindelin, "Detecting and countering modern attacks," *Synchroinfo Journal* **2026**, vol. 12, no. 2, pp. 2-7.

KEYWORDS: *Information security, IDS/IPS solutions, machine learning, network packet analysis, data security, intrusion prevention, cyber threats, behavioral analysis, network resiliency*.

Introduction

Current cybercrime statistics demonstrate a sharp increase in the number of large-scale breaches of confidential information, affecting thousands of organizations worldwide. Such incidents cause reputational and economic damage to a wide range of individuals, from ordinary consumers to major investors. Under these circumstances, the IT community has prioritized the implementation of monitoring and proactive defense tools, including IDS, IPS, and integrated IDS platforms. This paper provides a detailed analysis of existing threats, with a particular emphasis on the destructive impact of zero-day attacks, which have become a critical issue for US cybersecurity [1].

Logging and auditing functionality in the designed IPS system

The effectiveness of incident identification and subsequent analysis mechanisms in intrusion prevention systems (IPS) directly depends on the quality of the generated log files. Although various technological solutions (WIPS, NIPS, HIPS) (from English: Wireless Intrusion Prevention System, from English: Network Intrusion Prevention System, from English: Host Intrusion Prevention System) have their own specific data sets, there is a basic layer of information attributes common to most systems.

Within the proposed IPS model, key attention is paid to the following groups of parameters:

• Temporal determination: The use of precise timestamps allows for the construction of a strict chronology of the attack, which is necessary for the correct reconstruction of events.

• Session identification: Each network interaction (for example, within the TCP protocol) (from English: Transmission Control Protocol) is assigned a unique session ID. This simplifies the aggregation of disparate packets into a single data stream.

• Criticality Metrics: Differentiating incidents by threat and confidence (Impact/Confidence Scoring) allows automated systems to prioritize responses to the most dangerous anomalies.

• Network Attributes: Data collection includes identifying protocols used at different layers of the OSI (Open Systems Interconnection) model (transport, application, network), as well as recording the physical (MAC) and logical (IP) addresses of the sender and recipient. MAC address analysis can also serve as an additional tool for identifying the vendor of the attacked or attacking device.

• Byte-by-byte analysis (Deep Inspection): To ensure maximum transparency, IPS monitors the entire volume of transmitted content, analyzing every byte within the established connection.

The final element of the system's functionality is protective measures logging – recording active actions taken to block threats. This information is critical for assessing the quality of the chosen security strategy.

Centralization and storage of information

The solution implements a centralized data aggregation model. All incidents identified as confirmed threats (True Positive) are transferred to a single repository. This approach provides:

• Cross-platform correlation: the ability to correlate suspicious activity recorded simultaneously at the network (NIPS), wireless (WIPS), and host (HIPS) levels.

• Fault tolerance: the central database supports redundancy mechanisms, including cloud backup and the creation of identical mirror copies (cloning).

Data lifecycle and retention policies

The duration of data storage is directly related to the system's analytical potential and operating costs. The proposed architecture utilizes a two-stage approach:

1. Local storage: primary sensors and collection points retain information "onboard" for seven days.

2. Long-term archiving: after a week, the data migrates to a central storage facility, where it is accumulated for up to 12 months.

This extended planning horizon enables in-depth historical analysis (retrospective analysis) and the generation of high-quality security reporting over long periods.

Neighborhood Analysis-Based Anomaly Detection Methods

Within the proposed solution, anomaly identification is based on a geometric representation of the data. The primary implementation tool is a method used to process samples containing both normal and malicious traffic [2].

Method Rationale and Mechanics.

The choice of outlier detection is based on its ability to recognize threats not present in the training data. The algorithm operates according to the following principle:

1. Standard Determination: Clusters representing typical ("normal") network behavior are formed.

2. Distance Calculation: For each new event, the mathematical distance to the centroid of the corresponding cluster is calculated.

3. Threshold Filtering: If the obtained value exceeds the set limit, the object is marked as an anomaly.

Benefits for IDS Systems

The integration of this mathematical framework into the system's analytical core aims to reduce the rate of false positives. The main advantages of the method are:

• High performance: A small number of iterative calculations makes the approach ideal for analyzing data streams in real time.

• Adaptability: Resistance to minor fluctuations in network patterns and ease of software implementation.

• Detection flexibility: Unlike signature-based methods, this approach allows for the identification of previously unknown attack types (zero-day) without requiring their descriptions to be entered into a knowledge base [3].

Pattern Matching Method

In addition to anomaly detection algorithms, the IPS being developed includes a deterministic analysis module based on signature matching. This component operates by continuously verifying incoming packets for specific characteristics corresponding to known cyberthreats [4].

Operating principle

The algorithm accesses a structured repository containing pre-defined patterns of malicious activity. These patterns can range from single compromise markers to complex behavioral chains. If an identical pattern is detected in the current information flow, the system immediately generates an alert and activates attack blocking protocols.

Justification for the choice of method

The integration of a signature-based approach into the system's analytics stack is driven by three key factors:

1. High classification accuracy: This method minimizes the likelihood of type I and type II errors (False Positives/False Negatives). This avoids false alarms, eliminating the unnecessary consumption of computing power on processing non-existent incidents.

2. Performance: Using an optimized set of decision rules, the algorithm demonstrates high data processing speed, preventing network bottlenecks.

3. Informative reports: Thanks to detailed descriptions in the signature database, the security administrator receives comprehensive information about the type and vector of the current attack, significantly simplifying the response process [5].

Application of expert rules in the analytical core

The IPS mechanism is based on the (rule-based detection) continuous recording of system events and the subsequent generation of decision algorithms. These instructions serve as criteria for classifying network activity as legitimate or malicious. In modern practice, it is common to distinguish two main concepts: anomaly detection and intrusion

attempt identification. These two concepts, despite their differences, can complement each other within a single platform.

Specifics of rule-based anomaly detection

This method overlaps significantly with statistical analysis, but its distinctive feature is the formation of specific logical conditions ("rules") describing the normal state of the system. The implementation process includes the following steps:

• Analysis of historical data: Based on audit archives, consistent patterns of resource use by users, software systems, and network nodes are identified.

• Formalization of behavioral models: The identified patterns are converted into a set of rules describing standard work cycles.

• Comparative monitoring: The current activity of subjects is compared with accumulated historical patterns. Any significant deviation from the recorded "norm" is interpreted as a potential incident.

The effectiveness of such systems directly correlates with the size and quality of the rule base: the more detailed the behavioral profiles are described, the higher the accuracy of threat recognition.

Key features of the approach

• Contextual flexibility: The system is capable of identifying suspicious activity even when it formally fits within established use patterns. This is achieved by flagging specific system calls as potentially dangerous.

• Platform adaptation: Decision rules are designed taking into account the architectural features of specific nodes and the specific operating systems used, minimizing the likelihood of errors.

• Development methodology: The most effective way to build a rule base is through proactive analysis of exploits, hacking tools, and malicious scripts available in open and specialized sources. This allows the system to "know" the attacker's logic before an attack occurs.

Antivirus

Antivirus protection tools are a fundamental tool for identifying, blocking, and eliminating destructive software. Operating in the background, these solutions provide continuous monitoring of the operating environment, protecting not only user data but also the system's hardware resources. Modern products also include advanced functionality, such as web filtering and configurable firewalls [6].

Mechanics of interaction within the proposed IPS

In the designed intrusion prevention system, the antivirus component is installed directly on host computers. Its operation is based on the following principles:

• Signature verification: Software code is scanned for matches against global databases of known threats. Automated signature updates ensure up-to-date protection against the latest malware modifications.

• Reactive incident management: Upon receiving a signal from the IDS module about a detected intrusion, the antivirus software localizes the compromised objects. The system can automatically quarantine a suspicious file, restrict access to it, or completely delete it.

• Notification and auditing: Upon detection of virus activity, an instant notification is generated for the security administrator, allowing for prompt adjustment of the security policy.

The Importance of Maintenance

A key factor in the effectiveness of an antivirus module is the regularity of its intelligent database updates. Our model features a hybrid update scheme (manual and automatic), which is critical for maintaining a high level of security in the ever-changing cyberthreat landscape.

Advanced antivirus

Traditional antivirus solutions that rely on signature databases remain effective in blocking known threats, but they are ineffective against modern polymorphic attacks. Advances in endpoint protection are driven by the implementation of behavioral analysis, artificial intelligence (AI), and machine learning (ML) technologies. These tools enable the identification of malicious intent, not just searching for matches in file structures.

Intelligent analysis and preventive response

The use of AI (artificial intelligence) and ML algorithms is transforming the threat detection process:

• Behavioral monitoring: Systems detect anomalies in real time, which is critical for blocking zero-day exploits.

• Predictive classification: Predictive analytics methods enable new virus strains to be matched to known families based on common behavioral traits, increasing detection accuracy.

• Automated protection: The use of AI reduces response time through autonomous policy updates and instant suppression of malware activity.

Comparison of EDR, MDR, and XDR architectures

The modern cybersecurity landscape is represented by three key concepts being implemented by leading vendors (Kaspersky, CrowdStrike, FireEye, etc.):

1. EDR (Endpoint Detection and Response): Focuses on continuous event monitoring on specific nodes. In addition to blocking, EDR (Endpoint Detection and Response) provides forensic analysis tools, allowing for detailed reconstruction of the incident chronology.

2. MDR (Managed Detection and Response): This is a service model that combines tools (SIEM (Security Information and Event Management), EDR, and traffic analysis) with the expertise of external specialists. This is the optimal solution for organizations experiencing a shortage of in-house information security resources.

3. XDR (Extended Detection and Response): The highest level of security system evolution. XDR integrates data from various environments – network, clouds, and endpoints – providing intelligent event correlation and automatic suppression of false alarms.

Quarantine

The designed intrusion prevention system is based on a hybrid protection model integrating antivirus modules with object isolation and backdoor countermeasures [2].

The system's operational cycle is structured as follows:

1. Isolation and Initial Containment

If malicious code is identified, the IPS immediately blocks the threat, moving the destructive object to a dedicated secure storage area (quarantine). This measure helps stop the spread of an attack at an early stage and minimize damage to the infrastructure [8, 9].

2. Recursive Scanning

After initial threat containment, the antivirus component initiates a deep inspection of the entire system. The goal of this stage is to find hidden attack vectors or secondary malicious modules that may have been introduced during the incident. If correlated threats are detected, they undergo a similar isolation procedure. If there are no signs of compromise, the system is assigned the status of "verified security."

3. Notification and Feedback

To maintain transparency in security management processes, a notification subsystem has been implemented. The IPS generates detailed reports sent to administrators and users via secure communication channels (email). Notifications contain:

• The type and severity of the recorded incident;

• A history of security events;

• A list of automated measures taken to neutralize the threat.

Conclusion

The study confirms that intrusion detection and blocking systems (IDS/IPS) remain a critical component of a defense-in-depth strategy. However, the dramatic change in the cyber threat landscape and the widespread adoption of cryptographic protocols necessitate a transformation of traditional security paradigms.

Key Findings and Development Prospects

Shift in Technological Focus: Traditional signature-based analysis is losing its effectiveness against dynamic attack vectors. The IDS/IPS development vector is shifting toward intelligent analysis based on machine learning and AI. This enables a shift from reactive searches for known matches to proactive identification of hidden patterns and anomalous behavior.

System Integration and Synergy: Using IPS in isolation is becoming impractical. Modern security architecture requires tight convergence of security tools within unified platforms (XDR, SIEM, SOAR). XDR (Extended Detection and Response)

SIEM (Security Information and Event Management)

SOAR (Security Orchestration, Automation, and Response).

This integration provides end-to-end visibility into the infrastructure and enables threat intelligence mechanisms for the rapid exchange of data on current threats.

Adaptation to encapsulated traffic: Extensive use of TLS/SSL protocols. TLS (Transport Layer Security)

SSL (Secure Sockets Layer) creates significant obstacles to deep packet inspection (DPI). The optimal solution to this contradiction between privacy and security seems to be the transition to the analysis of network session metadata, which allows for the identification of signs of compromise without violating the integrity of encrypted communication channels [7, 10, 11].

REFERENCES

[1] K. Scarfone, Guide to Intrusion Detection and Prevention Systems (IDPS). NIST Special Publication 800-94. Washington: National Institute of Standards and Technology, 2024 (updated). 120 p.

[2] X. Chen, “Intrusion Detection and Prevention Systems: Hybrid Models and Isolation Mechanisms,” *Journal of Cybersecurity and Information Management*, 2018. Vol. 12, no. 4, pp. 45–58.

[3] V. I. Averchenkov, Intrusion Detection Systems: A Textbook for Universities. 3rd ed. Moscow: Flinta, 2022. 145 p.

[4] Yu. S. Vasiliev, “Machine Learning in Information Security Problems: Anomaly Detection Methods,” *Information Technology Security*. 2021. No. 2, pp. 88-101.

[5] E. Tanenbaum, D. Weatherall, Computer Networks. 6th ed. St. Petersburg: Piter, 2023. 992 p.

[6] Kaspersky Lab. Modern Cyber Threat Landscapes: EDR, MDR, and XDR Solutions / Kaspersky Lab: official website. URL: https://www.kaspersky.ru/enterprise-security/endpoint-detection-response (accessed: 27.01.2026).

[7] V. F. Shan'gin, Computer Information Protection. Effective Methods and Tools. Moscow: DMK Press, 2020. 544 p.

[8] V. B. Kreindelin, N. A. Legkov, “Protecting Authentication Data for Websites and WEB Applications,” *Telecommunications and Information Technology*. 2022. Vol. 9, No. 1, pp. 6-10.

[9] V. G. Olifer, N. A. Olifer, Computer Networks. Principles, Technologies, Protocols: Textbook for Universities. St. Petersburg: Piter, 2020. 992 p. (in the context of network infrastructure security).

[10] V. B. Kreindelin, G. A. Vakhromeev, “The Most Effective Machine Learning Algorithms for Risk-Based Authentication Systems,” *Telecommunications and Information Technology*. 2024. Vol. 11, No. 1, pp. 87-92.

[11] M.G. Bakulin, T.B.C. Ben Rejeb, V.B. Kreyndelin, D.Y. Pankratov, A.E. Smirnov, “Code domain NOMA in 3GPP specifications: 5G or 6G?,” *T-Comm*. 2022. vol. 16, no.1, pp. 4-14. DOI: 10.36724/2072-8735-2022-16-1-4-14.