INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com
Volume 14, Issue 1, No 23, 2026
ISSN: 2348-6600
REFERENCE ID: IJCS-687
PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

EVOLUTION OF MALWARE TACTICS IN 2025-2026: AI-DRIVEN THREATS, SUPPLY CHAIN VULNERABILITIES, AND MEMORY-BASED DETECTION

Mr.V.J.Fready Blesson
Assistant Professor,
PG Department of Commerce with Computer Applications,
Mannar Thirumalai Naicker College,
Madurai, Tamil Nadu, India.

Mrs.T.Sudhamathi
Assistant Professor ,
Department of Commerce(IT),
Mannar Thirumalai Naicker College,
Madurai, Tamil Nadu, India.

Abstract

The cybersecurity threat landscape has undergone significant transformation in 2025-2026, characterized by the integration of artificial intelligence across the attack lifecycle and the exploitation of software supply chains. This paper presents a comprehensive analysis of contemporary malware tactics, detection methodologies, and defense strategies based on recent industry reports and academic research. We examine the role of AI as a force multiplier in social engineering, reconnaissance, and malware development, alongside the fragmentation of ransomware operations toward decentralized models.

The paper investigates supply chain vulnerabilities in open-source ecosystems, particularly the PyPI repository, and evaluates machine learning-based detection frameworks including DySec, which achieves 96% accuracy in identifying malicious packages. Furthermore, we analyze memory forensics approaches enhanced by large language models for interpretable threat hunting and indicator extraction.

Our findings indicate that modern malware defense requires hybrid approaches combining static, dynamic, and memory-based analysis, with explainable AI playing an increasingly critical role in analyst workflow efficiency.

Keywords: Malware analysis; artificial intelligence; supply chain security; memory forensics; machine learning detection; ransomware evolution.

I. Introduction

The cybersecurity landscape in 2025-2026 reflects a paradigm shift in attacker methodologies, defensive technologies, and the underlying infrastructure supporting both. Malware, defined as covert software designed

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 23, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-687 PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

to perform malicious acts including data theft, data alteration, and service disruption, remains the most critical threat in cybersecurity.

The persistent evolution of malware has necessitated increasingly sophisticated detection and prevention techniques, driving the integration of artificial intelligence into both offensive and defensive cybersecurity operations Recent industry research indicates that artificial intelligence is now embedded across the attack lifecycle, accelerating the execution of familiar techniques at greater speed and scale Check Point Research's Cyber Security Report 2026 documents measurable shifts including a 97% increase in risky AI prompts and vulnerability in 40% of analyzed Model Context Protocols, highlighting how AI systems themselves have become direct sources of enterprise risk Concurrently, software supply chain attacks have emerged as a critical vulnerability vector, exploiting trust in open-source repositories such as the Python Package Index (PyPI).

Traditional metadata inspection and static code analysis have proven inadequate against advanced attack strategies including typosquatting, covert remote access activation, and dynamic payload generation This inadequacy has driven the development of dynamic analysis frameworks capable of monitoring real-time behavioral patterns during package installation. Memory forensics has likewise gained prominence as an effective methodology for analyzing living-off-the-land malware, including threats employing evasion, obfuscation, anti-analysis, and steganographic techniques By capturing volatile system state, memory analysis enables recovery of transient artifacts such as decrypted payloads, executed commands, credentials, and cryptographic keys that remain inaccessible through static or traditional dynamic analysis

This paper synthesizes findings from industry threat reports and academic research to provide a comprehensive view of the current malware landscape. Section II examines the evolution of malware tactics including AI-driven attacks and ransomware fragmentation. Section III analyzes supply chain vulnerabilities and detection frameworks.

Section IV explores memory forensics and AI-assisted analysis. Section V discusses detection methodologies and their comparative effectiveness. Section VI presents conclusions and future research directions.

II. Evolution of Malware Tactics in 2025-2026

A. Artificial Intelligence as a Force Multiplier

The integration of artificial intelligence into cyber attacks represents perhaps the most significant tactical evolution observed in 2025. Rather than enabling fundamentally new attack types, AI has primarily functioned as a force multiplier, accelerating and scaling existing techniques Key observations from industry research include increasingly convincing social engineering with fewer

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 23, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-687 PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

detectable indicators, faster reconnaissance and targeting reducing time-to-compromise, and accelerated malware development cycles Alongside its role as an enabler, AI has become a direct source of enterprise risk. Research conducted in 2025 identified measurable exposure tied to how organizations deploy and govern AI systems

Critical data points include: Risky AI prompts increased by 97% in 2025, indicating widespread experimentation with AI systems that may expose sensitive data or create security gaps 40% of analyzed Model Context Protocols (MCPs) were vulnerable, suggesting fundamental security weaknesses in how AI applications interact with external system. Elevated trust and autonomy in AI systems amplify the impact of prompt injection and workflow abuse, creating new attack surfaces

The implications for malware development are profound. Attackers now leverage AI to generate polymorphic code variants, automate reconnaissance, and personalize phishing campaigns at scale. Traditional signature-based detection methods struggle against AI-generated malware that can dynamically alter its code structure while maintaining malicious functionality.

B. Ransomware Fragmentation and Operational Evolution

Ransomware activity continued to increase throughout 2025 despite multiple law enforcement takedowns of high-profile groups [2]. Research findings document a significant shift away from centralized ransomware brands toward smaller, decentralized operators. This fragmentation reflects both successful law enforcement pressure and the maturation of ransomware-as-a-service business models.

Key Evolutionary Characteristics include:

Increased use of data-only extortion without encryption, reducing operational complexity while maintaining extortion leverage More personalized extortion tactics based on victim profiling, enabled by AI-powered reconnaissance and data analysis Shorter attack and negotiation timelines supported by automation and AI, compressing the window for defensive response

This evolution reflects a broader shift toward operational efficiency and decentralized execution. Rather than relying on single, monolithic ransomware families, attackers now employ diverse toolkits and adapt their approaches based on victim characteristics and defensive postures.

Unmonitored devices played a growing role in intrusion activity during 2025, particularly in large-scale and targeted attacks. Observed trends include exploitation of routers, gateways, VPN appliances, and other perimeter devices; use of edge devices for persistent access and lateral movement; delayed detection due to limited monitoring and patching coverage; and supply-chain and

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 23, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-687 PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

vendor ecosystem exposure amplifying risk. These devices often sit outside standard endpoint and identity security controls, creating blind spots that attackers exploit for initial foothold establishment.

Once compromised, edge infrastructure provides reliable persistence and facilitates internal network movement with reduced detection probability.

III. Software Supply Chain Vulnerabilities and Detection

A. The PyPI Ecosystem Threat Landscape

Malicious Python packages make software supply chains vulnerable by exploiting trust in open-source repositories like Python Package Index (PyPI). The popularity of PyPI as a distribution mechanism for Python libraries has made it an attractive target for attackers seeking to compromise downstream applications that depend on these packages. Traditional security approaches for open-source repositories rely heavily on metadata inspection and static code analysis.

However, these Methods Prove Inadequate Against Advanced Attack Strategies including:

- **Typosquatting:** Registering packages with names similar to popular libraries, exploiting typographical errors in installation commands
- **Covert remote access activation:** Establishing backdoor access that activates only under specific conditions
- **Dynamic payload generation:** Generating malicious code at runtime to evade static analysis
- Multiphase attack malware: Spreading malicious activity across multiple stages to complicate detection [3]

The inadequacy of static approaches stems from their inability to observe runtime behavior.

Malicious packages may appear benign during static inspection while executing harmful operations during or after installation.

B. DySec: Dynamic Analysis Framework

To address these challenges, researchers introduced DySec, a machine learning-based dynamic analysis framework for PyPI that uses eBPF kernel and user-level probes to monitor behaviors during package installation. The framework captures 36 real-time features spanning multiple behavioral dimensions:

I. Table i. Dysec dynamic feature categories [3]

Feature Category	Examples	Detection Value
System Calls	File operations, process creation	Identifies unauthorized system interactions

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 23, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-687 PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

Network Traffic	Connection attempts, data exfiltration	Detects command-and-control communication
Resource Usage	CPU spikes, memory allocation	Reveals resource-intensive malicious operations
Directory Access	File system modifications	Identifies payload placement
Installation Patterns	Hook installations, service registration	Detects persistence mechanisms

The research team developed a comprehensive dataset of 14,271 Python packages, including 7,127 malicious sample traces, by executing them in a controlled isolated environment. This dataset represents one of the largest collections of labeled malicious package behaviors available for research. Experimental results demonstrate DySec achieving 96% detection accuracy with machine learning inference latency below 0.5 seconds after dynamic feature extraction

More importantly, the framework reduces false negatives by 78.65% compared to static analysis and 82.24% compared to metadata analysis, demonstrating the critical importance of behavioral monitoring. During evaluation, DySec flagged eleven packages that PyPI classified as benign. Manual analysis, including installation behavior inspection, confirmed six as malicious. These findings were reported to PyPI maintainers, resulting in the removal of four packages [3]. This real-world impact validates the practical value of dynamic analysis approaches.

References

1. S. Khan, H. Raza, and M. Alam, "AI-Driven Malware Analysis and Detection: A Comprehensive Survey of Techniques, Trends and Challenges," Journal of Informatics and Web Engineering, vol. 5, no. 1, pp. 106–129, Feb. 2026. doi:10.33093/jiwe.2026.5.1.7.
2. Check Point Research, "Cyber Security Report 2026," Check Point Software Technologies, Tel Aviv, Israel, Jan. 2026. [Online]. Available: https://research.checkpoint.com/2026/cyber-security-report-2026/
3. S. T. Mehedi, C. Islam, G. Ramachandran, and R. Jurdak, "DySec: A Machine Learning-based Dynamic Analysis for Detecting Malicious Packages in PyPI Ecosystem," IEEE Transactions on Information Forensics and Security, vol. 21, pp. 6–1331, Feb. 2026. doi: 10.1109/TIFS.2026.3654388.
4. S. L. Sanna, D. Maiorca, and G. Giacinto, "An Explainable Memory Forensics Approach for Malware

INTERNATIONAL JOURNAL OF COMPUTER SCIENCE
Scholorly Peer Reviewed Research Journal - PRESS - OPEN ACCESS
ISSN: 2348-6600
Since 2012
www.ijcsjournal.com Volume 14, Issue 1, No 23, 2026 ISSN: 2348-6600
REFERENCE ID: IJCS-687 PAGE NO: 017-022
Special Issue - Innovative Commerce: Bridging Business and Computer Applications (ICBBCA-2026)
PG Department of Commerce with Computer Applications, Mannar Thirumalai Naicker College, Madurai – March 2026

Analysis," arXiv preprint arXiv:2602.19831, Feb. 2026. [Online]. Available: https://arxiv.org/abs/2602.1983

5. U. Prasad and A. Chawla, "A Unified Evaluation of Learning-Based Similarity Techniques for Malware Detection," arXiv preprint arXiv:2602.15376, Feb. 2026. [Online]. Available: https://arxiv.org/abs/2602.15376
6. K. Aryal et al., "Robustness and Adversarial Resilience for Malware ML," University of Nebraska Omaha, Omaha, NE, USA, 2026. [Online]. Available: https://www.unomaha.edu/college-of-information-science-and-technology/research-labs/collaboratoriums/cybersecurity.php
7. H. Manthena, S. Shajarian, J. Kimmell, M. Abdelsalam, S. Khorsandroo, and M. Gupta, "Explainable Artificial Intelligence (XAI) for malware analysis: A survey of techniques, applications, and open challenges," IEEE Access, vol. 13, pp. 61611-61640, 2025. doi: 10.1109/access.2025.3555926.
8. VMRay Labs, "December 2025 - January 2026 Detection Highlights: 12 new VTIs, 65+ YARA rules, and more config extractors," VMRay, Bochum, Germany, Feb. 2026. [Online]. Available: https://www.vmray.com/december-2025-january-2026-detection-highlights12-new-vtis-65-yara-rules-and-more-config-extractors/
9. A. Djenna, A. Bouridane, S. Rubab, and I. Marou, "Artificial intelligence-based malware detection, analysis, and mitigation," Symmetry, vol. 15, no. 3, pp. 677, 2023. doi: 10.3390/sym15030677.
10. R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, and S. Venkatraman, "Robust intelligent malware detection using deep learning," IEEE Access, vol. 7, pp. 46717-46738, 2019. doi: 10.1109/ACCESS.2019.2906934.