*International Journal of Scientific Research and Engineering Development-– Volume 8 Issue 5, Sep-Oct 2025*
*Available at www.ijsred.com*

RESEARCH ARTICLE OPEN ACCESS

# Malware and Anti-Malware: A Comprehensive Review

Rudra Tanti[1], Ashwini Vaidya[2]
[1](B Tech in Computer Engineering, Atmiya University, Rajkot, India
Email: rudratantu3040@gmail.com )
[2](Faculty of Engineering & Technology (CE), Atmiya University, Rajkot, India
Email: ashwini.vaidya@atmiyauni.ac.in )

## Abstract

With the explosive growth of digital connectivity and the professionalization of cybercrime, malware attacks have become one of the most persistent and sophisticated cybersecurity threats. This landscape now ranges from traditional viruses and worms to complex ransomware-as-a-service (RaaS) syndicates and advanced persistent threats (APTs). Anti-malware technologies are the critical countermeasure, evolving rapidly from simple signature-based detection to sophisticated behavioral analysis, AI-powered threat intelligence, and cloud-based scanning architectures. This paper reviews the contemporary landscape of malware and anti-malware approaches, analyzing the critical shift toward dynamic and behavioral defense methodologies. The analysis addresses persistent roadblocks, including polymorphic malware generated by generative AI, zero-day exploits, fileless attacks leveraging Living Off the Land (LotL) binaries, and the operational challenge of alert fatigue caused by false positives. Furthermore, the review explores future possibilities, including the deployment of AI-driven adaptive defense mechanisms, the implementation of blockchain for ensuring software integrity, the establishment of federated threat intelligence sharing frameworks, and the necessary transition to quantum-resistant cryptography.

## I.Introduction:

### The Persistent shadow of malware

### A. Historical Context and Exponential Growth

The digital revolution has fundamentally transformed global operations, creating vast new infrastructure but simultaneously opening fertile ground for cybercriminals. Malware—malicious software designed to disrupt, damage, or gain unauthorized access to systems—has expanded dramatically in sophistication, distribution speed, and potential impact. The threat has grown global and transcends conventional information technology concerns, now posing significant financial, supply chain, and national security risks. Modern threats have shifted drastically from early, isolated viruses to highly industrialized criminal enterprises. Today, this industrialization is largely characterized by the rise of Ransomware-as-a-Service (RaaS) syndicates, where core developers lease toolkits and infrastructure to a network of affiliates, thereby lowering the barrier to entry for complex, high-impact attacks.

### B. Scale and Financialization of the Threat (2023–2025 Landscape)

The threat landscape is accelerating exponentially, demanding an adaptive defensive posture. Current malware statistics reveal that cybersecurity systems detect approximately 560,000 new malware threats daily, highlighting the sheer scale of automated cybercrime. Analysis indicates a steady, rapid acceleration in threat volume, with projections estimating a rise from 5.8 billion infections globally in 2023 to approximately **6.5 billion infections in 2025**. This increase is primarily fueled by the proliferation of AI-generated malware and sophisticated phishing campaigns.

The motivation behind these threats is overwhelmingly economic. Data from 2024 shows

  

that **55% of threat groups active were financially motivated**, marking a steady increase, while 8% were primarily motivated by espionage. Ransomware remains the preferred tool for financial gain, with attacks experiencing a significant surge, showing a 40% year-over-year increase globally in the first half of 2024.

This increase in sophisticated, financially motivated attacks contributes directly to soaring operational costs for defense. The global average cost of a data breach reached **USD 4.9 million in 2024**. This financial impact is exacerbated by widespread staffing deficits; more than half of breached organizations in 2024 reported facing severe cybersecurity staffing shortages (the skills gap), which statistical analysis links to a **USD 1.76 million increase** in the average cost of a data breach. The implication is a negative feedback loop: artificial intelligence dramatically lowers the barrier to entry for adversaries, generating more threats faster, while the deficit in human defensive capacity makes detection and remediation slower and significantly more expensive.

Furthermore, a critical metric confirming the limitations of current defenses is the global median dwell time—the period an attacker remains undetected within a network. This metric rose to **11 days in 2024**. This sustained rise, despite the proliferation of Endpoint Detection and Response (EDR) solutions, indicates that standard defensive mechanisms are frequently failing against stealthy, memory-resident, and Living Off the Land (LotL) threats, thereby validating the urgent need for advanced behavioral analysis and memory forensics techniques.

## II. Core Concepts: Understanding Malware and Defense

### A. Modern Malware Taxonomy (Focus on Evasion)

Modern malware taxonomy is defined by its focus on evasion. While legacy categories like viruses, worms, and Trojans still exist, the most pressing threats employ techniques specifically designed to circumvent detection systems:

- **Ransomware-as-a-Service (RaaS):** This model represents the complete commercialization of the threat, where specialized syndicates provide toolkits, infrastructure, and negotiation services to affiliates for a cut of the ransom proceeds.
- **Fileless Malware & Memory-Resident Threats:** These malicious payloads reside entirely in the volatile random-access memory (RAM) or utilize native operating system scripting tools (e.g., PowerShell, WMI) rather than installing files on the disk. This approach allows the malware to bypass traditional signature-based anti-virus (AV) solutions that rely on scanning the static file system.

### B. Foundational Analysis Techniques and Their Limitations

Traditionally, anti-malware solutions relied on two primary methods, both of which are increasingly obsolete against modern adaptive threats:

- **Signature-Based Detection:** This foundational technique scans files for known malicious hashes or specific binary patterns. While fast, its efficacy is immediately rendered void by polymorphic malware or newly released threats (zero-days).
- **Heuristic Analysis:** This method moves beyond exact matching by assigning risk scores based on suspicious characteristics, such as attempts to modify core system components or unusual API call sequences. It serves as a necessary, intermediate layer of defense but is often easily bypassed by sophisticated code obfuscation.

### C. Advanced Behavioral and Runtime Detection

The modern defense paradigm centers on detecting the *intent* of the code rather than its static structure.

#### Behavioral Analysis Techniques (Dynamic Analysis)

Behavioral analysis monitors a program's runtime

  

activities, observing the dynamic sequence of API calls, system calls, network interactions, and file system modifications, often within isolated sandbox environments. A current challenge lies in translating these complex runtime behaviors into actionable features for Machine Learning (ML) models. Research is focusing on advanced feature extraction, using techniques like converting sequences of API calls into dense vector representations via Natural Language Processing (NLP)-style encoders, such as MalDetConv. This evolution aims to move beyond simple sequence detection to automatically extract high-level semantic features of malicious behavior.

Furthermore, novel approaches have demonstrated high efficacy by abandoning traditional high-privilege telemetry in favor of easily accessible system performance data. This method relies on collecting multi-valued time series information (CPU, RAM, disk, and network usage) and training Long Short-Term Memory (LSTM) networks, with data augmentation performed by Generative Adversarial Networks (GANs), achieving high accuracy (up to 0.99) in sandbox testing.

A significant challenge arises when shifting from laboratory conditions to real-world deployment. Studies have exposed a critical gap: ML detectors trained on curated, controlled sandbox traces (which often report performance exceeding 90% accuracy) drop dramatically to between 20% and 50% accuracy when deployed at real endpoint hosts. This massive performance degradation stems primarily from data *distribution shift* (the environment and execution context differ substantially between sandboxes and real machines) and *label noise*. This phenomenon necessitates a departure from current academic practice, compelling defenders to train models directly on messy, real-world endpoint telemetry data to achieve robust efficacy.

### D. Memory Forensics and Volatile Data Acquisition

To counter the rise of fileless and in-memory malware, defense systems have increasingly integrated memory forensics. This discipline focuses on acquiring and analyzing volatile data stored in RAM. Since data in RAM is dynamic, exclusive, and not saved to disk, it contains essential forensic information about running processes, malicious activity, and unauthorized network connections that would be invisible to disk-based scanning.

The process involves two critical phases: First, **Memory Acquisition**, where a suspicious process is executed in a controlled environment and the volatile memory is dumped using specialized tools (e.g., Magnet RAM Capture, FTK Imager). Second, **Analysis**, utilizing tools like Volatility to extract domain-specific characteristics. Recent advancements integrate ML and Computer Vision techniques applied directly to memory analysis data, resulting in high accuracy (e.g., 97.01% for detection and classification). Furthermore, mitigation against such threats includes implementing Automated Moving Target Defense (AMTD), which dynamically randomizes application memory layout to disrupt advanced threats.

## III. Industrial Architecture: Malware Defense Ecosystem

The industrial response to the evolving threat matrix has been a continuous expansion of security scope, culminating in highly integrated, threat-centric architectures.

### A. Endpoint Protection Platforms (EPP) and EDR

The foundational security layer remains the Endpoint Protection Platform (EPP), which combines traditional AV, firewalls, and basic behavioral monitoring. Building upon this, Endpoint Detection and Response (EDR) solutions emerged, focusing on continuous monitoring of endpoint processes, collecting deep telemetry, detecting anomalies, and enabling high-fidelity investigation and rapid remediation. EDR represents the indispensable foundation for all subsequent, advanced cyber capabilities.

  

### B. The Transition to Extended Detection and Response (XDR)

The increasing complexity of attacks that move laterally across domains (endpoint, email, cloud, network) necessitated a new architectural philosophy. Extended Detection and Response (XDR) represents a significant evolution, shifting from an endpoint-centric view to a **holistic, unified defense strategy**. XDR eliminates data silos by integrating telemetry from endpoints, network security devices, email gateways, cloud environments, and identity systems.

XDR architecture is built upon core components designed for cross-domain threat correlation: 1) Broad Data Collection and Ingestion from diverse security tools; 2) Advanced Analytics and Correlation (often AI-driven); 3) Real-time Threat Intelligence Integration; and 4) Automated, Cross-Domain Response Mechanisms.

The value proposition of XDR is clear: unlike SIEM systems, which primarily centralize information and logs, XDR centralizes and unifies security *tooling*, enabling a comprehensive, predictive defense. This orchestrated approach allows a coordinated response action to be triggered across the entire security stack instantaneously, directly addressing the failure of siloed EDR/SIEM to adequately reduce the rising median dwell time of attackers. This rapid adoption of XDR architecture is a direct industrial response to the increasing need for security automation and consolidated threat context.

Table 1 provides a comparison of these foundational defense solutions.

Table 1: Architectural Comparison of Key Defense Solutions

| Attribute | Endpoint Protection Platform (EPP) | Endpoint Detection & Response (EDR) | Extended Detection & Response (XDR) |
|---|---|---|---|
| **Primary Focus** | Prevention (Signature/Heuristic AV) | Deep endpoint monitoring and investigation | Unified threat context and cross-domain response |
| **Data Scope** | Single endpoint telemetry/files | Detailed endpoint process logs/events | Aggregated telemetry from Endpoints, Cloud, Network, Email, Identity |
| **Threat Handling** | Block known signatures | Alerting, threat hunting, guided manual response | Automated correlation, predictive modeling, orchestrated response across security tools |
| **Trend (2024-2028)** | Foundational Layer | Core capability, integrated into MXDR/XDR | Rapid adoption for holistic defense |

### C. Role of SIEM and SOAR in the Modern Ecosystem

Security Information and Event Management (SIEM) remains crucial, functioning as the primary data aggregator. SIEM systems collect, normalize, and analyze logs from the entire infrastructure, including servers, network devices, firewalls, and the telemetry generated by EDR/XDR systems. SIEM uses correlation rules and increasingly incorporates AI and automation to detect multi-domain threats and provide essential compliance reports.

Security Orchestration, Automation, and Response (SOAR), while often implicitly integrated into XDR, provides the critical mechanism for automating the response phase. SOAR executes predefined playbooks based on high-fidelity alerts generated by XDR or SIEM, enabling security teams to triage and mitigate threats much faster than human analysts could manually.

### D. Deep Integration of AI in Commercial Defense

Leading commercial platforms have deeply embedded Artificial Intelligence into nearly every layer of defense. Vendors like Sophos and SentinelOne now rely on numerous Deep Learning and Generative AI models (exceeding 50 models in some solutions) to deliver protection against both known and *never-before-seen* attacks. These specialized models are deployed for tasks such as web protection (malicious URL detection), email security (NLP for identifying impersonation attempts), and real-time behavioral defense against complex endpoint threats. This robust

  

integration represents an acceptance that only adaptive, machine-speed analytics can counter the speed and sophistication of modern automated malware.

## IV. Case Spotlights: Malware and Defense in Practice

### A. Supply Chain Vulnerabilities (The Ripple Effect)

The compromise of third-party vendors has become a dominant and catastrophic attack vector.

#### MOVEit Transfer (2023)

The MOVEit Transfer incident, beginning in June 2023, demonstrated the devastating impact of supply chain vulnerability combined with zero-day exploitation. The Cl0p RaaS group exploited a critical SQL injection zero-day (CVE-2023-34362) in the managed file transfer tool. This single flaw allowed the attackers to gain unauthorized access and steal data from customer databases, ultimately affecting over 620 organizations globally, including major entities like the BBC and British Airways.
This catastrophe underscores the inability of traditional vendor management to mitigate risk effectively, particularly concerning "vendor's vendors" who rely on third-party tools for processing data. It also highlights the urgency of promptly patching zero-day vulnerabilities, even though the exploitation by Cl0p often occurred before organizations could apply vendor-released patches.

#### XZ Utils Backdoor (2024) and Open Source Risk

The near-miss involving the XZ Utils backdoor in early 2024 revealed the pervasive risks inherent in the open-source software supply chain. A software engineer detected malicious code planted within the XZ compression utility, a fundamental component used across many Linux distributions. This incident occurred alongside a notable increase—a **28% rise in malicious packages** uploaded to open-source repositories in 2023—confirming that adversaries are consistently targeting software supply chains as a highly leveraged attack surface.

### B. Nation-State Espionage and Living Off the Land (LotL)

Nation-state Advanced Persistent Threat (APT) groups frequently pioneer sophisticated evasion techniques that eventually diffuse to financially motivated criminal groups.

#### Volt Typhoon (PRC-Nexus)

Volt Typhoon, identified as a Chinese state-sponsored APT group, has been active since at least 2021, focusing on espionage and gathering information, often targeting U.S. critical infrastructure sectors such as defense and utilities.

#### LotL Tactics

Volt Typhoon's primary tactic, technique, and procedure (TTP) is "Living Off the Land" (LotL). This technique involves using native, legitimate Windows binaries, scripts, and libraries—often referred to as LOLBAS—to carry out malicious operations. Volt Typhoon has been specifically documented using built-in administration tools like wmic, ntdsutil, netsh, and PowerShell for reconnaissance, persistence, and lateral movement.
This strategy allows the actor to evade detection by blending their malicious activities with normal system and network behavior. Importantly, LotL bypasses EDR products that typically flag the introduction of third-party executables, turning legitimate system functions into mechanisms for intrusion. The high level of stealth required by APTs, exemplified by the rise in median dwell time, demands that defense mechanisms move beyond simple file-based detection toward deep, contextual process chain analysis to identify the malicious *intent* behind otherwise benign commands.

### C. Modern RaaS Syndicates and High-Impact

  

**Attacks**

Ransomware remains the dominant high-impact threat, experiencing a **40% year-over-year increase** in global attacks in the first six months of 2024. Attackers favor two initial infection vectors: exploits of external-facing vulnerabilities, which account for **33% of initial access**, and the use of **stolen credentials (16%)**.
Ransomware operators consistently weaponize zero-day vulnerabilities for post-compromise privilege escalation, exemplified by the rapid adoption and exploitation of flaws like the Microsoft Common Log File System (CLFS) vulnerability in recent campaigns.

## V. Persistent Roadblocks

### A. Evasion through Code Mutation and Obfuscation

Attackers continuously employ code obfuscation to maximize the lifespan of their malware and complicate reverse engineering. Obfuscation fundamentally aims to prevent static analysis by modifying the code's structure without altering its execution logic.
Common mechanisms include **packing and encryption**, where the core malicious payload is compressed or encrypted and hidden within an outer stub that only decrypts and executes the payload at runtime. More advanced techniques include **Control Flow Obfuscation**, which manipulates the program's execution path with junk code, and **API Hashing**, which conceals crucial API function calls, making it difficult for analysts and tools to discern the malware's intent during static examination.

### B. The Paradigm Shift: AI-Driven Polymorphism

The introduction of Generative AI tools and large language models (LLMs) has fundamentally accelerated the arms race, creating a new class of threats: AI-driven polymorphic malware. Adversaries are leveraging these tools to automatically and dynamically generate, obfuscate, and modify malicious code at build-time or even at runtime.
A pivotal example is the **BlackMamba proof-of-concept (PoC) malware (2023)**, which utilized OpenAI's APIs to dynamically generate unique polymorphic keyloggers during execution. Because the payload's structure was constantly rewritten, never hardcoded, and functionally distinct across instances, it instantly defeated traditional static signature matching and pattern-based detection tools.
This capability is moving rapidly from PoC to real-world deployment. APT groups, such as the Russian-nexus **Forest Blizzard** and the Iranian-nexus **Crimson Sandstorm**, are confirmed to be using LLMs to generate automated scripts, accelerate attack processes, and generate specialized code designed specifically for detection evasion. This development signifies that the cybersecurity arms race has shifted into a high-speed machine-versus-machine conflict, where defensive success hinges entirely on the adaptive sophistication of defensive AI models.

### C. Operational Challenges in Detection

**Zero-Day Exploits**

The constant exploitation of unknown vulnerabilities before vendor patches exist (zero-day exploits) remains a critical entry point for high-profile attacks. The frequency of zero-day weaponization is accelerating, with threat actors using these flaws not just for initial access but also for privilege escalation and lateral movement.

**False Positives and Alert Fatigue**

As EDR and XDR systems ingest vast volumes of telemetry, traditional rule-based monitoring systems generate an overwhelming number of false positives. This noise leads to "alert fatigue," significantly slowing down security team response times and increasing the risk that genuine, high-priority threats will be missed. This inaccuracy carries a tangible financial toll; organizations are estimated to spend **$1.3 million per year** recovering from the costs associated with poor

  

security intelligence generated by false positives/negatives.

### D. Countermeasures for Advanced Evasion

Defense against these advanced evasive techniques requires a multi-layered, adaptive strategy.

- **Adaptive Behavioral Analysis:** Defense against polymorphic malware necessitates sophisticated behavioral analysis tools leveraging Machine Learning (ML) and heuristics to identify malicious intent and patterns, rather than relying on static file characteristics.
- **Hybrid AI Implementation:** To combat alert fatigue and improve efficiency, organizations are adopting Hybrid AI systems, which merge ML-driven anomaly detection with continuous human analysis and refinement. This blended approach has successfully reduced the volume of false positives by over 70% in certain deployments, allowing analysts to focus on genuine threats.
- **Zero-Trust and Resiliency:** Given the difficulty of achieving perfect detection, particularly against LotL and AI-mutating threats, defenses must prioritize resilience. The adoption of **Zero-Trust Architecture (ZTA)** and least-privilege principles limits the blast radius of a successful intrusion by severely restricting lateral movement and access to sensitive data.

Table 2 details the interaction between modern evasion techniques and their targeted countermeasures.

Table 2: Contemporary Malware Evasion Techniques and Defense Strategies

| Evasion Technique | Mechanism of Evasion | Impact | Primary Anti-Malware Countermeasure |
|---|---|---|---|
| **AI-Driven Polymorphism** | Generative AI dynamically mutates code structure in real-time | Defeats static signatures and increases the scale of unique variants | Advanced Deep Behavioral Analysis and Semantic Feature Extraction |
| **Living Off The Land (LotL)** | Use of native system binaries (e.g., PowerShell, wmic) for malicious actions | Blends in with legitimate system activity, evades EDR alerting on foreign executables | EDR/XDR Process Chain Analysis and Command-Line Argument Monitoring |
| **Memory-Resident Payloads** | Malicious code resides exclusively in volatile RAM | Bypasses traditional disk-based file scanners and AV | Automated Memory Forensics (RAM acquisition) and Moving Target Defense (AMTD) |
| **Sandbox Evasion** | etecting rtualized vironments or laying ecution using nctions like ep() | Causes sandboxes to prematurely conclude the file is benign | Full-system emulation, dynamic timing checks, and hardware-level hypervisors |

## VI. Future Directions

The next generation of anti-malware defense will be defined by resilience, collaboration, and pre-

  

emptive technological shifts to counter emerging computational threats.

### A. Federated Threat Intelligence (FL)

The increasing volume and complexity of threats demand global collaboration, yet legal and privacy concerns often preclude the centralization of sensitive, raw threat data. Federated Learning (FL) offers a solution by enabling collaborative malware detection across multiple disparate entities, such as Cloud Service Providers. Under FL, models are trained locally on proprietary data, and only the aggregated model parameters (weights) are shared with a central server. This approach preserves the privacy and confidentiality of the raw local threat data while benefiting from the collective global intelligence, improving adaptability against obfuscation techniques. FL thus represents the extension of the Zero Trust philosophy into the domain of collaborative threat intelligence sharing.

### B. Explainable AI (XAI) in Cybersecurity

As Deep Learning models used in malware detection become increasingly complex and opaque "black boxes," Explainable AI (XAI) has gained prominence. XAI is crucial for enhancing the transparency and trustworthiness of automated detection systems. Given the real-world performance discrepancies of ML models and the prevalence of alert fatigue, human analysts often distrust opaque AI decisions.

XAI techniques provide the necessary insights, allowing security analysts to comprehend *why* a specific file was flagged, which input features were influential in the decision, and the system's confidence level. This crucial analytical benefit transforms the AI from a cryptic oracle into a trustworthy assistant, maximizing the efficiency gains of AI while ensuring effective oversight. Future work focuses on integrating these explainable models directly into broader security ecosystems, including SIEM systems and incident response platforms.

### C. Blockchain for Integrity Verification

The immutable, decentralized, and transparent characteristics of blockchain technology are being adapted to cybersecurity to guarantee integrity and combat supply chain manipulation. Blockchain provides a secure ledger for storing cryptographic hashes of digital evidence, software components, and audit logs.

By storing hashes of critical software states on the blockchain, organizations can verify software authenticity and ensure that code has not been tampered with since its official creation, thereby mitigating supply chain risks (like the XZ Utils incident). This guarantees data integrity without requiring the raw, sensitive evidence to be stored in the decentralized ledger.

### D. Quantum-Resistant Malware Defense (PQC)

Looking ahead, the emergence of Cryptographically Relevant Quantum Computers (CRQCs) presents an existential threat to current data security infrastructure. Quantum computers utilizing algorithms like Shor's could quickly factorize large integers, rendering widely used asymmetric encryption methods (e.g., RSA, ECC) obsolete. This compromise threatens long-term data confidentiality and secure communications globally.

Furthermore, adversaries with access to quantum technology could leverage it to create significantly more sophisticated and stealthy malware, accelerating the discovery of zero-day vulnerabilities. To mitigate this imminent risk, the cybersecurity community must transition to **Post-Quantum Cryptography (PQC)**. PQC involves developing new, math-based public-key cryptographic algorithms derived from problems deemed difficult for both classical and future quantum computers, ensuring the long-term integrity and confidentiality of data against advanced threats.

## VII. Conclusion

Malware remains a continuously evolving threat, transitioning from simple file infection to an

  

industrialized, financially driven, and nation-state-supported digital war. The evidence suggests that traditional, reactive, signature-based approaches are functionally obsolete against modern evasion techniques, such as AI-driven polymorphism, Living Off the Land attacks, and zero-day exploitation.

The defense architecture has responded by migrating from siloed Endpoint Detection and Response (EDR) to holistic, integrated Extended Detection and Response (XDR) systems. This shift is a necessary move toward unified threat context and automated, cross-domain response capabilities, designed specifically to reduce the rising median dwell time of attackers.

The future of anti-malware defense lies in adaptive, preemptive, and collaborative technologies. This includes investing heavily in defensive AI models capable of combating AI-generated polymorphism; adopting Federated Learning frameworks for global, privacy-preserving threat intelligence sharing; securing critical infrastructure through immutable, blockchain-verified integrity controls; and initiating the essential migration to Post-Quantum Cryptography to safeguard data from future quantum-enabled threats. The ongoing resilience of the digital ecosystem depends on proactively anticipating threats rather than merely reacting to them.

## VIII. References (Recent, 2022–2025)

[1]:https://arxiv.org/pdf/2407.19153?utm_source=chatgpt.com "A Survey of Malware Detection Using Deep Learning"
[2]:https://www.sciencedirect.com/science/article/pii/S2666827024000227?utm_source=chatgpt.com "A survey of malware detection using deep learning"
[3]:https://pubs.aip.org/aip/acp/article/3217/1/020017/3327704/A-comprehensive-survey-on-robust-Malware-detection?utm_source=chatgpt.com "A comprehensive survey on robust Malware detection ..."
[4]:https://www.computer.org/csdl/journal/tq/2024/05/10430405/1UoCpDhfSBW?utm_source=chatgpt.com "A New Defense Method Against Crypto Ransomware"
[5]:https://www.researchgate.net/publication/385958493_Enhancing_Malware_Detection_Through_Convolutional_Neural_Networks_and_Explainable_AI?utm_source=chatgpt.com "Enhancing Malware Detection Through Convolutional ..."
[6]:https://dl.acm.org/doi/abs/10.1109/TIFS.2024.3433372?utm_source=chatgpt.com "Enhancing Malware Classification via Self-Similarity ..."
[7]:https://www.mdpi.com/1424-8220/25/4/1153?utm_source=chatgpt.com "A Survey on ML Techniques for Multi-Platform Malware ..."
[8]:https://www.mdpi.com/2076-3417/15/14/7747?utm_source=chatgpt.com "Systematic Review: Malware Detection and Classification ..."
[9]:https://arxiv.org/abs/2303.16004?utm_source=chatgpt.com "A Survey on Malware Detection with Graph Representation Learning"
[10]:https://arxiv.org/abs/2312.09636?utm_source=chatgpt.com "A Malware Classification Survey on Adversarial Attacks and Defences"
[11]:https://www.researchgate.net/publication/367763690_A_comprehensive_survey_on_deep_learning_based_malware_detection_techniques?utm_source=chatgpt.com "A comprehensive survey on deep learning based malware ..."
[12]:https://dl.acm.org/doi/10.1145/3732365.3732410?utm_source=chatgpt.com "A Survey of Machine Learning Approaches for Malware ..."

  