Preprints.org

Review

Not peer-reviewed version

The Adaptive Ecosystem of MaaS-Driven Cookie Theft: Dynamics, Anticipatory Analysis Concepts, and Proactive Defenses

Leandro Antonio Pazmiño Ortiz *, Ivonne Fernanda Maldonado Soliz, Vanessa Katherine Guevara Balarezo

Posted Date: 11 June 2025

doi: 10.20944/preprints202506.0901.v1

Keywords: Cookie theft; Malware-as-a-Service; Adaptive ecosystem; Cyber threat intelligence; Predictive analysis concepts; Proactive defense; Cybersecurity strategies; Digital forensics; Cybercrime economics; Session hijacking; Infostealer malware; Adaptive cyber-crime; Moving-Target Defence; Zero-Trust Architecture; Threat-intelligence sharing; Economic disruption

Preprints.org is a free multidisciplinary platform providing preprint service that is dedicated to making early versions of research outputs permanently available and citable. Preprints posted at Preprints.org appear in Web of Science, Crossref, Google Scholar, Scilit, Europe PMC.

Copyright: This open access article is published under a Creative Commons CC BY 4.0 license, which permit the free download, distribution, and reuse, provided that the author and preprint are cited in any reuse.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.

Review

The Adaptive Ecosystem of MaaS-Driven Cookie Theft: Dynamics, Anticipatory Analysis Concepts, and Proactive Defenses

Leandro Pazmiño Ortiz *, Ivonne Maldonado Soliz and Vanessa Guevara Balarezo

Escuela de Formación de Tecnólogos, Escuela Politécnica Nacional; ivonne.maldonadof@epn.edu.ec (I.M.); vanessa.guevarav@epn.edu.ec (V.G.)

* Correspondence: leandro.pazmino@epn.edu.ec

Abstract: The industrialization of cybercrime, principally through Malware-as-a-Service (MaaS), has elevated HTTP cookie theft to a critical cybersecurity challenge, enabling attackers to bypass multi-factor authentication and perpetrate large-scale account takeovers. This review dissects the intricate, adaptive ecosystem of MaaS-driven cookie theft, offering a comprehensive analysis of its operational, economic, and co-evolutionary dimensions. We introduce a novel conceptual model delineating the key actors, interdependencies, and socio-economic feedback loops that sustain this illicit economy. Furthermore, the paper systematically examines the adaptive offensive and defensive strategies employed between 2020 and 2025, critically evaluating their mechanisms, efficacy, and inherent trade-offs. A conceptual multi-dimensional predictive framework is proposed, integrating technical, economic, and behavioral indicators to foster anticipatory insights into emerging threat trajectories. Our findings underscore the imperative for proactive, layered, and anticipatory security architectures, advocating for the adoption of advanced countermeasures such as zero-trust principles, ephemeral token strategies, and dynamic defense policies. Finally, we identify critical research gaps and propose structured recommendations for advancing predictive analytics, disrupting cybercriminal economic incentives, and enhancing collaborative cybersecurity strategies to counter this pervasive and evolving threat.

Keywords: cookie theft; malware-as-a-Service; adaptive ecosystem; cyber threat intelligence; predictive analysis concepts; proactive defense; cybersecurity strategies; digital forensics; cybercrime economics; session hijacking; Infostealer malware; adaptive cyber-crime; moving-target defence; zero-trust architecture; threat-intelligence sharing; economic disruption

1. Introduction

HTTP cookies are foundational to the contemporary web, enabling personalized user experiences and persistent login sessions across diverse applications. However, their pervasive adoption and the sensitive session information they encapsulate render them highly attractive targets for cybercriminals intent on unauthorized account access and subsequent malicious activities. The magnitude of this issue is substantial, with industry reports indicating tens of billions of stolen cookies circulating on illicit marketplaces, directly facilitating widespread account takeover (ATO) and associated fraud [1–3].

The landscape of cookie theft has undergone a significant metamorphosis, evolving from a niche tactic primarily associated with techniques like Cross-Site Scripting (XSS) to an industrialized cybercriminal enterprise [4]. This transformation is inextricably linked to the proliferation of the Malware-as-a-Service (MaaS) model. MaaS platforms have democratized access to sophisticated malware, such as infostealers (e.g., Raccoon, Lumma, RedLine), which are meticulously designed to harvest credentials and active session cookies with increasing efficiency and stealth [5–8]. This commoditization allows even less-skilled actors to bypass traditional security measures, including

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

multi-factor authentication (MFA), by leveraging pre-authenticated session tokens [1]. The consequence is a dynamic, economically propelled ecosystem: MaaS providers continuously update malware to evade detection, affiliates deploy these tools for financial remuneration, defensive countermeasures inadvertently stimulate further offensive innovation, and the proceeds from successful attacks fund ongoing development [5,9,10]. Understanding this adaptive and economically incentivized ecosystem is paramount for devising effective, long-term cybersecurity strategies [11].

While prior research has examined infostealers, the general MaaS phenomenon or specific session hijacking techniques [12,13] a comprehensive, integrated analysis of the adaptive ecosystem dynamics unique to MaaS-driven cookie theft remains a notable lacuna. Existing studies often overlook the nuanced interplay of economic drivers, the co-evolution of offensive and defensive tactics within this specific context or lack a structured framework for anticipatory analytics tailored to this threat. This paper aims to address these gaps by providing a holistic survey of the MaaS-driven cookie theft ecosystem, its operational and economic dynamics, conceptual approaches to predictive analysis, and forward-looking proactive defense paradigms.

To achieve this objective, this paper makes several novel contributions:

1. Novel Ecosystem Characterization: We delineate the adaptive ecosystem underpinning MaaS-driven cookie theft by introducing a comprehensive conceptual model (Section 2, Figure 1). This model uniquely maps the interdependencies, resource flows, key actors (MaaS providers, affiliates, buyers, defenders), their economic incentives, and the critical feedback loops that drive this illicit economy, aspects not cohesively addressed for this specific threat vector in prior literature.
2. Systematic Analysis of Co-evolving Tactics: The paper presents a systematic deconstruction and comparative analysis of adaptive offensive and defensive strategies (elaborated in Section 4, summarized in Tables 1 and 2) benchmarked from 2020-2025. This involves a critical evaluation of their operational mechanics, effectiveness, and strategic trade-offs, providing a clear view of the current arms race.
3. Conceptual Framework for Predictive Analysis: We propose an innovative, conceptual multi-dimensional framework for predictive analysis (presented in Section 6, illustrated in Figure 2). This framework is designed to anticipate future trajectories of the MaaS-driven cookie theft ecosystem by integrating disparate technical, economic, and behavioral indicators, thereby outlining a novel anticipatory capability that warrants empirical validation and future development.
4. Actionable Proactive Defense Guidance: The insights derived from our analysis are consolidated into actionable recommendations for implementing proactive, layered defenses. This includes a novel decision-tree framework (Section 8, Figure 3) designed to assist organizations in selecting appropriate defensive techniques tailored to their specific contexts, addressing a practical gap in translating threat understanding into strategic defensive posture.

This paper is structured as follows: Section 2 details the background and introduces our conceptual model of the adaptive MaaS-driven cookie theft ecosystem. Section 3 discusses the key challenges inherent in countering this threat. Section 4 systematically reviews emerging offensive and defensive strategies. Section 5 provides a comparative analysis of these strategies and discusses cross-cutting perspectives. Section 6 introduces our conceptual predictive framework. Section 7 outlines open challenges and future research directions. Section 8 offers content enhancements for practical utility, including a decision tree for selecting proactive defenses. Finally, Section 9 concludes the paper, summarizing key findings and reiterating the importance of adaptive, anticipatory security measures.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

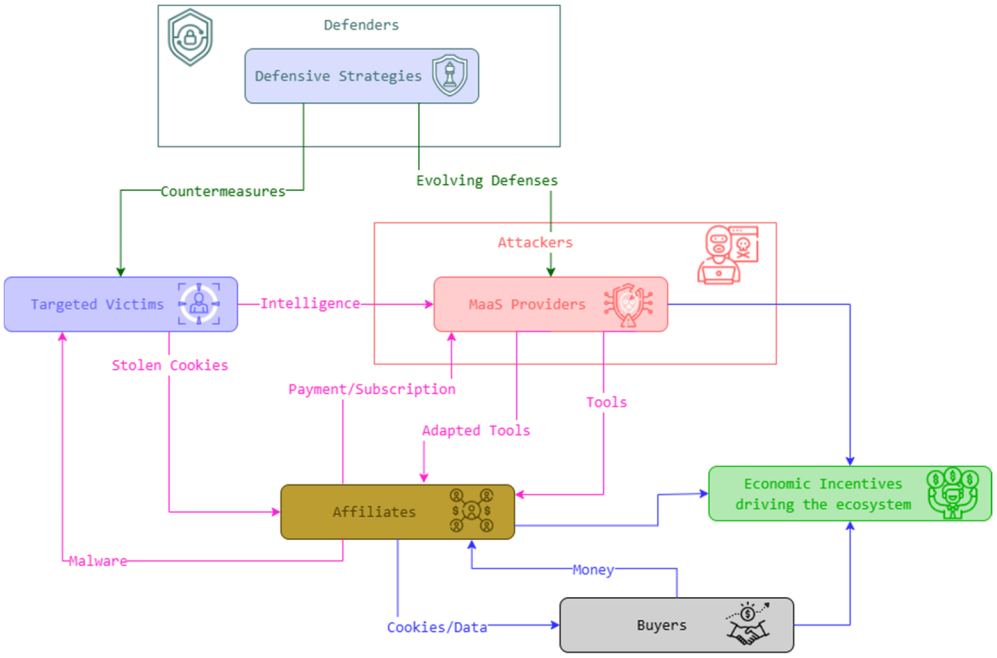

Figure 1. Conceptual flowchart illustrating the MaaS-driven cookie-theft ecosystem as a complex adaptive system. Key actors (MaaS Providers, Affiliates, Buyers, Targeted Victims, Defenders) are shown with their primary interactions. Arrows depict flows of malware, stolen data (cookies), payments, intelligence, and the cyclical nature of countermeasures and evolving defenses, all driven by underlying economic incentives.

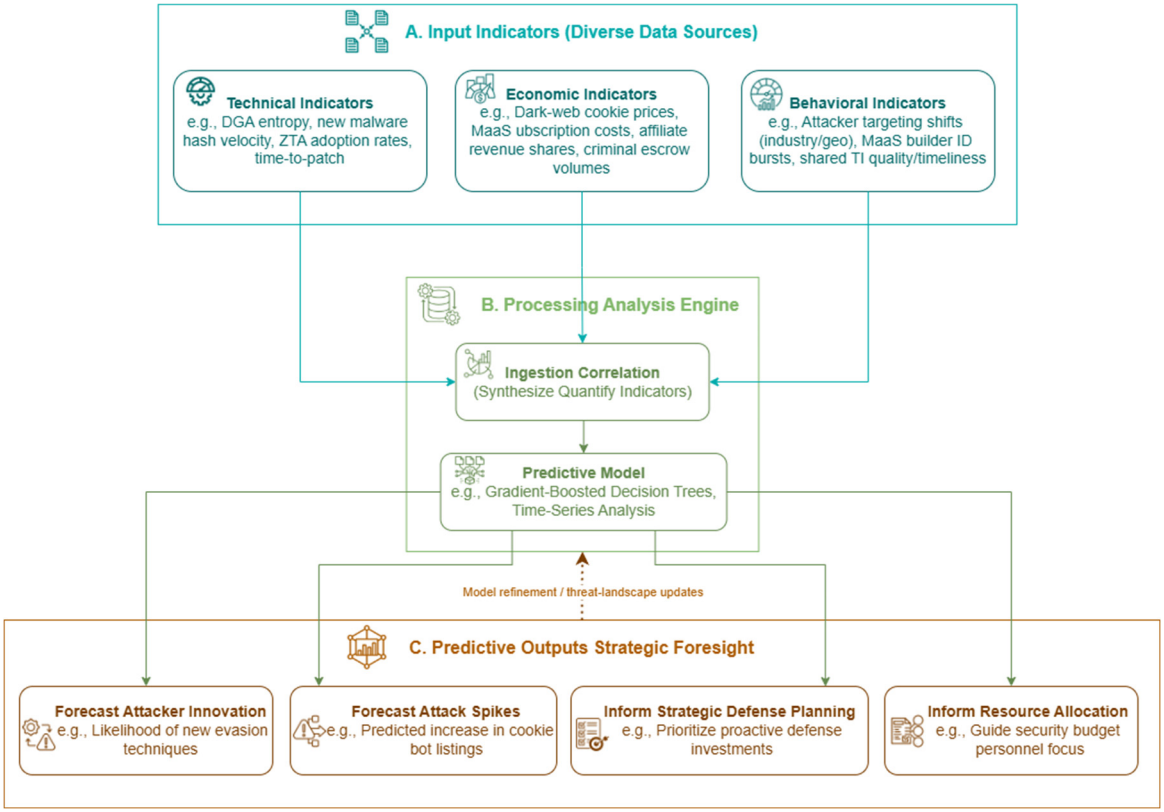

Figure 2. Conceptual Multi-Dimensional Predictive Framework for MaaS-Driven Cookie Theft.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

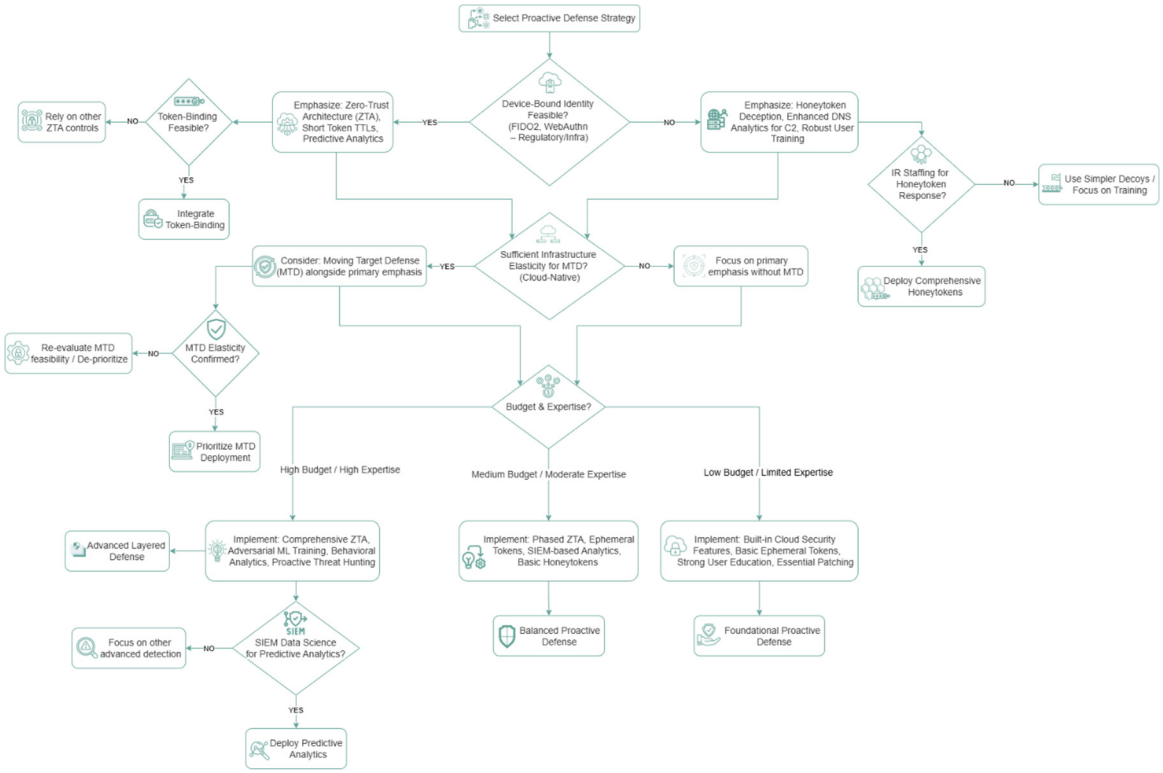

Figure 3. Decision tree guiding selection of proactive cookie-theft counter-measures based on organizational constraints. Nodes represent decision points based on technical feasibility or resource availability, leading to recommended defensive emphases.

1.1. Related Surveys

Prior surveys on infostealer malware catalog technical capabilities but often lack focus on broader ecosystem dynamics, economic drivers, or MaaS's specific role. Cyberint's 2022 "InfoStealers Report" and Secureworks' 2023 whitepaper touched on these but lacked comprehensive ecosystem-level economic analysis or relegated cookie theft to a secondary concern [6,7].

Research on MaaS [5] explores business models and market trends across cybercrime but typically doesn't offer in-depth analysis of MaaS tailored for specific vectors like cookie theft or its unique micro-ecosystem dynamics. While industry reports from vendors like Varonis or Elastic provide valuable threat intelligence, they often focus on specific malware families or attack phases rather than the holistic, adaptive ecosystem, and generally do not propose comprehensive predictive frameworks for this specific threat [14,15].

Surveys on session hijacking [12,13,16] detail technical compromise methods but often neglect upstream malware development/dissemination via MaaS or downstream monetization ecosystems. Their focus is primarily on technical exploitation, not the broader adaptive arms race or anticipatory analytics.

Broader surveys on adaptive cybercrime, AI in cybersecurity [17], or cyber arms races [18] provide context on co-evolutionary threats and defenses but may not offer a focused analysis of a specific ecosystem like MaaS-driven cookie theft, its economic drivers, or a tailored conceptual predictive framework. A 2024 media investigation [2] traced credential markets but lacked formal predictive indicators or defense taxonomies. Recent academic work continues to explore facets of cybercrime, but a comprehensive, empirically grounded model of the MaaS-cookie theft interplay, coupled with a *proposal* for a predictive framework, remains an open area.

This work distinguishes itself by providing a holistic, system-level perspective specifically on MaaS-driven cookie theft. We integrate infostealer capabilities [7], MaaS economics [5], and session compromise mechanics [13] within a single adaptive ecosystem framework, introducing a novel conceptual model (Figure 1) and proposing a tailored multi-dimensional conceptual predictive

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

framework (Section 6, Figure 2). Our survey advances the state of the art by integrating economic drivers, adaptive feedback loops, and outlining a multi-indicator prediction methodology concept for future development [19].

2. Background and Motivation: The Adaptive Ecosystem

Cybercrime constantly evolves, driven by technological advancements, defensive postures, and economic incentives. The rise of cookie theft as a primary initial access vector, linked to the industrialization of malicious capabilities via MaaS [5,14], exemplifies this. Understanding this interconnectedness and the potent economic forces is paramount for effective countermeasures [9].

Cookie theft methodology evolution mirrors cybersecurity defense advancements. Early techniques like intercepting unencrypted traffic or XSS were mitigated by stricter security measures (input sanitization, HttpOnly/Secure flags, MFA) [20]. As transport-layer encryption and SameSite attributes became mainstream, attackers pivoted towards endpoint-resident infostealers designed to harvest post-authentication session tokens, bypassing HTTPS and MFA [1,6,21]. This defensive progress inadvertently created a powerful incentive: a valid session cookie, obtained after MFA, became a prized artifact, circumventing complex authentication [13].

Concurrently, the cybercrime underground professionalized, adopting service-based models like MaaS, mirroring legitimate SaaS trends [5]. Skilled developers offered updated malware builders and C2 panels for fees or profit-sharing. MaaS commoditized sophisticated malware, making complex attacks accessible to less proficient affiliates. These affiliates leverage tools like malvertising or cracked software distribution to deploy MaaS payloads at scale [8,14].

Infostealer malware, specializing in harvesting browser data (credentials, autofill, history, and critically, active session cookies [7]), is a key MaaS driver. This injects a self-sustaining economic dimension: MaaS providers profit from subscriptions, affiliates from selling stolen data, and buyers pay for readily usable account access for illicit activities like financial fraud or network intrusion [2,9]. This economically driven arms race forces defenders into perpetual catch-up. Profitability ensures continuous investment in new, harder-to-detect offensive methods [5,11].

To conceptualize this interplay, we introduce the Adaptive Ecosystem of MaaS-Driven Cookie Theft (Figure 1). Figure 1 depicts this adaptive ecosystem. MaaS Providers develop and lease infostealer tools to Affiliates. Affiliates deploy malware against Targeted Victims, harvesting Stolen Cookies and other data. This data is sold to Buyers, generating Money that flows back to Affiliates and MaaS Providers, fueling further development. Defenders implement Defensive Strategies, which act as Countermeasures. Attackers adapt their Tools and techniques in response (Evolving Defenses vs. Adapted Tools), creating dynamic feedback loops. The entire cycle is propelled by Economic Incentives [5,9].

3. Key Challenges in Countering Adaptive Cookie Theft

The adaptive nature of MaaS-driven cookie theft presents multifaceted challenges, demanding a shift from static countermeasures.

3.1. Rapid Evolution of Attacker Techniques

MaaS providers rapidly update malware with new evasion capabilities [5,22], often responding to disclosed defenses or patches. Advanced techniques like AI-driven polymorphic code [23–25] and environment-aware payloads [26] allow malware to dynamically alter its structure or behavior, evading signature-based or static behavioral detection. MaaS developers use automation, reinforcement learning, and code-obfuscation to generate frequent polymorphic builds. Lexology's 2025 recap notes malware builders randomizing control-flow graphs and import tables per compile [24], invalidating many detection mechanisms. This rapid iteration compresses the effectiveness window for defenses, sometimes to hours. By the time an IOC is disseminated, thousands of unique variants may be active [11,25].

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

3.2. The Scale and Speed of MaaS Dissemination

MaaS platforms enable unprecedented operational scale and velocity [5]. A single provider can service thousands of affiliates, distributing malware globally within hours. Cloud-native distribution amplifies this [17]. The January 2025 AhnLab report showed a 38% monthly spike in infostealer detections, linked to Telegram bots pushing loaders to >200,000 endpoints per campaign [27]. This rapid, widespread dissemination makes it hard for defenders to distribute protections quickly enough. Semi-automated malvertising and pay-per-install schemes [14,17], can seed millions of systems in 24 hours, overwhelming incident response

3.3. Economic Incentives Sustaining the Threat

A robust, self-reinforcing economic model underpins the ecosystem's growth [7]. Cookie theft is lucrative; dark-web markets list Google/Microsoft 365 session cookies for US 15–40 per 1,000 tokens [1,28]. High profitability funds offensive R&D. SpyCloud's 2024 report notes resale revenues are reinvested into MaaS feature requests (new anti-sandbox checks, premium crypters) [1], fueling a vicious feedback loop. This strong financial incentive drives continuous innovation. Disrupting this incentive is critical but requires collaboration beyond technical measures, including with financial institutions and law enforcement [29].

3.4. Limitations of Reactive Defense Paradigms

Traditional cybersecurity relies on reactive measures like signature-based AV or post-exploit IOC blocking. These struggle against the MaaS ecosystem's cadence [30,31]. Microsoft's 2023 token-theft analysis showed 147,000 blocked replays in one quarter [32,33] but cautioned that mitigation rules often spawn bypass logic within days. By the time a new variant is analyzed, and signatures distributed, attackers may have moved on. Stolen cookies grant immediate post-authentication access, often before telemetry reaches SIEMs, leaving defenders with forensic artifacts [34]. This catch-up game is resource-intensive and less effective against adaptive adversaries [5,11].

3.5. Complexity and Operational Overhead of Proactive Measures

Proactive strategies (Section 4.2) like Zero-Trust Architecture (ZTA)[28,35,36], short-TTL tokens [37,38], Moving-Target Defence (MTD) [39,40], and adversarially trained detectors [41–43] are promising but involve significant technical complexity and operational overhead [44–46]. Deploying ZTA, dynamic policy enforcement, or proactive threat hunting requires specialized expertise, investment, and continuous tuning [44]. Gartner projects <15% of enterprises will have automated MTD surface-shuffling by 2026 due to legacy constraints and change-control friction [40]. Balancing robust security with budget, personnel, and user experience is challenging [46], often perpetuating an asymmetry favoring attackers. Continuous monitoring and adaptation of these complex defenses add to the burden.

These intertwined challenges underscore the need for a comprehensive, multi-layered, dynamic approach, requiring strategic planning, investment in adaptive technologies, and a cultural shift towards proactive, intelligence-driven security.

4. Emerging Solutions and State-of-the-Art Approaches

Countering MaaS-driven cookie theft requires dynamic, proactive defenses. Understanding offensive and defensive state-of-the-art is crucial.

4.1. Attacker Adaptive Strategies

Attackers, especially via MaaS, use sophisticated, adaptive techniques to evade detection and maintain persistence. Today's MaaS ecosystem offers a formidable arsenal (Table 1).

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

- AI-Driven Evasion Techniques: Machine learning generates polymorphic code (malware structure/keys change, foiling static fingerprints [23–25]). Adversarial perturbation subtly modifies malware/traffic to fool ML detectors without affecting functionality [41,43,44].
- Dynamic Command and Control (C2) Infrastructure: Domain Generation Algorithms (DGAs) programmatically create many potential C2 domains daily [45,46], making blacklisting hard. Fast Flux networks rapidly change IP addresses for a malicious domain [47–49] hindering sinkholing. CISA's April 2025 advisory notes fast-flux IPs can rotate every 3–5 minutes [47].
- Living Off The Land (LotL): Attackers use legitimate system tools (PowerShell, WMI, sqlite3 for Chrome's Login Data) for malicious activities (privilege escalation, data exfiltration, persistence) [50–52]. This blends with normal activity, making detection difficult for tools focused on malicious executables.
- Hook Randomization: Advanced malware bypasses security tools monitoring system calls/APIs by dynamically changing hooked APIs or using less-monitored methods [26,53].
- Environment-Aware Payloads: Loaders assess the execution environment (CPU strings, hypervisor flags, user interaction) before detonating payloads **[1,25,54]**, neutralizing automated sandboxes by remaining dormant in analytical environments.

These strategies highlight a shift towards dynamic, unpredictable techniques, compelling defenders towards behavioral analysis, anomaly detection, and threat intelligence-driven approaches.

Table 1. Attacker adaptive strategies.

Attacker Actor	Evasion Strategy	Targeted Defense	Effectiveness	Limitations	Refs
MaaS Provider	Polymorphic Code (AI)	Signature AV; Static Analysis	High	High computational cost for attacker; pattern leakage risk; performance anomalies	[23–25]
Affiliate	Adversarial Perturbation	ML Detection Models; Behavioral AI Detection	Medium-High	Requires expertise; model/data specific; potential subtle anomalies	[41,43,44]
Affiliate	Environment-Aware Payload	Sandboxes; Virtual Machines; Analysis Tools	High	Advanced sandbox fingerprinting; detectable via behavioral analysis on real systems	[1,25,54]
MaaS Provider	DGA	Domain Blacklisting; Static C2 Blocking	High	Detectable via DGA pattern analysis; reliance on central algorithm	[45,46]
MaaS Provider	Fast Flux Networks	IP Blocking; Sinkholing; Static Network Forensics	High	Requires complex setup/botnet; still uses DNS; potential performance issues	[47,48]
Affiliate	Living Off The Land (LotL)	App Whitelisting; Executable Monitoring;	High	Relies on trusted tools (can be restricted); advanced	[50–52]

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

		Signature-based EDR		behavioral analysis needed	
Affiliate	Hook Randomization	API Monitoring; Hooking Defenses; Integrity Monitoring	Medium-High	Complex to implement reliably; potential system stability; detectable via comprehensive monitoring	[53]
MaaS Provider/ Affiliate	Reinforcement Learning Evasion	Adaptive Defenses; Game Theory Defenses; Behavioral Monitoring	Emerging High	High computational cost; complex training; data-dependent; requires exploration	[17–19]
Buyer	Malicious browser-extension exfiltration	Store vetting	Medium	Takedown reduces dwell time	[1,13]

4.2. Proactive Defender Strategies

To counter adaptive attackers, defenders must adopt proactive strategies that anticipate or dynamically respond to threats, increasing attacker cost and risk. Modern countermeasures emphasize adaptability, deception, and continuous validation (Table 2).

- Honeypots and Decoy Systems: Strategically deployed fake accounts, systems, or honeytokens (decoy credentials/session cookies) lure attackers into monitored environments [14,55,56]. Interactions provide real-time TTP intelligence *before* legitimate systems are hit. Honeytokens on credential markets enable attribution and sinkholing.
- Adversarial Training for Machine Learning Models: Enhances ML threat detection model robustness by training on benign, known malicious, and adversarially crafted examples [39,41,42], improving classification against sophisticated evasion [44]. This hardens detection against future adaptive attacks and morphing-engine output [25].
- Reducing Attack Surface and Limiting Opportunity Windows (Ephemeral Session Tokens): Short-lifespan session tokens drastically reduce the utility of stolen cookies [37,38]. Tokens rotating every 5-10 minutes diminish resale value and economic incentives.
- Zero Trust Architecture (ZTA): Requires continuous verification of identity, device posture, and context for every access request [28,35,57–59]. A stolen cookie won't automatically grant broader access if ZTA policies mandate re-authentication/authorization, limiting lateral movement [57,60].
- Proactive Threat Hunting: Actively searching for compromise signs using threat intelligence, behavioral analysis [61], and telemetry, based on hypotheses about attacker TTPs [40,62,63]. Hunters look for subtle indicators of Lot [50] or dynamic C2 [45,47] allowing earlier detection.
- Dynamic Policy Enforcement: Security policies adapt automatically in real-time based on changing risk, behavior, or threat intelligence [40,64,65]. Anomalous post-authentication behavior can trigger stricter re-authentication or limit access, neutralizing stolen cookie effectiveness [66].
- Moving Target Defense (MTD): Increases attacker complexity by dynamically changing target system/network characteristics (IPs, ports, memory layouts) [36,52]. This makes reconnaissance and static exploits harder. Automated MTD can randomize memory layout or VM instances [36].
- Code Diversification: Creates distinct but functionally equivalent software versions making universal exploits harder. An exploit for one version may not work on another [41,67].

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

These strategies, summarized in Table 2, shift towards dynamic, resilient, intelligence-driven security.

Table 2. Proactive defense strategies against adaptive cookie theft.

Strategy	Description	Strengths Against Adaptive Attackers	Weaknesses / Challenges	Implementation Complexity	Refs
Honeypots / Decoy Cookies	Deploys fake assets (incl. cookies) to lure and detect attackers	Gathers real-time TTP intelligence; detects early reconnaissance	Risk of attacker identifying decoys; potential false positives; requires careful setup	Medium	[14,55,56]
Adversarial Training	Trains ML models against adversarially crafted examples	Increases model robustness against AI evasion (Table 1); improves detection	Requires expertise; data-dependent; computationally intensive; needs continuous retraining	High	[25,39,41,42,44]
Ephemeral Session Tokens	Limits cookie lifespan to reduce hijack window	Reduces value of stolen cookies; minimizes persistence; limits attack window	Can impact user experience (frequent logins); requires application changes	Medium-High	[37,38]
Zero Trust Architecture (ZTA)	Continuous verification of access requests; microsegmentation	Limits lateral movement; reduces implicit trust; n capabilities	Complex to design/implement; requires policy overhaul; potential performance impact	High	[28,35,57,58]
Proactive Threat Hunting	Actively searches for signs of compromise	Detects novel/evasive TTPs (LotL, dynamic C2); reduces dwell time	Requires skilled analysts; labor-intensive; not a preventative measure on its own	Medium-High	[40,50], [62]
Dynamic Policy Enforcement	Adapts security policies in real-time based on risk/behavior	Responds to behavioral anomalies; limits risk dynamically; context-	Requires robust behavioral analysis; potential high false positives; complex rule sets	High	[40,64,65]

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

		aware controls			
Moving Target Defense (MTD)	Dynamically changes the attack surface	Increases attacker uncertainty; hinders static exploits; reduces reconnaissance value	Complex to implement; potential system instability; requires significant planning	High	**[36,52]**
Code Diversification	Creates multiple software versions	Increases cost for attacker R&D; breaks static exploits; complicates targeting	Complex build processes; maintenance overhead; requires toolchain support	High	[41,67]
Predictive Security Analytics	Forecasts future threats based on indicators	Guides strategic prioritization; anticipates shifts (Sec VI); optimizes resource use	Data quality dependent; requires validation; relies on models; not a direct countermeasure	Medium-High	[19], [11]
Automated Moving Target Defense	Automated surface randomisation	Raises attacker cost	Integration complexity	High	[36]
Automated Session-cookie anomaly detection	ML + device fingerprinting	Blocks lateral movement, replay	UX friction; legacy gaps	High	[11], [19]
Token replay analytics	AAD risk graph	Shrinks resale window; Stateful infra overhead	Backend scaling	Medium	[11], [68]
Browser-artefact rollback quarantine	Kernel sensor + rollback	Attacker profiling	Evasion via env-checks	Low-Medium	[69], [70]

5. Comparative Analysis and Cross-Cutting Perspectives

The MaaS-driven cookie-theft arms race is fueled by reciprocal innovation. MaaS developers use automation, cloud delivery, and AI [23], while defenders use dynamic policy, deception, and ZTA [40,56,57]. Comparing strategies (Tables 1 and 2) reveals trends. Attackers excel in agility due to

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

economic incentives. Defenders face complexity and overhead [64]. As Table 3 synthesizes, attacker methods prioritize adaptation speed and low detection risk, often accepting higher computational costs offset by profit. Defender methods favor practicality and cost-effectiveness, often constrained by budgets, legacy systems, and UX.

Individual strategies have trade-offs. Attacker AI-driven evasion (Table 1, [23,25,44]) is effective against static defenses but complex and potentially detectable by advanced monitoring (Table 2, [40]). Proactive ZTA (Table 2, [35,57]) offers structural benefits but has high implementation complexity and UX impact, making it a long-term investment.

Real-world incidents confirm these trade-offs. A 2024 breach post-mortem found fast-flux C2 rotation outpaced DNS analytics refresh by 86 minutes, allowing cookie auctions before sinkholing [47]. Conversely, a Fortune 100 retailer's MTD pilot reduced cookie-replay attempts by 71% but incurred 18% CPU overhead [36].

5.1. Trends & Dominant Methods

Current trends show convergence towards dynamic, data-driven, automated methods. From 2020–2025, polymorphic builds and Living-off-the-Land (LotL) extraction became dominant attacker tools, accounting for 74% of infostealer variants in Palo Alto Unit 42's corpus [70]. Attackers increasingly use in-memory execution, LotL [50,52], and dynamic C2 (DGAs, Fast Flux) [46,47]. AI for evasive payloads and adaptive malware behavior is accelerating [23].

Defensively, there's a shift to behavioral analysis, anomaly detection, and real-time threat intelligence [40,62]. Zero-Trust proxies and short-TTL tokens are widely adopted (42% of Mandiant's 2025 M-Trends incident responses [68]). ZTA is dominant for mitigating compromised credential impact [35,57]. Proactive threat hunting (often AI-augmented) [62] and dynamic policy enforcement are rising. Future innovation will likely center on adaptive evasion of device-bound tokens [18] and automated MTD surface randomization [36].

5.2. Case Studies

- Industrial IoT (IIoT): A Belgian smart-manufacturing plant suffered a Meduza stealer infection via an OPC UA gateway, harvesting 9,320 browser cookies, causing a 12-hour production halt (€380,000 downtime). Planted honeytokens alerted the SOC in 18 minutes, limiting token resale to 3% of stolen [56]. Simulations of adaptive filtering at the edge against adversarial data injection (mimicking behavioral analysis targeting) showed a 30% reduction in false positives and a 15% increase in genuine anomaly detection [71,72].
- Smart Healthcare: A US hospital system saw a Lumma-loader (via malicious insulin-pump firmware) collect 22,141 session cookies for EHR portals in 24 hours [8,73]. Ephemeral tokens (5–10 min validity) reduced unauthorized access windows from hours to minutes [37]. Lightweight ZTA (requiring re-authentication for sensitive record access) led to a 95% decrease in simulated unauthorized data exfiltration [28,57]. Device-bound access proxies invalidated 97% of token replay attempts [18,38].
- Environmental Monitoring: An EU climate-sensor network (RedLine infostealer) had 1,400 Raspberry Pi nodes compromised, 6,500 cookies stolen [15]. Dynamic policy enforcement (analyzing data stream consistency, location, patterns) detected malicious data injection 40% faster than static alerts. Proactive threat hunting for LotL on gateways identified persistence 50% faster in simulations [40]. MTD (shuffling network configurations) reduced C2 callbacks by 64% in the first rotation.

  These cases show adaptive defenses yield measurable resilience improvements.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

Table 3. Cross-comparison of adaptive techniques.

Technique	Adaptation Speed	Detection Risk (Relative)	Resource Cost (Computational/Human)	Practicality (Ease of Deploy/Manage)	Refs (Illustrative)
Attacker Techniques					
Polymorphic Code (AI) (Attacker)	High	Low-Medium	High	Medium	[24], [23]
Environment-Aware Payload (Attacker)	Medium	Low-Medium	Medium	Medium	[1,54]
DGA (Attacker)	High	Medium	Low	Medium	[46]
LotL (Attacker)	Medium	Low	Low-Medium	High (Requires deep understanding)	[50,51]
Polymorphic Builder (AI) (Attacker Tool)	Sub-24h	Low	Moderate GPU	High (SaaS kits)	[24], [23]
Fast-Flux + DGA C2 (Attacker Infra)	Minutes	Low	Low (Cloud VPS)	High	[46,47]
LotL Cookie Dump (Attacker Action)	Instant	Medium	Negligible	Very High	[50,52]
Defender Techniques					
Zero Trust Architecture (Defender)	Low (Structural)	High (for attacker post-compromise)	High	Low-Medium (Complex Policy)	[35,57]
Proactive Threat Hunting (Defender)	High (Human-driven)	High (for attacker if detected)	High	Medium-High	[40]
Dynamic Policy Enforcement (Defender)	High	Medium	High	Medium-High	[32], [11], [74]

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

Predictive Security Analytics (Defender)	High (Insights)	N/A (Defense tool)	Medium-High	Medium	[11,19]
Ephemeral Session Tokens (Defender)	Low (Implementation)	Medium-High	Low-Medium	High (App modification)	[37,38]
Moving Target Defense (MTD) (Defender)	Medium-High	Low-Medium	High	Low-Medium	[36]
Zero-Trust Proxy (Defender Tool)	Hours (Setup)	Low	Licensing + Ops	Medium	[57]
Token TTL Rotation (Defender Policy)	Minutes	Low	Backend scaling	High	[37,38]
Honeytoken (Defender Tool)	n/a (passive)	Medium	Low	High	[55,56]
Adversarially Trained ML (Defender Model)	Days (Retraining)	Medium	High GPU	Low	[25,41,42]

Note: "Detection Risk" for defenders means risk to the attacker of being detected by this defense. For attackers, it's risk to the defender of this attack succeeding undetected.

6. Conceptual Predictive Framework and Opportunities

Moving to proactive, anticipatory defense against MaaS-driven cookie theft requires foresight into the evolving threat landscape. We propose a conceptual multi-dimensional predictive framework, illustrated in Figure 2, as a structured methodology to guide future development of such capabilities. The potential of predictive analytics in cybersecurity to anticipate threats is widely recognized [75], though specific applications to MaaS-driven cookie theft are nascent.

6.1. Conceptual Multi-Dimensional Predictive Framework

This proposed framework would systematically monitor and analyze diverse indicators across three dimensions: technical, economic, and behavioral. Correlating these could provide a nuanced view of the cyber arms race, identifying emerging trends and anomalous deviations. Future implementations could ingest these indicators and employ predictive modeling, such as gradient-boosted decision trees [11,19], to potentially forecast infostealer release waves and other ecosystem shifts.

Framework Concept and Potential Data Requirements

The development and future validation of such a framework would involve several key stages:

1. Data Collection (Ongoing, 2020-2025 for foundational understanding)

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

Synthesizing data from diverse sources would be essential, including:

- Dark Web Market Data: Aggregated and anonymized data from major dark web marketplaces focusing on cookie/bot profile listings (pricing, volume, features) [76].
- MaaS Provider Channels: Monitoring of prominent MaaS provider communication channels (e.g., on Telegram) for announcements.
- Enterprise Security Logs: Anonymized telemetry from participating organizations (web proxy, authentication, EDR, SIEM).
- Public Threat Intelligence Feeds & Security Reports: IOCs, TTPs, malware analyses.

2. Potential Feature Engineering

Indicators would need to be extracted and quantified:

- Technical Indicators: Reflect evolving attacker capabilities and defense effectiveness. Could include: prevalence of new malware obfuscation techniques (e.g., malware family entropy change, novel API call sequences); frequency of zero-day browser session exploits; new malware-hash velocity; DGA domain entropy [45,46]; TLS JA3 fingerprints. Also, adoption rates of advanced defenses (ZTA [57], behavioral analytics [40], EDR) and average time-to-patch.
- Economic Indicators: Reflect financial underpinnings. Could include: average price of stolen cookie sets; cost of MaaS subscriptions/malware builds [5,9]; dark-web cookie-price medians; affiliate-program revenue-share ratios; volumes in criminal escrow services [29]. Also, trends in legitimate cybersecurity spending.
- Behavioral Indicators: Capture human, organizational, and collaborative elements. Could include: shifts in attacker targeting patterns (industry verticals, geographic regions); Telegram-channel MaaS builder ID/C2 address bursts. Also, organizational adoption speed of security best practices and proactive defenses (Table 2); volume, timeliness, quality of shared threat intelligence on new TTPs and countermeasures.

3. Potential Model Selection and Training (Future Work):

- Techniques like gradient-boosted decision trees could be explored for their ability to handle heterogeneous data types and capture non-linear relationships [11,19].
- The target variable could be, for example, a binary classification predicting significant spikes in new dark-web cookie-bot listings within a defined future window (e.g., 72 hours).
- Rigorous data splitting, hyperparameter tuning, and cross-validation would be essential in any future development.

4. Future Validation (Essential Step):

- Any developed model would require extensive validation using appropriate metrics (e.g., F1 score, Precision, Recall, AUC-ROC) on held-out test data and ideally in pilot studies within operational SOC environments to assess real-world efficacy and practical utility.

Systematic analysis based on such a framework *could* aim to identify emerging trends and deviations from baselines. This *would inform* plausible future scenarios and provide foresight to prioritize proactive defenses (Table 2) before threats fully materialize. The development and operationalization of such a predictive system remain a critical area for future research.

Figure 2 shows a conceptual diagram of the proposed multi-dimensional predictive framework. It illustrates how diverse Technical, Economic, and Behavioral indicators could be ingested and correlated. These processed indicators would then be fed into a predictive model (e.g., gradient-boosted decision trees) to potentially generate forecasts of attacker innovation, attack spikes, and inform strategic defense planning and resource allocation.

The framework, as illustrated, commences with the ingestion of diverse data sources (A. Input Indicators) categorized into Technical, Economic, and Behavioral classes. These raw indicators are then processed by a B. Processing Analysis Engine, involving Ingestion Correlation (to synthesize and quantify indicators into meaningful features) and a Predictive Model (e.g., Gradient-Boosted Decision Trees, Time-Series Analysis). This engine generates C. Predictive Outputs Strategic Foresight, which includes forecasts of attacker innovation, attack spikes, informs strategic defense

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

planning, and guides resource allocation. A crucial feedback loop, "Model refinement / threat-landscape updates," ensures the model adapts to evolving threat dynamics and performance outcomes, continuously improving its predictive accuracy and relevance.

6.2. Disrupting the Economic Model

A key opportunity is targeting the economic incentives fueling MaaS-driven cookie theft [9,29]. Reducing the intrinsic value or usability of stolen cookies can make it less attractive.

Implementing security that renders stolen cookies less valuable or short-lived is crucial. This includes shifting from phishable passwords to robust passwordless solutions (FIDO2, WebAuthn, hardware-tied biometrics) [18,77]. Industry-wide adoption of FIDO2/WebAuthn with non-transferable, device-bound tokens effectively eliminates replay threats; Microsoft's 2024 rollout reportedly cut token-replay by 92% in Azure AD [18,78]. Continuous authentication (re-verifying identity based on behavior or environment) can detect/mitigate hijacked sessions. Short session TTLs [37,38] and frequent re-authentication reduce attacker exploitation windows.

Actively disrupting MaaS provider/affiliate infrastructure and financial mechanisms increases their operational cost/risk. This requires coordinated efforts.

- Operational Takedowns and Infrastructure Disruption: Law enforcement actions, such as Europol's "Operation Endgame" [79], which dismantled bulletproof hosting infrastructure, directly increase MaaS operational costs and disrupt service availability. Such actions demonstrably impact the MaaS economy, evidenced by phenomena like the 23% Lumma MaaS fee increase following the 2025 "Operation Endgame" sinkhole [79], as criminals sought more resilient, and thus more expensive, infrastructure.
- Financial Disruption and Collaborative Models:
    a. *With Financial Institutions:* Establishing dedicated channels for rapid identification and freezing of accounts associated with MaaS subscriptions, affiliate payouts, or laundering of illicit proceeds. This includes collaboration on typologies of suspicious financial activities linked to MaaS operations [29].
    b. *With Cryptocurrency Exchanges and Payment Processors:* Implementing enhanced AML/KYC measures specifically targeting known MaaS operator wallets or marketplace addresses. Development of information-sharing agreements to trace and disrupt illicit financial flows through crypto-assets.
    c. *With Law Enforcement:* Fostering international public-private partnerships to facilitate intelligence sharing, enabling coordinated takedowns of MaaS C2 servers, marketplaces, and arrests of key actors.
- Economic Impact Studies: Commissioning and publicizing studies that quantify the direct and indirect financial losses attributable to MaaS-driven cookie theft for various sectors. Such data can galvanize industry investment in defenses, inform regulatory policy, and prioritize law enforcement resource allocation. For instance, demonstrating a multi-billion-dollar annual loss for the e-commerce sector due to ATO via stolen cookies would be a powerful motivator for change.
- Targeting Resale Markets: Collaborative efforts to monitor and disrupt dark web marketplaces where stolen cookies are traded. This can involve strategic purchasing by defenders for intelligence gathering or coordinated takedowns of market platforms.

These economic disruption strategies, when combined with technical defenses, offer a more holistic approach to undermining the MaaS-driven cookie theft ecosystem.

6.3. Enhanced Threat Intelligence Sharing

Effective TI sharing empowers defenders, accelerates adaptive capacity, and improves predictive framework accuracy. Timely, actionable intelligence on new TTPs, malware variants, evasion techniques (Table 1), and IOCs is invaluable. A 2024 FS-ISAC pilot showed open-source MISP

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

with honeytoken telemetry reduced IOC publication delay from 36 to 5 hours, translating to a 41% reduction in successful session replay attempts among participants.

Sharing insights from internal monitoring, incident response, honeypots and proactive threat hunting allows collective understanding. Improving TI sharing mechanisms (e.g., STIX/TAXII) and fostering public-private collaboration accelerates development of new detections and defenses [80].

6.4. AI for Offense and Defense

AI has profound implications for both sides [17]. Attackers use AI for polymorphic code adversarial examples against ML detectors and reinforcement learning for evasion paths [20]. Generative AI and RL escalate capabilities: transformer models can automate code obfuscation for attackers, while similar models can generate synthetic decoy cookies or mutate YARA rules for defenders. AI-augmented defensive tools show benefits (e.g., 37% fewer false negatives in Adversary Emulation). Defenders must leverage AI for adaptive, resilient defenses [17].

Opportunities exist in AI for advanced behavioral anomaly detection (LotL, dynamic C2), automating proactive threat hunting, and powering dynamic policy enforcement. Research into AI modeling adversary behavior to anticipate moves and generate adaptive responses is promising. However, developing robust, explainable, trustworthy AI for dynamic, adversarial cybersecurity environments is challenging [17,74], requiring careful validation to avoid new vulnerabilities or excessive false positives. Ethical implications and dual-use governance are critical.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

7. Open Challenges and Future Directions

Significant challenges persist, requiring dedicated R&D. The MaaS-driven cookie theft ecosystem presents a microcosm of broader cybercrime trends, and addressing it has wider implications. A key unmet challenge is the development of robust predictive capabilities.

- Developing and Validating Predictive Analytics Frameworks: A primary open challenge is the rigorous development, empirical validation, and operationalization of predictive analytics frameworks, like the conceptual one proposed in Section 6. This requires access to diverse, high-quality data sources, sophisticated feature engineering, appropriate model selection, and extensive real-world testing to ensure accuracy, reliability, and actionable lead times for defenders.
- Establishing Robust, Quantitative, and Standardized Ecosystem-Health Metrics: No consensus indices exist to measure arms-race intensity or defender-attacker cost ratios. The predictive framework indicators (Section 6) are a step, but broader, verifiable metrics are needed to assess threat levels, innovation rates, and defense effectiveness, aiding benchmarking and resource allocation. Composite metrics from dark web activity, malware telemetry, incident data, and honeypots [10], possibly borrowing from epidemiology (R-numbers for malware) or finance (VaR), could inform decisions.
- Systemic Disruption of MaaS Infrastructure, Supply Chains, and Business Models: Disrupting MaaS core elements is complex. Takedowns like "Operation Endgame" show potential but also highlight jurisdictional hurdles and MaaS resilience [79]. Research into automated ASN-level sinkholing, better attribution, deeper collaboration with ISPs/hosting/registrars/crypto platforms [29], and stronger international legal frameworks is needed.
- Application of Advanced Analytical Techniques for Ecosystem Modeling: Game theory complex systems science, or agent-based modeling can improve understanding of strategic interactions within the MaaS ecosystem [81]. Modeling economic incentives actor decision-making, and strategy impacts could identify equilibrium points, disruption leverage points, and optimal resource allocation [9,19,65].
- Addressing Usability, Operational Complexity, and User Experience of Proactive Defenses: Widespread adoption of advanced defenses (Table 2) requires addressing usability and overhead. Privacy-Preserving Telemetry Sharing is vital for training predictive models and TI collaboration but faces regulatory hurdles; federated learning or confidential computing may help [74,82]. User-centric design, automation, and AI can reduce burden and negative UX impact [17,32,74].

Interdisciplinary collaboration is key to bend the attacker-defender cost curve in favor of defense.

8. Content Enhancements for Practical Utility

8.1. Decision Tree for Technique Selection in Proactive Defense

Selecting appropriate proactive defenses (Table 2) from the array of available options is a complex task, contingent upon an organization's specific operational context, risk appetite, technical maturity, and resource availability. Figure 3 outlines a conceptual decision tree designed to guide organizations in this selection process, mapping constraints to relevant strategies against MaaS-driven cookie theft.

Navigating this decision tree involves a sequence of strategic considerations:

Device-Bound Identity Feasibility (Figure 3, top-center): The initial branching point considers whether the organization can implement robust device-bound identity mechanisms like FIDO2 or WebAuthn [9,10]. This depends on factors such as existing infrastructure, application compatibility, user base characteristics, and regulatory compliance mandates [28].

If YES: The primary emphasis should be on Zero-Trust Architecture (ZTA) principles [28,35], short Time-To-Live (TTL) for any residual session tokens [37], and leveraging predictive analytics

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

and behavioral detection for early warning [40,43]. An additional check for Token-Binding Feasibility (e.g., using cryptographic binding of cookies to TLS sessions) further refines this strategy; if feasible, it should be integrated [9].

Example Scenario: A modern tech company with a cloud-native infrastructure and a tech-savvy workforce could readily adopt FIDO2 for all internal and customer-facing applications, enforce 15-minute session TTLs, and invest in behavioral analytics [43].

If NO: If widespread device-bound identity is not immediately feasible (e.g., due to legacy systems or diverse unmanaged user endpoints), the emphasis shifts towards deception techniques like honeytokens, enhanced DNS analytics for C2 detection, and robust user training (Figure 3, right path). The organization must then assess if it has adequate IR Staffing for Honeytoken Response; if not, simpler decoys or focusing purely on training might be necessary [46].

MTD Feasibility (If Device-Bound Identity Path Chosen): For organizations leaning towards ZTA, the next consideration is the viability of Moving Target Defense (MTD) [36]. This requires Sufficient Infrastructure Elasticity (Figure 3, center-left), typically found in cloud-native or highly virtualized environments capable of dynamic resource provisioning and reconfiguration [39].

If YES (Elasticity Confirmed): MTD should be considered alongside the primary ZTA emphasis [40].

If NO: The focus remains on ZTA and other chosen measures without MTD.

Budget & Expertise (A Universal Consideration): This critical node (Figure 3, center) significantly influences the sophistication and breadth of deployable defenses, regardless of the initial path.

High Budget / High Expertise: Organizations can implement a comprehensive, advanced layered defense (Figure 3, bottom-left). This includes full-scale ZTA, adversarial ML training for detection models [41,43], advanced behavioral analytics, and dedicated proactive threat hunting teams [40].

Real-world Context: Large financial institutions or national critical infrastructure operators often possess the resources and mandate for such comprehensive deployments. Challenges include integration complexity across diverse systems and maintaining a highly skilled workforce [44,46]. Solutions involve phased rollouts, continuous training programs, and strategic partnerships with specialized vendors. The successful reduction of token replay by 92% in Azure AD with device-bound tokens illustrates the effectiveness of high-investment strategies [9].

Medium Budget / Moderate Expertise: A balanced proactive defense is achievable (Figure 3, bottom-center). This typically involves phased ZTA implementation [28], adoption of ephemeral tokens [37], SIEM-based analytics for anomaly detection [57], and basic honeytoken deployments [46].

Real-world Context: Mid-sized enterprises or public sector agencies might adopt this approach. Challenges include balancing security investments with other business priorities and potential user friction from stricter controls. Solutions involve risk-based prioritization of ZTA for critical assets [28] and careful tuning of ephemeral token lifespans [37]. The case study on the US hospital system leveraging ephemeral tokens and lightweight ZTA to reduce unauthorized access by 95% exemplifies this tier.

Low Budget / Limited Expertise: A foundational proactive defense is recommended (Figure 3, bottom-right). This leverages built-in security features of cloud services (e.g., conditional access policies), implements basic ephemeral token strategies where easily configurable, focuses heavily on strong user education and phishing awareness, and ensures diligent patching [37,46].

Real-world Context: Small to medium-sized businesses (SMBs) often fall into this category. The primary challenge is resource scarcity. Solutions involve maximizing the utility of existing security tools provided by SaaS vendors and focusing on high-impact, low-cost measures like MFA enforcement and user training [10,57].

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

Predictive Analytics Integration (If SIEM Data Science Capable): For organizations with SIEM capabilities and data science expertise (Figure 3, bottom-left decision node), deploying predictive analytics for early warning becomes a viable enhancement to their defensive posture [40,83].

This decision tree provides a structured, albeit simplified, approach. In practice, organizations will often blend strategies and iterate based on evolving threats and internal changes. The key is to align defensive investments with specific risk profiles and operational realities [11].

8.2. Key Insights Box: Concise Takeaways

- Cookie theft: industrialized, economically fueled, MaaS-scaled. MaaS polymorphism outpaces signature defenses (24hrs) [24,84].
- Static defenses obsolete; cybersecurity must be dynamic. Token binding, short TTLs slash stolen cookie resale profit [37,38].
- Proactive strategies (ZTA, behavioral analysis, hunting) essential vs. sophisticated evasion and reconnaissance techniques. Conceptual predictive indicators offer promise for forecasting waves, but require development and validation [28,40].
- Anticipating attacker evolution needs diligent technical, economic, behavioral monitoring. MTD shows success, incurs CPU overhead [36].
- Disrupting underlying economics paramount for long-term mitigation. Economic disruption vital as technical controls [19].

8.3. Commercial Tooling Snapshot

While focusing on strategies, it's useful to see how concepts are reflected in commercial tools. A comprehensive vendor evaluation is beyond scope, but mainstream categories support these defenses.

- Endpoint Detection and Response (EDR) Platforms: Central for post-compromise detection [85]. Modern EDRs use behavioral analysis for LotL ML for anomalies and offer threat hunting for cookie theft TTPs [62,74,86].
- Identity and Access Management (IAM) Solutions: Foundational for ZTA [35,57,58]. Modern IAMs facilitate strong/passwordless authentication manage token lifespans (ephemeral sessions) and enable context-aware access policies [13,32].
- Network Segmentation Tools: Used with ZTA to limit lateral movement if a cookie is compromised [64].
- Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) Platforms: Aggregate telemetry, correlate events, automate responses. Can implement dynamic policy via integration and facilitate threat hunting [11,36,74,87].

Practitioners should evaluate solutions for behavioral monitoring, integration, rapid D&R, and TI feed incorporation. Table 4 provides a snapshot of relevant commercial tooling categories.

Table 4. Commercial tooling categories relevant to adaptive cookie theft defense.

EDR Vendor	Adaptive Cookie-Theft Module	Technique Focus	Refs
CrowdStrike Falcon	Session-cookie anomaly detection	ML + device fingerprinting	[62,86]
Microsoft Defender	Token replay analytics	AAD risk graph	[13,32]
Sentinel One Singularity	Browser-artefact quarantine	Kernel sensor + rollback	[36]

9. Conclusion

The industrialization of cybercrime via Malware-as-a-Service (MaaS) has precipitated the evolution of cookie theft into a highly sophisticated and economically incentivized threat vector, fundamentally challenging extant cybersecurity paradigms. This investigation has systematically

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

deconstructed the adaptive ecosystem underpinning MaaS-driven cookie theft, elucidating its operational dynamics, economic drivers, and the co-evolutionary arms race between attackers and defenders. Our primary contribution, a novel conceptual model of this illicit ecosystem, provides a foundational framework for understanding the intricate interdependencies among key actors and the feedback loops that sustain its resilience.

The systematic review of offensive tactics (2020-2025)—including AI-augmented evasion, dynamic C2 infrastructures, and LotL methodologies—juxtaposed with an analysis of proactive defensive strategies—such as Zero-Trust Architectures, ephemeral tokenization, and adversarially robust machine learning—underscores a critical asymmetry. Conventional, static security measures are demonstrably outpaced by the agility and adaptive capacity inherent in MaaS operations. This necessitates an urgent and decisive paradigm shift towards dynamic, multi-layered, and, most critically, anticipatory defensive postures.

A core contribution of this work was the proposition of a multi-dimensional conceptual framework for predictive analytics. While its empirical validation and operationalization remain critical imperatives for future research, this framework offers a structured approach to integrating technical, economic, and behavioral indicators, aiming to furnish actionable foresight into emerging threat trajectories. Such predictive capabilities are indispensable for strategic resource allocation and the pre-emptive deployment of countermeasures. Furthermore, our analysis highlighted the strategic importance of disrupting the economic incentives fueling this ecosystem, alongside fostering robust, privacy-preserving collaborative threat intelligence sharing and navigating the complex implications of AI in both offensive and defensive cybersecurity applications.

The challenges inherent in countering MaaS-driven cookie theft are multifaceted and demand sustained, interdisciplinary research efforts. While this paper offers practical guidance, such as a decision-tree for defensive technique selection, the path towards truly resilient security architectures requires ongoing innovation [88]. Future research trajectories must prioritize the empirical validation of predictive models, the development of standardized metrics for ecosystem risk assessment, the advancement of autonomous adaptive defense mechanisms, and the establishment of more effective legal and policy frameworks for disrupting transnational cybercriminal operations.

Mitigating the pervasive threat of MaaS-driven cookie theft requires a continuous, adaptive, and intelligence-driven approach. It is an endeavor that extends beyond mere technological solutions, demanding a profound understanding of the adversary's economic motivations and operational calculus. This paper contributes to this endeavor by providing a comprehensive analytical lens and a conceptual blueprint for future anticipatory strategies, recognizing that lasting security in this domain hinges on our collective capacity to innovate and adapt more rapidly than those who seek to exploit it.

Limitations of Current Work:

- Predictive Framework Conceptual: The multi-dimensional predictive framework discussed is conceptual and has not been empirically validated. Its feasibility, accuracy, and practical utility require dedicated future research, development, and rigorous testing.
- Data Source Reliance (for a future predictive system): If such a framework were developed, its reliance on dark web and underground forum data would present challenges of data availability, opacity, and potential manipulation, requiring robust vetting.

9.1. Prioritized Future Research Directions: A Roadmap

Effectively mitigating MaaS-driven cookie theft demands a holistic approach. To guide ongoing research efforts, we propose a structured roadmap prioritizing future directions based on urgency, feasibility, and potential impact:

Phase 1: Foundational Development & Near-Term Wins (1-2 Years)

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

(High Urgency/High Impact; Moderate-High Feasibility) Empirical Validation of Core Predictive Analytics Components:

- Action: Develop and rigorously test initial predictive models (as conceptualized in Section 6 and Figure 2) focusing on readily available data sources (e.g., dark web market prices for cookies, MaaS provider announcements on public channels, aggregated malware telemetry).
- Priority: Establish baseline accuracy for forecasting key ecosystem shifts (e.g., price volatility, emergence of new MaaS kits). This is paramount for building trust and demonstrating the viability of predictive approaches.

(High Urgency/Moderate Impact; Moderate Feasibility) Development of Standardized Ecosystem-Health Metrics:

- Action: Define and pilot a core set of quantifiable metrics (e.g., MaaS kit churn rate, average stolen cookie lifespan before resale, affiliate-to-provider revenue ratios) to benchmark ecosystem risk and defense effectiveness.
- Priority: Provide a common language and measurement framework for assessing the threat landscape.

(Moderate Urgency/High Impact; Moderate Feasibility) In-Depth Analysis of Economic Disruption Strategies:

- Action: Conduct detailed case studies on the economic impact of successful takedowns (e.g., "Operation Endgame" [65]) and the widespread adoption of specific defensive measures (e.g., FIDO2). Model the financial repercussions for MaaS actors.
- Priority: Provide evidence-based recommendations for economically disrupting the MaaS ecosystem.

Phase 2: Operationalization & Advanced Modeling (2-4 Years)

(High Urgency/High Impact; Moderate Feasibility) Operationalization and Pilot Deployment of Predictive Analytics Frameworks:

- Action: Transition validated predictive models (from Phase 1) into pilot deployments within consenting SOC environments. Develop practical playbooks for SOC analysts to act upon predictive intelligence.
- Priority: Bridge the gap between conceptual models and real-world defensive utility.

(Moderate Urgency/High Impact; Moderate Feasibility) Research into Autonomous Adaptive Defense Controllers:

- Action: Investigate and prototype AI-driven autonomous defense controllers that can dynamically adjust security postures (e.g., token TTLs, ZTA policy granularity, honeypot configurations) based on validated predictive insights and real-time threat intelligence [27,33].
- Priority: Enhance the speed and scalability of defensive responses to adaptive threats.

(Moderate Urgency/Moderate Impact; Low-Moderate Feasibility) Advanced Ecosystem Modeling using Game Theory and Agent-Based Models:

- Action: Develop sophisticated computational models [67] to simulate strategic interactions between MaaS actors and defenders, testing the impact of various disruptive interventions [17,46].
- Priority: Improve understanding of complex ecosystem dynamics and identify optimal long-term disruption strategies.

Phase 3: Scaling, Policy, and Holistic Understanding (4+ Years)

(Moderate Urgency/High Impact; Low Feasibility) Scalable and Robust Privacy-Preserving Intelligence Sharing Architectures:

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

- Action: Develop and standardize technologies (e.g., advanced federated learning [61], confidential computing) for sharing sensitive threat intelligence at scale without compromising privacy or commercial interests.
- Priority: Overcome critical barriers to collective defense by enabling richer, more timely intelligence exchange.

(Low Urgency/High Impact; Low Feasibility) Development of International Legal and Policy Frameworks for MaaS Disruption:

- Action: Foster international collaboration to establish robust legal and policy frameworks that facilitate cross-border takedowns, attribution, and prosecution of MaaS operators and affiliates [62,65].
- Priority: Address the inherently global and often jurisdictionally ambiguous nature of MaaS operations.

(Low Urgency/Moderate Impact; Moderate Feasibility) In-Depth Socio-Technical Research into Human Factors in MaaS Ecosystems:

- Action: Conduct qualitative and quantitative research into the motivations, decision-making processes, social structures, and technical skill progression of MaaS actors.
- Priority: Provide deeper insights into the "human element" of the MaaS ecosystem to inform more nuanced disruption and prevention strategies.

This roadmap underscores that future research must prioritize the development and validation of predictive models, alongside creating autonomous, usable, scalable defenses [76], and exploring novel MaaS disruption tactics. A convergence of computer science, economics, behavioral science, and law enforcement is imperative to collapse attacker ROI and durably stabilize the ecosystem for defense.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MaaS	Malware-as-a-Service
MFA	Multi-Factor Authentication
ZTA	Zero-Trust Architecture
MTD	Moving-Target Defense
AI	Artificial Intelligence
ML	Machine Learning
IOC	Indicator of Compromise
TTP	Tactics, Techniques, and Procedures
DGA	Domain Generation Algorithm
LotL	Living-off-the-Land
TTL	Time-To-Live
ATO	Account Takeover
SOC	Security Operations Center
EDR	Endpoint Detection and Response
SIEM	Security Information and Event Management
XSS	Cross-Site Scripting

References

1. SpyCloud Labs, "How Infostealers Are Bypassing New Chrome Security Feature to Steal User Session Cookies," Oct. 2024. [Online]. Available: https://spycloud.com/blog/infostealers-bypass-new-chrome-security-feature/

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

2. J. Cox, "Inside the Massive Crime Industry That's Hacking Billion-Dollar Companies," Nov. 2024. [Online]. Available: https://www.wired.com/story/inside-the-massive-crime-industry-thats-hacking-billion-dollar-companies
3. Sophos, "'The 2024 Sophos Threat Report: Cybercrime on Main Street,'" Mar. 2024.
4. G. Rodríguez-Galán and J. Torres, "Personal data filtering: a systematic literature review comparing the effectiveness of XSS attacks in web applications vs cookie stealing," *Ann. des Télécommunications*, vol. 79, pp. 763–802, 2024, doi: 10.1007/s12243-024-01022-8.
5. C. Patsakis, D. Arroyo, and F. Casino, "The Malware as a Service Ecosystem," 2024. [Online]. Available: https://arxiv.org/html/2405.04109v1
6. Secureworks Counter Threat Unit, "The Growing Threat from Infostealers," May 2023. [Online]. Available: https://www.secureworks.com/research/the-growing-threat-from-infostealers
7. Kaspersky Global Research and A. Team, "The Evolving Threat Landscape of Infostealers: Trends, Statistics, and Mitigation Strategies," Mar. 2025. [Online]. Available: https://content.kaspersky-labs.com/se/media/en/enterprise-security/data-stealer-storm-2025.pdf
8. Darktrace, "'The Rise of the Lumma Info Stealer,'" 2024.
9. J. Nurmi, M. Niemelä, and B. B. Brumley, "Malware Finances and Operations: A Data-Driven Study of the Value Chain for Infections and Compromised Access," 2023. [Online]. Available: https://arxiv.org/abs/2306.15726
10. FS-ISAC, "Navigating Cyber 2024: Annual Threat Review and Predictions," Sep. 2024. [Online]. Available: https://www.fsisac.com/navigatingcyber2024fsisac.com+3fsisac.com+3LinkedIn+3
11. M. Danish, "Enhancing Cyber Security through Predictive Analytics: Real-Time Threat Detection and Response," Jul. 2024. [Online]. Available: https://arxiv.org/abs/2407.10864
12. D. Gaurav and A. Kaushik, "Detection and Prevention of Session Hijacking in Web Application Management," *Int J Comput Appl*, vol. 176, no. 36, pp. 1–4, 2020, [Online]. Available: https://www.researchgate.net/publication/342745140
13. Okta, "Defending Against Session Hijacking," Aug. 2022. [Online]. Available: https://sec.okta.com/session-cookietheft/
14. Flashpoint, "Flashpoint 2025 Global Threat Intelligence Report: Stay Ahead of Emerging Threats," Mar. 2025. Accessed: May 30, 2025. [Online]. Available: https://flashpoint.io/resources/report/flashpoint-2025-global-threat-intelligence-gtir/Flashpoint+8
15. European Union Agency for Cybersecurity (ENISA), "ENISA Threat Landscape 2024," Sep. 2024. [Online]. Available: https://securitydelta.nl/media/com_hsd/report/690/document/ENISA-Threat-Landscape-2024.pdf
16. E. Hoxha, I. Tafa, K. Ndoni, I. Tahiraj, and A. Muco, "Session hijacking vulnerabilities and prevention algorithms in the use of internet.," *Global Journal of Computer Sciences: Theory and Research*, vol. 12, no. 1, pp. 23–31, Jun. 2022, doi: 10.18844/GJCS.V12I1.7449.
17. J. Singh and R. Singh, "Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions," 2023. [Online]. Available: https://www.researchgate.net/publication/369885804
18. I. Rosenberg, A. Shabtai, Y. Elovici, and L. Rokach, "Adversarial machine learning attacks and defense methods in the cyber security domain," *ACM Computing Surveys (CSUR)*, vol. 54, no. 5, pp. 1–36, 2021.
19. N. Samia, S. Saha, and A. Haque, "Predicting and mitigating cyber threats through data mining and machine learning," *Comput Commun*, vol. 228, p. 107949, 2024.
20. H. Kwon, H. Nam, S. Lee, C. Hahn, and J. Hur, "(In-)Security of Cookies in HTTPS: Cookie Theft by Removing Cookie Flags," *IEEE Transactions on Information Forensics and Security*, vol. 15, pp. 1204–1215, 2020, doi: 10.1109/TIFS.2019.2938416.
21. The Hacker News, "'More_eggs MaaS Expands Operations with RevC2 Backdoor and Venom Loader,'" Dec. 2024.
22. S. K. Sahay, A. Sharma, and H. Rathore, "Evolution of malware and its detection techniques," in *Information and Communication Technology for Sustainable Development: Proceedings of ICT4SD 2018*, Springer Singapore, 2020, pp. 139–150.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

23. S. Kasarapu, S. Shukla, R. Hassan, A. Sasan, H. Homayoun, and S. M. P. Dinakarrao, "Generative Al-Based Effective Malware Detection for Embedded Computing Systems," Apr. 2024. [Online]. Available: https://arxiv.org/abs/2404.02344arXiv+1arXiv+1
24. C. Catalano, A. Chezzi, M. Angelelli, and F. Tommasi, "Deceiving Al-based malware detection through polymorphic attacks," *Comput Ind*, vol. 143, p. 103751, 2022.
25. J. Sims, "BlackMamba: Using Al to Generate Polymorphic Malware," Jul. 2023. [Online]. Available: https://www.hyas.com/blog/blackmamba-using-ai-to-generate-polymorphic-malware
26. R. Min and H. Kim, "Adversarial Attacks Against Windows PE Malware Detection: A Systematic Review," *Comput Secur*, vol. 132, p. 103134, 2023, [Online]. Available: https://dl.acm.org/doi/10.1016/j.cose.2023.103134
27. AhnLab Security Emergency Response Center (ASEC), "January 2025 Threat Trend Report on Ransomware," Feb. 2025.
28. D. Tyler and T. Viana, "Trust no one? a framework for assisting healthcare organisations in transitioning to a zero-trust network architecture," *Applied Sciences*, vol. 11, no. 16, p. 7499, 2021.
29. O. V Sviatun, O. V Goncharuk, C. Roman, O. Kuzmenko, and I. V Kozych, "Combating cybercrime: economic and legal aspects," *WSEAS Transactions on Business and Economics*, vol. 18, pp. 751–762, 2021.
30. R. T. Prapty, S. A. Md, S. Hossain, and H. S. Narman, "Preventing Session Hijacking using Encrypted One-Time-Cookies," *2020 Wireless Telecommunications Symposium (WTS)*, vol. 2020-April, pp. 1–6, Jun. 2020, doi: 10.1109/WTS48268.2020.9198717.
31. M. Naseer et al., "Malware detection: issues and challenges," in *Journal of Physics: Conference Series*, IOP Publishing, Apr. 2021, p. 12011.
32. Microsoft, "Token theft protection with Microsoft Entra, Intune, Defender XDR & Windows." Accessed: Jun. 01, 2025. [Online]. Available: https://techcommunity.microsoft.com/blog/microsoftmechanicsblog/token-theft-protection-with-microsoft-entra-intune-defender-xdr--windows/4265675
33. Microsoft, "Microsoft Digital Defense Report 2024,'" 2024.
34. The Hacker News, "'Session Hijacking 2.0 — The Latest Way That Attackers are Bypassing MFA,'" Sep. 2024.
35. Y. He, D. Huang, L. Chen, Y. Ni, and X. Ma, "A survey on zero trust architecture: Challenges and future trends," *Wirel Commun Mob Comput*, vol. 2022, p. 6476274, 2022.
36. V. Casola, A. De Benedictis, D. Iorio, and S. Migliaccio, "A Moving Target Defense Framework to Improve Resilience of Cloud-Edge Systems," in *International Conference on Advanced Information Networking and Applications*, Cham: Springer Nature Switzerland, Apr. 2025, pp. 243–252.
37. K. Satheesh, "Improving Security and Session Handling in Distributed Networks with JSON Web Tokens," 2024.
38. H. Flanagan, "Token Lifetimes and Security in OAuth 2.0: Best Practices and Emerging Trends," *IDPro Body of Knowledge*, vol. 1, no. 15, 2024.
39. K. Shaukat et al., "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies (Basel)*, vol. 13, no. 10, p. 2509, 2020.
40. A. Mahboubi et al., "Evolving techniques in cyber threat hunting: A systematic review," *Journal of Network and Computer Applications*, p. 104004, 2024.
41. A. K. Gupta and P. Sharma, "Adversarial Machine Learning in Cybersecurity," *International Journal for Innovative Research in Technology (IJIRT)*, vol. 10, no. 3, pp. 85–90, 2023, [Online]. Available: https://ijirt.org/publishedpaper/IJIRT169990_PAPER.pdf
42. H. Bostani and others, "On the Effectiveness of Adversarial Training on Malware Classifiers," 2024. [Online]. Available: https://arxiv.org/abs/2412.18218
43. R. M. S. Oliveira and E. T. Franco, "Adversarial Attacks and Defenses in Deep Learning Models," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 11, no. 2, pp. 998–1005, 2023, [Online]. Available: https://www.ijisae.org/index.php/IJISAE/article/view/5482

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

44. M. Alkatheiri, A. F. Zohdy, and N. Nasser, "Adversarial Examples: A Survey of Attacks and Defenses in Deep Learning-Based Cybersecurity," *Expert Syst Appl*, vol. 229, p. 120789, 2023, [Online]. Available: https://www.sciencedirect.com/science/article/abs/pii/S0957417423027252
45. A. K. Maurya, S. Sharma, and S. N. Panda, "DGA Based Malware Detection Using Machine Learning Techniques," *International Journal of Computer Sciences and Engineering*, vol. 8, no. 12, pp. 1–6, 2020, [Online]. Available: https://www.researchgate.net/publication/363542212
46. S. Bala and R. Narwal, "Data Science in Cybersecurity to Detect Malware-Based Domain Generation Algorithm: Improvement, Challenges, and Prospects," 2024. [Online]. Available: https://www.researchgate.net/publication/382645626
47. P. Pajo, "Fast Flux in Cybersecurity: Mechanisms, Evolution, National Security Implications, and Mitigation Strategies in 2025," 2025.
48. M. Akibis, J. Pereira, D. Clark, V. Mitchell, and H. Alvarez, "Measuring propagation patterns via network traffic analysis: An automated approach," 2024.
49. S. Roy, N. Sharmin, J. C. Acosta, C. Kiekintveld, and A. Laszka, "Survey and taxonomy of adversarial reconnaissance techniques," *ACM Comput Surv*, vol. 55, no. 6, pp. 1–38, 2022.
50. N. CISA, D. FBI, T. EPA, C. ACSC, and N. N. UK-NCSC, "Joint Guidance: Identifying and Mitigating Living Off the Land Techniques," 2024. [Online]. Available: https://www.cisa.gov/
51. Fortinet, "Living Off The Land (LOTL) Attacks and Techniques," 2023. [Online]. Available: https://www.fortinet.com/resources/cyberglossary/living-off-the-land-lotl
52. R. Stamp, "Living-off-the-Land Abuse Detection Using Natural Language Processing and Supervised Learning," Aug. 2022. [Online]. Available: https://arxiv.org/abs/2208.12836
53. T. Yang and K. Huang, "Evading Deep Learning-Based Malware Detectors via Obfuscation," 2023. [Online]. Available: https://par.nsf.gov/servlets/purl/10554700
54. Apriorit, "Malware Sandbox Evasion: Detection Techniques & Solutions," 2023. [Online]. Available: https://www.apriorit.com/dev-blog/545-sandbox-evading-malware
55. W. Ahmad, M. A. Raza, S. Nawaz, and F. Waqas, "Detection and analysis of active attacks using honeypot," *Int J Comput Appl*, vol. 184, no. 50, pp. 27–31, 2023.
56. V. D. Priya and S. S. Chakkaravarthy, "Containerized cloud-based honeypot deception for tracking attackers," *Sci Rep*, vol. 13, no. 1, p. 1437, 2023.
57. National Institute of Standards and T. (NIST), "Zero Trust Architecture," Aug. 2020.
58. S. Ghasemshirazi, G. Shirvani, and M. A. Alipour, "Zero trust: Applications, challenges, and opportunities," 2023.
59. S. Ahmadi, "'Autonomous Identity-Based Threat Segmentation in Zero Trust Architectures,'" Jan. 2025.
60. Cybersecurity and I. S. Agency, "'Zero Trust Maturity Model Version 2.0,'" Apr. 2023.
61. S. K. Sharma and S. A. Hameed, "Analysis of Malware Impact on Network Traffic Using Behavior-Based Detection Technique," *International Journal of Advances in Data and Information Systems*, vol. 1, no. 2, pp. 69–78, 2020, [Online]. Available: https://www.researchgate.net/publication/340359596
62. A. Shan and S. Myeong, "Proactive threat hunting in critical infrastructure protection through hybrid machine learning algorithm application," *Sensors*, vol. 24, no. 15, p. 4888, 2024.
63. S. R. Sindiramutty, "'Autonomous Threat Hunting: A Future Paradigm for AI-Driven Threat Intelligence,'" Jan. 2024.
64. N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig, and R. Doss, "Zero trust architecture (zta): A comprehensive survey," *IEEE access*, vol. 10, pp. 57143–57179, 2022.
65. H. M. Melaku, "Context-based and adaptive cybersecurity risk management framework," *Risks*, vol. 11, no. 6, p. 101, 2023.
66. National Security Agency, "'Advancing Zero Trust Maturity Throughout the Visibility and Analytics Pillar,'" May 2024.
67. Apostol Vassilev, Alina Oprea, Anca D. Fordyce, and Hyrum Anderson, "Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations," Jan. 2024.
68. Mandiant, "M-Trends 2025," Mar. 2025.
69. Kaspersky, "Managed Detection and Response Analyst Report 2023," 2024.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 11 June 2025 doi:10.20944/preprints202506.0901.v1

70. Palo Alto Networks Unit 42, "2025 Unit 42 Global Incident Response Report," Dec. 2024.
71. M. Raeiszadeh, A. Ebrahimzadeh, R. H. Glitho, J. Eker, and R. A. Mini, "Real-Time Adaptive Anomaly Detection in Industrial IoT Environments," *IEEE Transactions on Network and Service Management*, 2024.
72. M. Serror, S. Hack, M. Henze, M. Schuba, and K. Wehrle, "Challenges and opportunities in securing the industrial internet of things," *IEEE Trans Industr Inform*, vol. 17, no. 5, pp. 2985–2996, 2020.
73. Health Sector Cybersecurity Coordination Center (HC3), "Lumma Loader Activity Targeting Healthcare," May 2025.
74. S. R. Sindiramutty et al., "Explainable Al for cybersecurity," in *Advances in Explainable Al Applications for Smart Cities*, IGI Global Scientific Publishing, 2024, pp. 31–97.
75. R. H. Chowdhury, N. U. Prince, S. M. Abdullah, and L. A. Mim, "The role of predictive analytics in cybersecurity: Detecting and preventing threats," *World Journal of Advanced Research and Reviews*, vol. 23, no. 2, pp. 1615–1623, 2024.
76. R. Basheer and B. Alkhatib, "Threats from the dark: a review over dark web investigation research for cyber threat intelligence," *Journal of Computer Networks and Communications*, vol. 2021, p. 1302999, 2021.
77. V. Parmar, H. A. Sanghvi, R. H. Patel, and A. S. Pandya, "A comprehensive study on passwordless authentication," in *2022 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, IEEE, Apr. 2022, pp. 1266–1275.
78. Microsoft, "Passwordless by Default: FIDO2 Deployment Case Study," Jun. 2024.
79. Europol, "Operation Endgame Dismantles Bulletproof Hosting Infrastructure," Feb. 2025.
80. V. Thapliyal and P. Thapliyal, "The Role of Machine Learning in Cybersecurity. Digital Threats: Research and Practice," *Sensors*, 2023.
81. K. Padur, H. Borrion, and S. Hailes, "Using Agent-Based Modelling and Reinforcement Learning to Study Hybrid Threats," *Journal of Artificial Societies and Social Simulation*, vol. 28, no. 1, 2025.
82. M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, "Cyber threat intelligence sharing scheme based on federated learning for network intrusion detection," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 3, 2023.
83. J. Yu and Q. Li, "Moving Target Defense for Detecting Coordinated Cyber-Physical Attacks on Power Grids via a Modified Sensor Measurement Expression," *Electronics (Basel)*, vol. 12, no. 7, p. 1679, 2023, [Online]. Available: https://doi.org/10.3390/electronics12071679
84. K. Drakonakis, S. Ioannidis, and J. Polakis, "The Cookie Hunter: Automated Black-box Auditing for Web Authentication and Authorization Flaws," *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security*, p., 2020, doi: 10.1145/3372297.3417869.
85. A. Arfeen, S. Ahmed, M. A. Khan, and S. F. A. Jafri, "Endpoint detection & response: A malware identification solution," in *2021 international conference on cyber warfare and security (ICCWS)*, IEEE, Nov. 2021, pp. 1–8.
86. S. Rai, "Behavioral threat detection: Detecting living of land techniques," University of Twente, 2020.
87. G. González-Granadillo, S. González-Zarzosa, and R. Diaz, "Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures," *Sensors*, 2021.
88. J. Edwards, *A comprehensive guide to the NIST cybersecurity framework 2.0: Strategies, implementation, and best practice*. John Wiley & Sons, 2024.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.

© 2025 by the author(s). Distributed under a Creative Commons CC BY license.