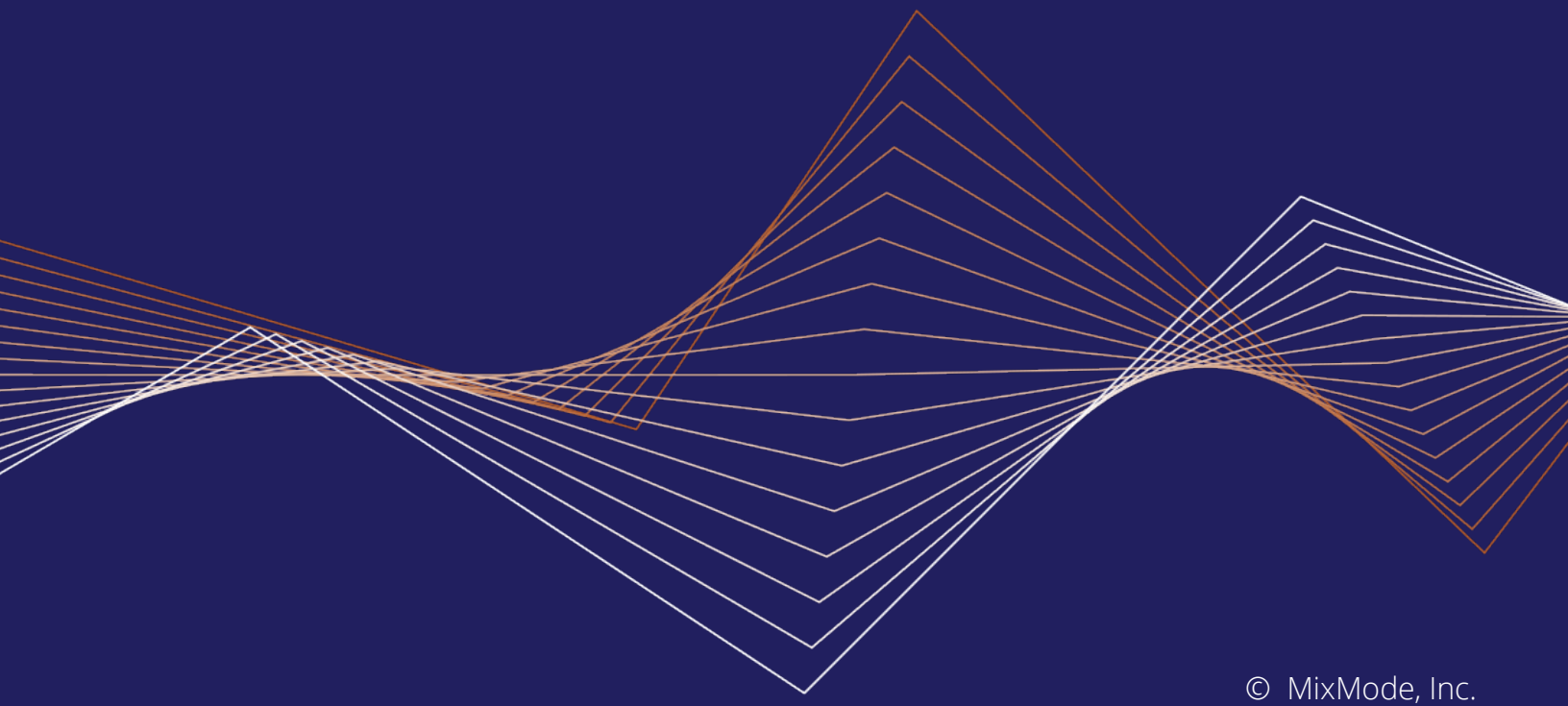
MixMode®

THREAT REPORT

Hiding in Plain Sight: Why Geolocation Data is One of Many Risk Indicators in Cloud Environments

Michael Yelland
MixMode's Architect & Principal Researcher



Cybercriminals are increasingly leveraging legitimate cloud services such as AWS, Microsoft Azure, and Google Cloud to mask malicious activities, a tactic known as infrastructure laundering. This method enables attackers to hide within trusted cloud environments, complicating detection and mitigation efforts. The recent OAuth security risks we previously outlined serve as a foundation for understanding how attackers manipulate cloud-based authentication and infrastructure. Now, with the rise of advanced techniques like DeepSeek exploits, organizations must adopt a more nuanced approach to cloud security—one that prioritizes behavioral analytics over traditional indicators like geolocation.

The Growing Threat: Infrastructure Laundering in Cloud Environments

Key Threat Actor: The Funnull Network

The Funnull network, a cybercriminal operation linked to Chinese actors, has been abusing cloud infrastructure to conduct fraud, phishing campaigns, and illicit financial transactions. The network leverages these platforms to create fake business identities, distribute malware, and host command-and-control (C2) operations. These cybercriminals choose cloud environments for multiple reasons:

- **Legitimacy:** Cloud-hosted resources are trusted by default.
- **Scalability:** Cloud environments allow attackers to quickly pivot.
- **Evasion:** Dynamic cloud IPs evade traditional filtering.
- **Affordability:** Pay-as-you-go services offer cost-efficient cybercrime infrastructure.

By using major cloud providers, their activities appear more legitimate, reducing suspicion from cybersecurity defenses.

Cloud providers face significant challenges when combating such abuse, as their mitigation strategies often remain reactive, lacking proactive detection mechanisms. Identity verification processes are frequently circumvented using stolen credentials, fake businesses, or cryptocurrency payments.

Shifting Risk Landscape: TikTok's Data Migration and DeepSeek Exploits

The TikTok Cloud Migration Controversy

Recent reports reveal that TikTok's migration of servers to less-regulated cloud environments raises significant cybersecurity concerns. This move complicates geolocation-based risk assessments, increasing risks like:

- **User Tracking:** Potential surveillance of user interactions.
- **Data Sovereignty:** Uncertainty around access control in foreign jurisdictions.
- **Influence Campaigns:** Algorithmic manipulation to shape public discourse.

These developments illustrate the limitations of geolocation as a primary risk indicator, highlighting the need for behavioral data analysis.

DeepSeek Exploits: AI-Driven Reconnaissance

DeepSeek exploits utilize advanced AI techniques to uncover vulnerabilities within cloud environments. Attackers using DeepSeek can:

- Identify misconfigured AWS S3 buckets.
- Locate abandoned or unprotected APIs.
- Discover exposed authentication keys from repositories like GitHub.

These tactics enable attackers to infiltrate systems by mimicking legitimate cloud services, often disguising their malicious infrastructure as familiar Content Delivery Networks (CDNs) or security tools.

Weaponizing Collaboration Tools for Cybercrime

Popular collaboration platforms such as Slack, Trello, and Discord have become attractive targets for cybercriminals. Attackers exploit these tools' built-in encryption and persistent connectivity to:

- Exfiltrate sensitive data unnoticed.
- Maintain covert command-and-control (C2) channels.
- Automate attack sequences via bot integrations.

The Intersection with OAuth Security Risks

This evolving threat landscape directly parallels the OAuth vulnerabilities discussed in our previous report. Attackers bypass traditional access controls by stealing and manipulating OAuth tokens. The persistent nature of these tokens across multiple services grants attackers prolonged access without detection, posing substantial risks to cloud-based infrastructure.

The Shared Weakness: Trust Assumptions

Both infrastructure laundering and OAuth exploits share a critical flaw: the implicit trust granted to authenticated sessions. Traditional security tools often fail to continuously validate these sessions, especially in Zero Trust environments where OAuth token monitoring is neglected.

Why Geolocation Alone is Insufficient

Historically, geolocation data served as a key metric for identifying malicious activity. However, modern attackers leverage cloud services worldwide, rendering this approach inadequate. Infrastructure laundering techniques obscure true origins, allowing attacks to appear as if they originate from legitimate regions.

Behavioral Analytics as the New Standard

Effective detection now depends on understanding behavior patterns rather than relying on static indicators. Behavioral analytics detect deviations from normal activity, such as:

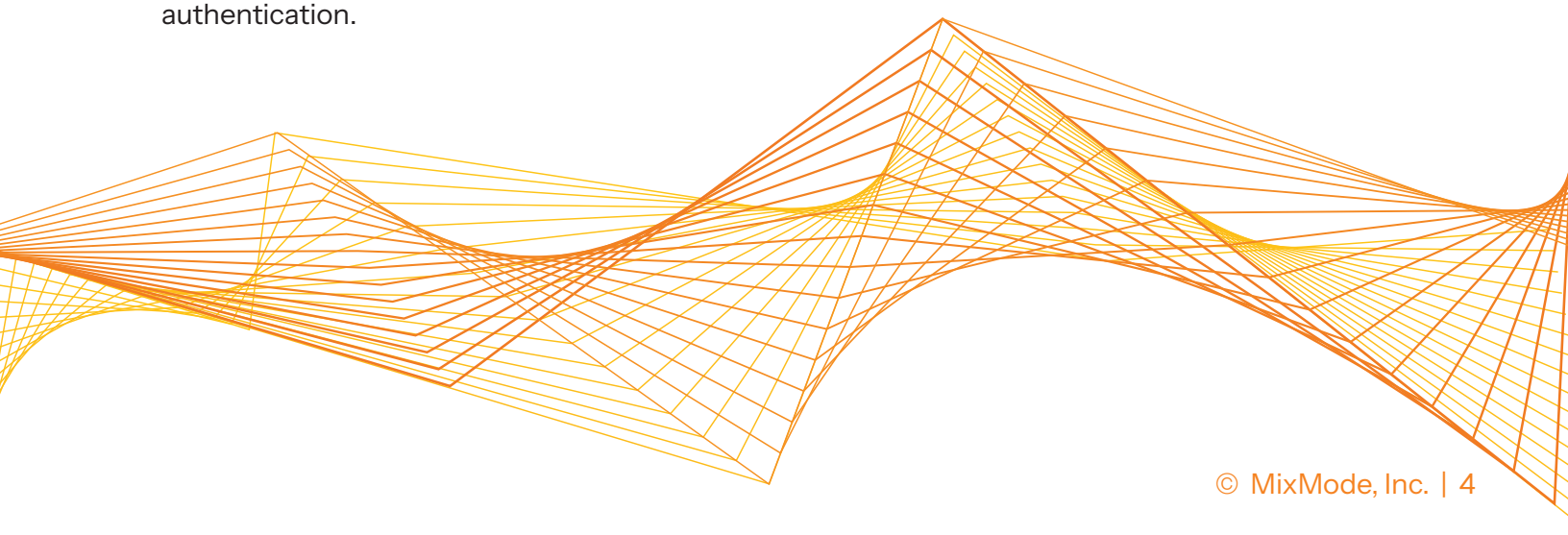
- Unusual access patterns.
- Anomalous API usage.
- Sudden spikes in data exfiltration activities.

MixMode's AI-Driven Approach to Cloud Security

MixMode's platform addresses these evolving threats by applying self-learning, generative AI to monitor and analyze cloud environments in real-time. Unlike traditional SIEMs that rely on static rules, MixMode dynamically adapts to new threats through continuous learning.

Key Capabilities of MixMode's AI:

- **Real-Time Anomaly Detection:** Identifies deviations indicative of potential OAuth or infrastructure laundering exploits.
- **Cross-Domain Data Correlation:** Integrates CloudTrail logs, network traffic, and API activity to detect sophisticated attack vectors.
- **User Analytics Integration:** Focuses on understanding user behavior to differentiate between legitimate access and malicious activity.
- **Zero Trust Reinforcement:** Continuously monitors OAuth tokens, ensuring session integrity even after authentication.



Cloud Security Insights: Lessons from a Financial Services Institution

A large financial services institution previously deployed MixMode to address cloud-based authentication and API abuse. The implementation led to a 96% reduction in false positives and real-time detection of OAuth-based session hijacking. These outcomes underscore the platform's ability to deliver actionable insights without overwhelming analysts with irrelevant alerts.

Industry-Wide Trends and Recent Research Recent cybersecurity studies echo these findings:

- A 2024 Gartner report found that 85% of successful cloud attacks involve human-related factors, including misconfigured OAuth tokens and neglected identity monitoring.
- A research paper by Unit 42 revealed that nearly 70% of publicly accessible cloud buckets contain sensitive data due to poor configuration.
- Salt Labs' investigation into OAuth token misuse demonstrated the critical need for continuous token monitoring in cloud applications.

The Need for Proactive Cloud Security

The evolution of infrastructure laundering, OAuth abuse, and DeepSeek exploits underscores the urgency for modern, AI-driven security solutions. Geolocation remains a useful component of risk assessment, but true cybersecurity resilience comes from analyzing multi-dimensional signals, ensuring organizations can spot hidden threats before they escalate into major breaches. Organizations must implement continuous behavioral monitoring to detect, analyze, and mitigate emerging threats.
MixMode's AI-powered platform delivers the necessary capabilities by autonomously adapting to evolving risks, ensuring robust defense mechanisms against cloud-based attacks. As threat actors continue to refine their tactics, proactive, behavior-focused analytics will remain essential for safeguarding critical infrastructure and sensitive data.

Contact MixMode today for more information.