Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

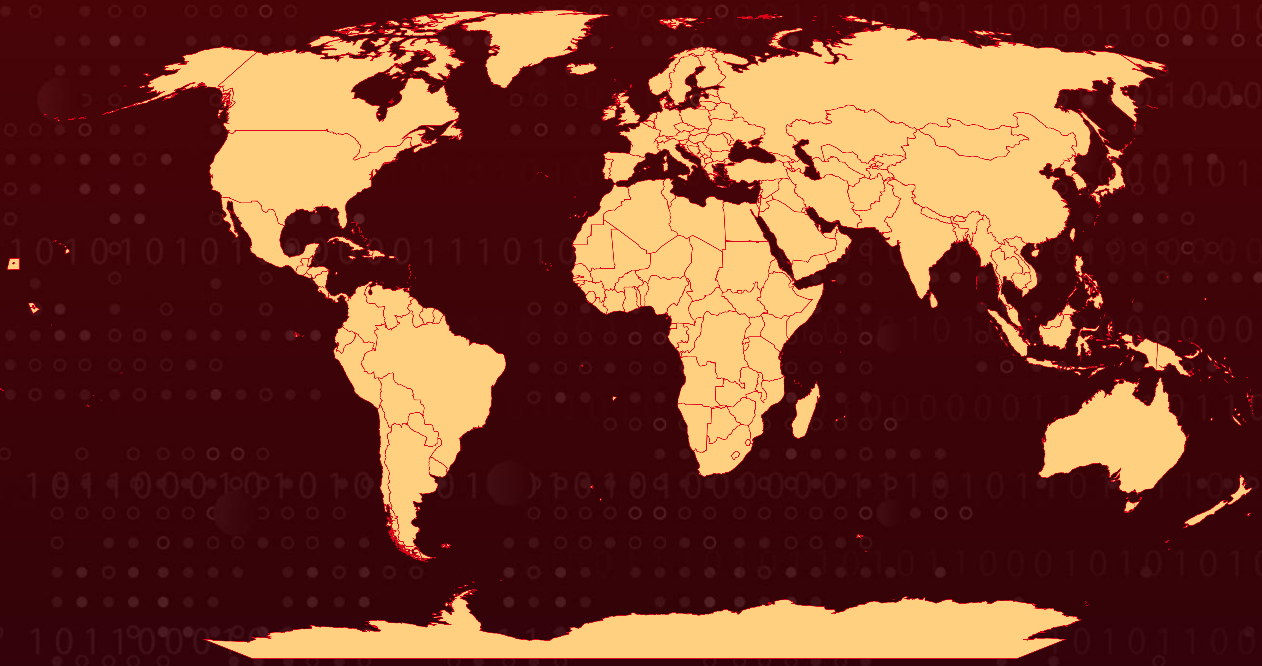
Critical Cloud Threat: Azure Blob Storage Under Active Attack

Date of Publication	Admiralty Code	TA Number
October 23, 2025	A1	TA2025321

Summary

First Seen: October 2025
Targeted Countries: Worldwide
Targeted Platform: Microsoft Azure
Targeted Azure Services: Blob Storage, Azure Functions, Logic Apps
Attack Vector: Misconfigured or publicly exposed Blob Storage accounts, leaked credentials (SAS tokens, account keys), and insecure automation triggers
Threat Actor: Unattributed (TTPs align with financially motivated and espionage-driven groups)
Attack: Azure Blob Storage, widely used for unstructured data such as backups, analytics datasets, and AI models, has become a prime target for attackers. Threat actors exploit misconfigured or publicly exposed storage accounts, stolen credentials, and vulnerable blob-triggered automation to gain access and establish persistence. Once inside, they perform data discovery, lateral movement, and exfiltration, sometimes using Blob Storage itself for command-and-control or malware distribution. The attacks can result in large-scale data theft, corruption, or ransomware deployment, posing significant operational, financial, and reputational risks.

Attack Regions



Attack Details

#1

Azure Blob Storage is a scalable cloud object storage solution used to store large volumes of unstructured data, including documents, backups, analytics data, and AI training datasets. While attackers historically targeted compute workloads, Blob Storage has become a favored entry and persistence point because it often contains high-value data and can trigger downstream workloads via Azure Functions or Logic Apps. Misconfigured or publicly exposed storage accounts are therefore highly appealing targets.

#2

There are ongoing campaigns where threat actors actively target weakly secured Blob Storage environments. Attacks typically begin with reconnaissance, including enumeration of storage accounts and containers, harvesting leaked credentials, and, in some cases, AI-assisted prediction of storage endpoints. Initial access is most often gained through compromised credentials, such as storage account keys or Shared Access Signatures (SAS), or through misconfigured blob-triggered automation that inadvertently exposes execution paths.

#3

Once inside, attackers establish malicious infrastructure and persistence, often issuing long-lived tokens, modifying access controls, or tampering with diagnostic and firewall settings to evade detection. They perform discovery of sensitive data and weak defenses, and pivot laterally across linked compute or data services. Blob Storage's integration with Azure workloads enables stealthy and efficient lateral movement.

#4

Attackers also use Blob Storage for data staging, exfiltration, and command-and-control (C2). Replication and copy features allow quiet movement of large datasets, while blob metadata or updates can serve as covert C2 channels. Some campaigns weaponize storage to distribute malware, host phishing pages, or poison AI datasets. The impact includes large-scale data theft, data corruption, and ransomware encryption, posing serious operational, financial, and reputational risks to affected organizations.

Recommendations

Enable Microsoft Defender for Storage: Activate Microsoft Defender for Storage on all accounts to detect and alert on unusual activities such as data exfiltration, malware uploads, or suspicious access scenarios. The service uses advanced threat intelligence and anomaly detection to identify potential compromises in real time.

Use Microsoft Entra ID (Azure AD) for Authorization: Configure Azure Blob Storage to use Microsoft Entra ID–based authentication instead of shared keys or SAS tokens. Entra ID enforces identity-aware, least-privilege access controls and significantly reduces exposure from credential theft or token misuse.

Disable Anonymous and Shared Key Access: Disallow anonymous read access and Shared Key authorization across all storage accounts, particularly those hosting sensitive workloads or AI data. This limits the risk of unauthorized access through exposed or misused credentials.

Require Secure Transfer and Network Isolation: Enforce HTTPS-only connections and implement network access restrictions using private endpoints, service endpoints, or network rules. This ensures encrypted data transfer and isolates Blob Storage from untrusted networks and public exposure.

Enable Immutability and Soft Delete Protection: Enable blob immutability policies and soft delete features to prevent data tampering, accidental deletion, or ransomware-driven encryption. These controls preserve data integrity and allow recovery from malicious or unintended modifications.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0007 Discovery
TA0005 Defense Evasion	TA0040 Impact	TA0010 Exfiltration	TA0009 Collection

TA0008 Lateral Movement	TA0043 Reconnaissance	TA0042 Resource Development	TA0011 Command and Control
T1526 Cloud Service Discovery	T1078 Valid Accounts	T1190 Exploit Public-Facing Application	T1593 Search Open Websites/Domains
T1594 Search Victim-Owned Websites	T1078.004 Cloud Accounts	T1595.003 Wordlist Scanning	T1595 Active Scanning
T1596 Search Open Technical Databases	T1596.001 DNS/Passive DNS	T1583.004 Server	T1593.002 Search Engines
T1583 Acquire Infrastructure	T1566.001 Spearphishing Attachment	T1566 Phishing	T1566.002 Spearphishing Link
T1078.004 Cloud Accounts	T1098 Account Manipulation	T1562.011 Spoof Security Alerting	T1562 Impair Defenses
T1562.007 Disable or Modify Cloud Firewall	T1098.001 Additional Cloud Credentials	T1528 Steal Application Access Token	T1003 OS Credential Dumping
T1040 Network Sniffing	T1580 Cloud Infrastructure Discovery	T1619 Cloud Storage Object Discovery	T1021 Remote Services
T1021.007 Cloud Services	T1074.002 Remote Data Staging	T1074 Data Staged	T1530 Data from Cloud Storage
T1105 Ingress Tool Transfer	T1567 Exfiltration Over Web Service	T1030 Data Transfer Size Limits	T1020 Automated Exfiltration
T1537 Transfer Data to Cloud Account	T1567.002 Exfiltration to Cloud Storage	T1485 Data Destruction	T1486 Data Encrypted for Impact
T1565 Data Manipulation			

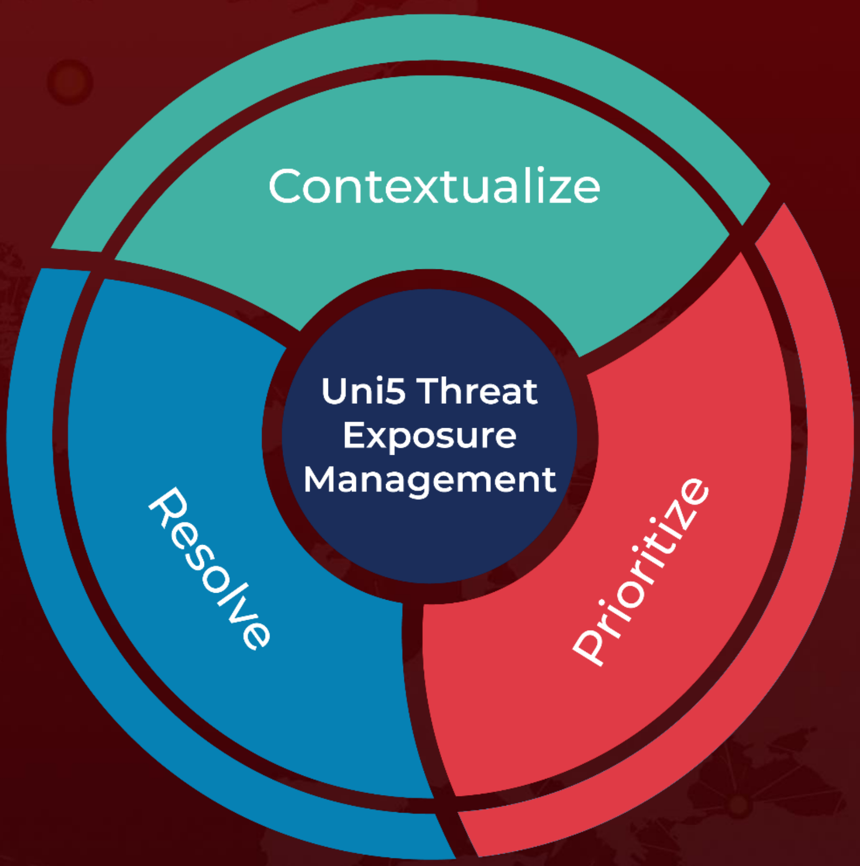
References

https://www.microsoft.com/en-us/security/blog/2025/10/20/inside-the-attack-chain-threat-activity-targeting-azure-blob-storage/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

October 23, 2025 • 2:30 AM

More at www.hivepro.com