Threat Intelligence Report

Security for the Cloud: Mitigating Risk and Vulnerabilities

Cloud environments have evolved from basic data storage solutions to comprehensive computing platforms. While increasing efficiency and productivity, cloud solutions also introduce new vulnerabilities, due in part to the vast amounts of sensitive data transmitted between organizations and cloud service providers. As a result, cyber attacks within these environments have escalated as threat actors aim to capitalize on weak credentials, misconfigurations, and human error. These security challenges pose risks to end users, whose personal data is at risk of being compromised, and organizations, whose networks and systems can be infiltrated through insecure cloud environments. Mitigating cloud-related cyber risk requires cybersecurity protocols that include identity and access management, encryption, continuous monitoring, and proper vendor due diligence.

THREAT ACTIVITY

- **Snowflake Unauthorized Access (2024):** In June 2024, the cloud-based data storage and analytics company Snowflake observed a targeted threat campaign aiming to gain unauthorized access to customer accounts. Snowflake believes the attackers exploited already-stolen customer credentials, likely obtained through previous breaches or infostealer malware infections, to access to Snowflake environments lacking multi-factor authentication (MFA). FTI Cybersecurity investigations into client Snowflake environments corroborated these reports, and shed additional light on threat actor activity within compromised environments.[1]
- **Microsoft Azure Active Directory Exploit (2023):** In early 2023, a security flaw in Microsoft Azure Active Directory (AD) was discovered. This vulnerability allowed attackers to manipulate Azure AD Connect to gain unauthorized access to cloud resources. By exploiting this flaw, attackers could bypass multi-factor authentication (MFA) and potentially gain control over Azure environments, posing significant risks to organizations relying on Azure AD for identity management.
- **Google Cloud Platform (GCP) BigQuery Exfiltration:** In March 2023, a significant security incident occurred due to a misconfiguration in the access controls of BigQuery datasets managed by a large financial services company. This error allowed public access to sensitive financial data, which attackers exploited to exfiltrate customer information and transaction records over several weeks. The breach was detected through unusual data access patterns, prompting immediate corrective action.
- **Amazon Web Services (AWS) Lambda Code Injection:** In 2023, a vulnerability in AWS Lambda was exploited to inject unauthorized code into serverless environments. Attackers used this vulnerability to execute malicious actions, such as data theft and unauthorized access to other cloud resources. The incident was discovered when unusual function behavior and unexpected resource access were detected.

THREAT ASSESSMENT

Cloud breaches can result in business disruption, loss of consumer trust, regulatory penalties, and other financial implications. Cloud environments are targets for both cybercriminal threat actors, who aim to exfiltrate sensitive data and extort victims for profit, and state-sponsored advanced persistent threat actors, who may seek access to cloud environments for intelligence collection purpose. Threat actors can exploit cloud vulnerabilities through: User Account Takeovers, Misconfigurations, Vulnerable, Public APIs, and Third-Party Vendors.

RECOMMENDED ACTION

Organizations should conduct regular cloud security assessments to ensure alignment with industry standards and best practices surrounding:

- **Identity and Access Management:** Implement the least privilege strategy and enable multi-factor authentication (MFA) for all cloud-based accounts
- **Logging:** Properly manage and review logs to identify abnormalities
- **Storage:** Ensure encryption is enabled for all types of storage and implement proper storage policies to safeguard the sensitive data
- **Monitoring:** Continuously monitor for threats and stay up-to-date on the latest cybersecurity risks and intelligence reports
- **Networking:** Ensure networks are properly segmented and encrypted within the cloud environment

[1] See Emerging Threat: Unauthorized Access to Snowflake Customer Accounts Lacking Multi-Factor Authentication for more information.

SOURCES

Sources include open-source information from public and private industry reporting.

- CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices
- Azure AD 'Log in With Microsoft' Authentication Bypass Affects Thousands
- Cloud Data Exfiltration via GCP Storage Buckets and How to Prevent It
- Lambda Threat – Best Practices for Lambda Security
- Snowflake Forums: Detecting and Preventing Unauthorized User Access
- Snowflake Recommends Customers Take Steps to Prevent Unauthorized Access

Why FTI Cybersecurity

MULTIDISCIPLINARY EXPERTISE

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

GLOBALLY POSITIONED

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

INTEGRATED & COMPREHENSIVE

Comprehensive services include crisis communications, e-discovery, forensic investigations, and more

Seamless integration of FTI Consulting's expertise across service offerings

FTI Cybersecurity Global Offices

AMERICAS

Atlanta
Boston
Chicago
Dallas
Houston
Irvine
Los Angeles
Mexico City
Miami
New York
Philadelphia
Roseland
San Francisco
Sao Paulo
Seattle
Toronto
Washington, DC
Wayne

EMEA

Berlin
Brussels
Cape Town
Dubai
Dublin
Dusseldorf
Frankfurt
Johannesburg
London
Madrid
Mumbai
Munich
Paris
Zurich

APAC

Brisbane
Hong Kong
Melbourne
Perth
Shanghai
Singapore
Sydney
Tokyo

CONTACT FTI CYBERSECURITY

Email: #fticybersecurity@fticonsulting.com

Phone: +1-844-CYBR-FTI (+1-844-292-7384)

FTI CONSULTING