SLIDE SHOW

Breach Files: Non-Human Identity Edition

aembit

CASE FILE 01

The New York Times

DISCLOSED: JUNE 2024

SOURCE CODE LEAK

Internal source code and data belonging to the news organization was leaked on the 4chan message board after being stolen from the company's GitHub repositories.

- 273GB archive containing 5,000 repositories and 3.6 million files, including source code for Wordle.
- Exposed data included a WordPress database with user information, authentication URLs, API tokens, and secret keys.
- Breach occurred due to an exposed GitHub token.

aembit

SOURCE CODE LEAK The New York Times

Response

Confirmed no unauthorized access to Times-owned systems or impact on operations.

Implemented continuous monitoring for anomalous activity.

CASE FILE 02

Hugging Face

DISCLOSED: JUNE 2024

EXPOSED ACCESS TOKENS VIA UNAUTHORIZED ACCESS

The popular AI platform experienced a breach resulting in the theft of authentication tokens.

- Tokens were exposed on public repositories like GitHub.
- Researchers from Lasso Security identified 1,681 valid tokens, some with write permissions.
- Potential manipulation of AI models and data for major organizations like Microsoft, Google, and VMware.

aembit

EXPOSED ACCESS TOKENS VIA UNAUTHORIZED ACCESS Hugging Face

Response

- Invalidated compromised tokens and enhanced security protocols.
- Advised users to avoid publishing tokens in public code.
- Collaborated with EleutherAI and Stability AI to develop new checkpointing formats.

CASE FILE 03

Dropbox

DISCLOSED: MAY 2024

AUTHENTICATION TOKEN THEFT

The file-sharing service reported a breach affecting its Dropbox Sign service, where a compromised service account granted unauthorized access.

- Exploited an automated system configuration tool.
- Accessed customer data: emails, usernames, phones, passwords, API keys, tokens, MFA details.

aembit

SERVICE ACCOUNT COMPROMISE

Dropbox

Response

- Reset passwords and logged out users.
- Initiated API key rotations.
- Commenced ongoing forensic investigation and customer support.

CASE FILE 04

sisense

DISCLOSED: APRIL 2024

GITLAB REPOSITORY COMPROMISE

The business intelligence company disclosed a breach impacting its Fusion Managed Cloud product, with attackers accessing GitLab repositories.

- Exfiltrated Amazon S3 buckets and terabytes of customer data: access tokens, passwords, SSL certificates.
- U.S. CISA involved due to potential critical infrastructure impacts.

Response

- Rotated all authentication credentials.
- Enhanced security monitoring and restricted firewall ports.
- Supported customers with password resets, API key rotations, and SSO updates.

CASE FILE 05

CLOUDFLARE

DISCLOSED: FEBRUARY 2024

AUTHENTICATION TOKEN THEFT

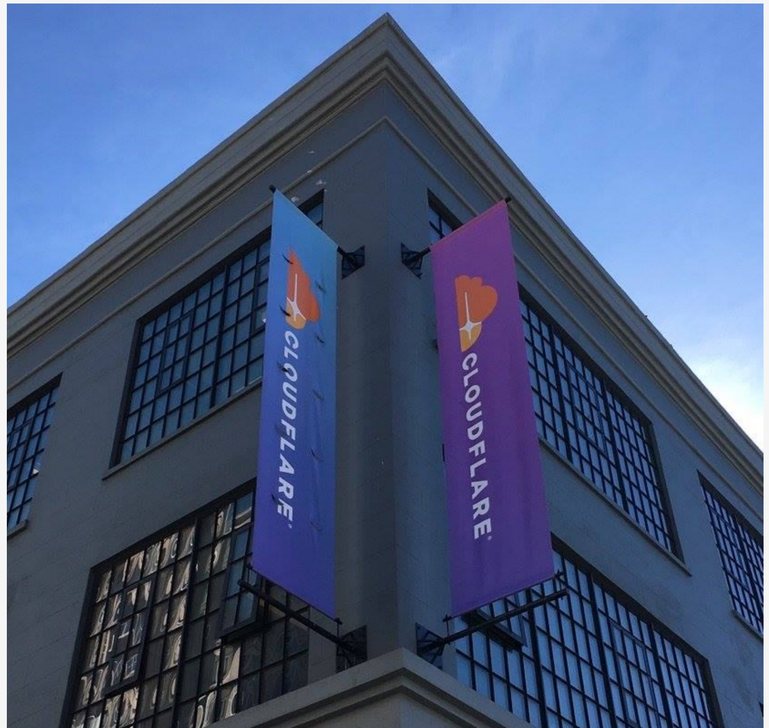
The connectivity cloud company faced a nation-state attack due to stolen service tokens and account credentials from a previous Okta breach.

- Unwarranted access to Atlassian software, Jira instance, Bitbucket, and AWS environment.
- Attack aimed to gather intelligence for future actions.

CLOUDFLARE

Response

- Rotated 5,000+ production credentials.
- Segmented test and staging systems.
- Conducted forensic examinations and rebooted all systems.



CASE FILE 06

Microsoft

DISCLOSED: JANUARY 2024

OAUTH APPLICATION ABUSE

The software giant thwarted a sophisticated attack by the Russian state-sponsored group, Midnight Blizzard, using malicious OAuth apps.

- Attackers used password spray tactics to exploit accounts without MFA.
- Targeted service accounts, compromising workload identities.

aembit

OAUTH APPLICATION ABUSE

Microsoft

Response

- Audited identity privileges.
- Tightened conditional access controls.
- Enhanced anomaly detection for OAuth apps.

CASE FILE 07

sumo logic

AWS CREDENTIAL COMPROMISE

DISCLOSED: NOVEMBER 2023

The cloud and log monitoring provider's AWS account was breached using stolen credentials.

- Method of credential theft undisclosed (likely phishing, weak passwords, or previous leaks).
- Company systems and encrypted customer data remained unaffected.

aembit

AWS CREDENTIAL COMPROMISE

sumo logic

Response

- Secured compromised infrastructure.
- Rotated potentially exposed credentials.
- Advised customers to reset API keys and other shared credentials.

CASE FILE 08

circleci

DISCLOSED: DECEMBER 2022

APPLICATION KEY THEFT

The continuous integration and continuous delivery (CI/CD) platform maker suffered a supply chain attack when an engineer's laptop was compromised.

- Malware bypassed anti-virus, stole session cookies, and accessed databases.
- Extracted tokens and keys from customer organizations.

aembit

APPLICATION KEY THEFT

circleci

Response

- Implemented mandatory secret rotations.
- Established new authentication barriers.
- Plans for automatic OAuth token rotations.

CASE FILE 09

Uber

HARDCODED CREDENTIALS

DISCLOSED: SEPTEMBER 2022

An 18-year-old hacker infiltrated the transportation company's systems using hardcoded credentials found in a PowerShell script.

- Gained admin access to Thycotic PAM platform.
- Accessed AWS console, VMware vSphere, and Google Workspace admin dashboard.

aembit

UBER HARDCODED CREDENTIALS

Uber

Response

Increased scrutiny on stored credentials.

Enhanced security protocols and monitoring.

7 Tips for Securing Non-Human Credentials

01

Inventory All Workload Credentials

Identifies credential sprawl and high-risk areas, especially on platforms like GitHub.

02

Monitor and Log Workload Activity

Detects suspicious behavior and over-privileged accounts.

03

Automate Credential Rotation

Keeps credentials up to date and limits the window of attacker opportunity.

04

Validate Workload Identity

Confirms legitimacy before accessing resources.

05

Remove Hard-Coded Secrets

Allows reliance on dynamic, policy-based credentials instead.

06

Enforce Conditional Access

Permits access only to workloads meeting certain security criteria.

07

Implement Workload IAM

Generates short-lived access tokens to accomplish all the above tips in one solution.

Manage Access, Not Secrets.

Aembit is the Workload Identity Platform that lets every business safely build its next generation of applications by inherently trusting how it connects to partners, customers, and foundational services. Aembit provides seamless and secure access from your workloads to the services they depend on, like APIs, databases, and cloud resources, while simplifying application development, delivery, compliance, and audit. For more information visit aembit.io

aembit