LastPass•••|

LASTPASS BREACH ANALYSIS

THROUGH THE LENS OF IAM OPERATIONS

1st Identity & Access Breach

Aug 8: Attacker gained access to S3 bucket containing source code folder and an encrypted backup folder of LastPass customer data

Shadow Access Problem

Identity with over-permissioned access

IAM OPS BEST PRACTICE

- Continuously monitor the provisioned access risk and policies associated with an identity and remove unused or dormant access and excessive access permissions.

Data Exfiltration

Aug 12: Attacker exfiltrates source code and encrypted LastPas customer data (without master key)

Shadow Access Problem

Anomalous activity of identity moving data

IAM OPS BEST PRACTICE

- Look for a drift in actions or permissions of a possibly over-privileged identity with access to critical data assets and set notifications via some webhook framework such as Slack.

2nd Identity & Access Breach

Oct 26: Attacker targets DevOps engineer identity, installs keylogger and exfiltrates all keys inside secret vault

Shadow Access Problem

Compromised identity and unauthorized access

IAM OPS BEST PRACTICE

- Track permissions for roles providing cross account access to federated identities.
- Follow just in time governance for IAM roles that have access to services such as KMS and secret vaults and ensure keys are periodically rotated.
- Generate reports every 24 hours to monitor access to the KMS and avoid using permanent secret/access keys for any orchestration/ backup platforms storing the key-value pairs.
- Keep track of who has access to what and what actions manifest into weak links.

STACK IDENTITY
www.stackidentity.com