ermetic

Misconfigurations Leading to AWS S3 Ransomware Exposure

Ermetic recently researched ransomware exposure of misconfigured S3 buckets. We sought scenarios with all the following: an identity had a permissions combination that threat actors could exploit to perform ransomware, the identity had at least one risk factor that made it vulnerable to compromise and effective S3 risk mitigation was not applied.

90% or more

Every environment surveyed had 1 or more identities with a permissions combo that allowed them to perform ransomware on ≥90% of the S3 buckets in at least 1 AWS account.

More than **70%**

More than 70% of the environments had machines that were publicly exposed and linked to identities whose permissions could be exploited to perform ransomware.

Identities and Permissions are Leading Risk Factors

Almost **80%**

had misconfigured IAM users with enabled access keys not used for 180+ days and whose permissions enabled them to perform ransomware

Almost **60%**

had misconfigured IAM users with console access without MFA required at login and whose permissions enabled them to perform ransomware

Almost **45%**

had misconfigured 3rd-party identities that could elevate their own privileges to admin level and then perform ransomware

S3 Ransomware Execution Vectors

We defined the execution vectors that a malicious actor could use to successfully wage a ransomware attack — one-off or even a full campaign. We then translated those scenarios into the combinations of permissions that would make the attack vector possible.

Access and Destroy

Resource-Based Policy Denial of Service for KMS Keys

Bucket Privilege Escalation

Mitigation Strategies

Least Privilege Access as a Strategy

A very effective way to prevent malicious actors from attacking your environment is to not assign unnecessary access. By granting the minimum of permissions that legitimate users need to perform their jobs, you also minimize the blast radius from a hack.

Removing Risk Factors

"Easy wins" like rotating access keys, enabling MFA and disabling unused credentials can reduce the chance of exploited identities.

Logging and Monitoring

Enable AWS CloudTrail on buckets that matter most. Use AWS event selectors for more granular logging control. Set up rules to detect unusual or suspicious behavior.

Preventing Malicious Deletion

AWS S3 built-in mechanisms that may prevent deletion of objects or versions: object locking for a retention period or a legal hold, or MFA-delete.

Replicating Buckets

AWS offers a built-in mechanism for replicating buckets to different S3 buckets for backup purposes and to mitigate malicious delete operations.

www.ermetic.com