CYBERCRIME IS ON THE RISE...

CLOUD SECURITY ADVOCATES UNITE

SHILPI BHATTACHARJEE ASHISH RAJAN

CLOUDSECURITYPODCAST.TV

NOV '22

TOP 5 AWS SECURITY VILLAINS

AND HOW TO AVOID THEM

Adopting Amazon Web Services — the dominant Cloud Service Provider — can help organizations innovate faster and accelerate their digital transformation. But there are common security pitfalls when moving to AWS, and steps your team can take to avoid them.

MISCREDS

OR LEAKED CREDENTIALS

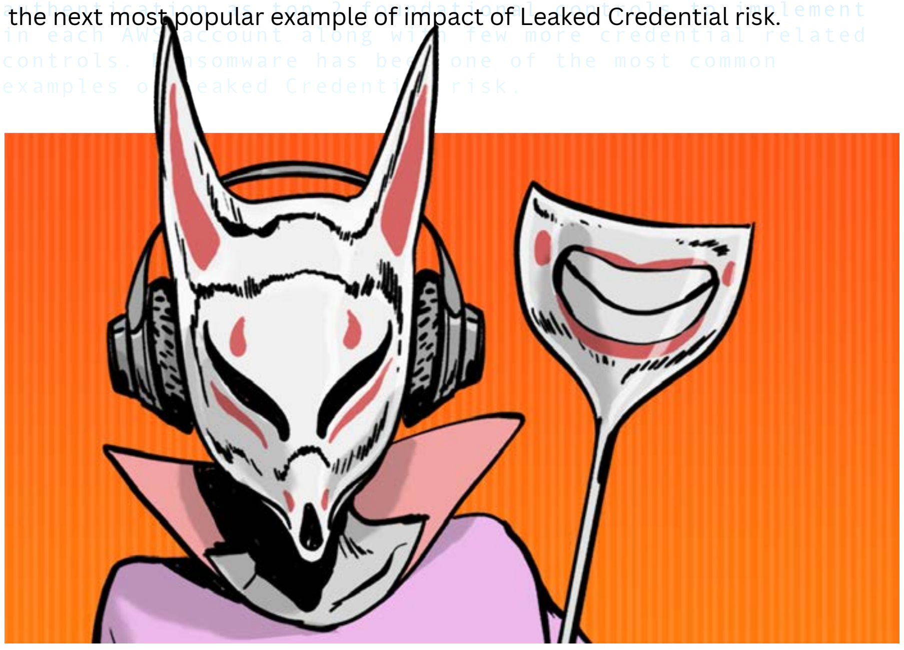
Identity is the new perimeter in the public cloud like AWS and exposure of credentials or compromised credentials linked to these identities to external malicious actors have been found to be the most common reason for most data breaches. The CIS Benchmark for AWS lists - avoiding the use of root user (administrator account) and usage of Multi-factor authentication as top 2 foundational controls to implement in each AWS account along with few more credential related controls. Outside of Data breaches, Ransomware is the next most popular example of impact of Leaked Credential risk.

authentication as top 2 foundational controls to implement in each AWS account along with few more credential related controls. Ransomware has been one of the most common examples of Leaked Credential risk.

ABRACONFDABRA

OR INSECURE RESOURC CONFIGURATION

With the migration of applications & storage to cloud for cost savings and digitization projects due to digital transformation being exercised at large scale in enterprises globally, the resources that were behind the closed doors of hardware firewall are at the mercy of software misconfiguration that can modify the infrastructure definition being developed as code to become vulnerable. This leads to Cloud Workload or resource hosted in AWS exposed to the internet. An AWS S3 bucket left open to the internet is one of the most common examples of Cloud resource Misconfigurations which has got a lot of public coverage.



CON-IDENTITY

OR IDENTIFICATION AND AUTHENTICATION FAILURES

Linked closely to Leaked credentials and insecure Resource Configuration is the business logic of the applications themselves that are running with either weak/no authentication or bad session management which leaves the application vulnerable to both internal malicious users, external attackers and vulnerable third parties with exploited vulnerabilities. Unauthenticated Access to services behind an unauthenticated APIs have been identified as common examples of the risk.

SUBDOMINE

OR DANGLING DNS

A DNS entry for your organization website asset that points to a de-provisioned resource in a public cloud like AWS can be taken over simply by provisioning the same resource with the same name in the attacker's AWS Account. There are not a lot of examples of breaches caused by this as these are classified more as reputational risk and malicious actors who squat DNS entries exposed to sub-domain takeover until they are discovered. Technically unless the organization is keeping a close eye of each of the DNS entries and its content these types of risks usually exist in environments for a long time before they get discovered with potential long term risk impacts.

WHOIAM

OR LACK OF CONTROL

With 94% of organizations using large scale cloud accounts, Role Based Access Control which has been a known challenge to achieve in normal circumstances in large organizations is a harder challenge to solve now in a remote first world with no trust boundaries and without consistent validation of whether each identity has the right access for the credentials. Identity credential is the most important piece of data in Cloud which could makes it the #1 Risk: most organizations must work towards improving. Without appropriate role based access control the potential to reduce the attack surface exposed to an external attacker. CIS benchmark for AWS lists not having * permission as a control and a common example of this hack has been the SSRF vulnerabilities exploited by a rogue AWS employee for Capital One breach in 2019.