radware

ANATOMY OF A CLOUD-NATIVE DATA BREACH

DISSECTING A REAL-WORLD CLOUD DATA BREACH AND HOW IT COULD HAVE BEEN AVOIDED

Migrating computing resources to cloud environments opens up new attack surfaces previously unknown in the world of premise-based data centers. As a result, cloud-native data breaches frequently have different characteristics and follow a different progression than physical data breaches. Here is a real-life example of a cloud-native data breach, how it evolved and how it possibly could have been avoided.

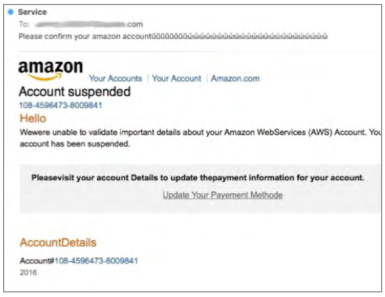
TARGET PROFILE: A SOCIAL MEDIA/MOBILE APP COMPANY

The company is a photo-sharing social media application, with over 20 million users. It stores over 1PB of user data within Amazon Web Services (AWS), and in 2018, it was the victim of a massive data breach that exposed nearly 20 million user records. This is how it happened.

STEP 1

COMPROMISING A LEGITIMATE USER[1]

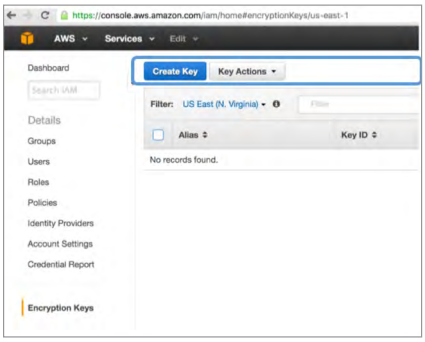
Frequently, the first step in a data breach is that an attacker compromises the credentials of a legitimate user. In this incident, an attacker used a spear-phishing attack to obtain an administrative user's credentials to the company's environment.



STEP 2

FORTIFYING ACCESS

After compromising a legitimate user, a hacker frequently takes steps to fortify access to the environment, independent of the compromised user. In this case, the attacker connected to the company's cloud environment through an IP address registered in a foreign country and created API access keys with full administrative access.

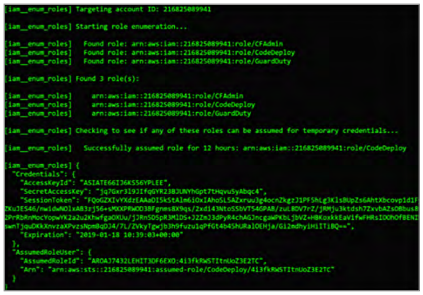


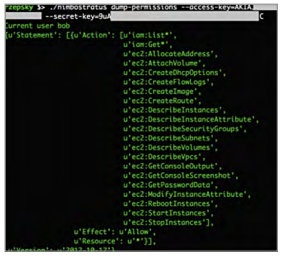
1 The information presented in this document is based on the breach disclosure details provided by the company on its website. The accompanying screenshots are for illustration only and are not screenshots of the actual incident.

STEP 3

RECONNAISSANCE

Once inside, an attacker then needs to map out what permissions are granted and what actions this role allows.

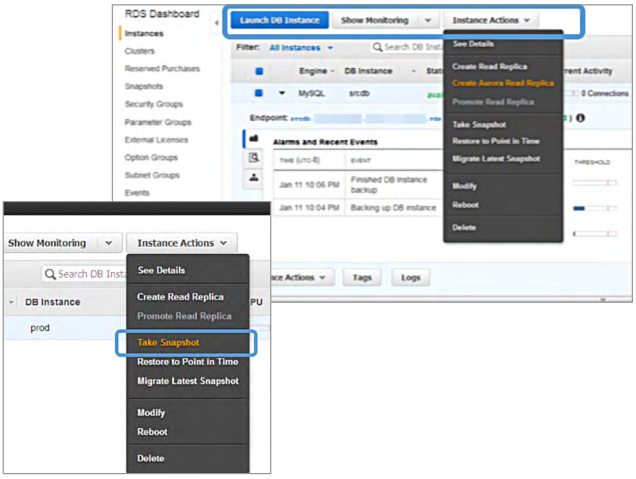




STEP 4

EXPLOITATION

Once the available permissions in the account have been determined, the attacker can proceed to exploit them. Among other activities, the attacker duplicated the master user database and exposed it to the outside world with public permissions.



STEP 5

EXFILTRATION

Finally, with customer information at hand, the attacker copied the data outside of the network, gaining access to over 20 million user records that contained personal user information.

LESSONS LEARNED

- **Your Permissions Equal Your Threat Surface:** Leveraging public cloud environments means that resources that used to be hosted inside your organization's perimeter are now outside where they are no longer under the control of system administrators and can be accessed from anywhere in the world. Workload security, therefore, is defined by the people who can access those workloads and the permissions they have. In effect, your permissions equal your attack surface.

- **Excessive Permissions Are the No. 1 Threat:** Cloud environments make it very easy to spin up new resources and grant wide-ranging permissions but very difficult to keep track of who has them. Such excessive permissions are frequently mischaracterized as misconfigurations but are actually the result of permission misuse or abuse. Therefore, protecting against those excessive permissions becomes the No. 1 priority for securing publicly hosted cloud workloads.

- **Cloud Attacks Follow Typical Progression:** Although each data breach incident may develop differently, a cloud-native attack breach frequently follows a typical progression of a legitimate user account compromise, account reconnaissance, privilege escalation, resource exploitation and data exfiltration.

WHAT COULD HAVE BEEN DONE DIFFERENTLY

- **Protect Your Access Credentials:** Your next data breach is a password away. Securing your cloud account credentials — as much as possible — is critical to ensuring that they don't fall into the wrong hands.
- **Limit Permissions:** Frequently, cloud user accounts are granted many permissions that they don't need or never use. Exploiting the gap between granted permissions and used permissions is a common move by hackers. In the aforementioned example, the attacker used the accounts' permissions to create new administrative-access API keys, spin up new databases, reset the database master password and expose it to the outside world. Limiting permissions to only what the user needs helps ensure that, even if the account is compromised, the damage an attacker can do is limited.
- **Alert of Suspicious Activities:** Since cloud-native data breaches frequently have a common progression, there are certain account activities — such as port scanning, invoking previously used APIs and granting public permissions — which can be identified. Alerting against such malicious behavior indicators (MBIs) can help prevent a data breach before it occurs.
- **Automate Response Procedures:** Finally, once malicious activity has been identified, fast response is paramount. Automating response mechanisms can help block malicious activity the moment it is detected and stop the breach from reaching its end goal.

HOW RADWARE CAN HELP YOU

Radware's Cloud Native Protector provides an agentless cloud-native solution for comprehensive protection of AWS assets. It uniquely protects both the overall security posture of the cloud environment and individual cloud workloads, and protects against cloud-native attack vectors.

Radware analyzes the gap between defined permissions and permissions that are actually being used. This helps detect excessive permissions that might leave you exposed and provides smart hardening recommendations based on the principle of least privilege.

To protect against data breaches, Radware uses machine learning algorithms to detect malicious behavior in your account and places events in contextual attack storylines to detect potential attacks and block them as they evolve. Finally, Radware's solution includes automated response mechanisms, so you block data theft activities as soon as they are detected and ensure that your data isn't compromised.

CONTACT US TO LEARN HOW RADWARE'S **CLOUD NATIVE PROTECTOR** CAN HELP PROTECT YOU!