The 3 most popular attacks targeting clouds today

Both the security capabilities of the cloud platforms are becoming more and more complete, but not without vulnerabilities.

According to CSO, more than 80% of organizations and businesses have been using services from 2 or more public cloud infrastructure providers, and nearly 2/3 of them It is using the service of 3 or more providers.

Switch to cloud environment has been and is a trend of digitalization on a global scale. But besides the obvious benefits, organizations also face the risk of falling victim to data breaches, malware attacks and many other security risks.

Both the security capabilities of cloud platforms are becoming more and more complete, but not without vulnerabilities. For example, the recent 'Cloud Snooper' attack, which used rootkits to push malicious traffic through an AWS client, bypassed the firewall platform of the cloud platform before it was distributed. Remote access trojan on platform.

So, are there any ways for hackers to exploit holes in the cloud and access data of organizations and businesses?

API attack

Leaking API credentials or misconfigured API credentials is one of the common vulnerabilities that pave the way for hackers to gain access to cloud platforms. Once an attacker gains one of the access keys, they use it to gain access and control over the server, then make an API call for malicious activities or escalate system privileges. . Normally, the keys will be leaked / shared via GitHub, BitBucket . in the form of shared images and

snapshots.

The recent data breach affecting more than 6.5 million Israeli citizens is a prime example of this type of attack.

Revealing an API key can also be a mistake by the developers as happened to Starbuck. If the API keys are exposed and fall into the hands of hackers, they will have access to internal systems and manipulate the authorized user list.

The biggest API leak was reported in March 2019, when a team of security researchers discovered 100,000 GitHub repositories with API token leaks and cryptographic keys, freely accessible in a period of 6 months, causing heavy losses to related organizations.

Wrong configuration

Misconfigured databases and servers are one of the common causes behind many cloud security disasters.

Cloud-based resources are complex and constantly changing, making it difficult for system administrators to configure. Hackers, especially sponsored groups, always target misconfigured vulnerabilities on cloud servers to deploy ransomware and backdoors to exploit cryptocurrencies or steal sensitive data. Some of the major cloud servers that have fallen victim to this attack include Oracle's Weblogic server, Atlassian Confluence, and Microsoft Exchange email server.

Server-side spoofing (SSRF)

SSRF (Server Side Request Forgery) - a server-side request forgery - is an attack that allows hackers to change parameters used on web applications to make or control requests from vulnerable servers. attack.

SSRF is a form of attack that has been on the rise recently, with real access to configuration access, logs, logins and many other types of data in the cloud infrastructure.

The recent massive data breach targeting Capital One shows the potential and risk of SSRF. Attackers successfully deployed a large-scale SSRF campaign to capture AWS credentials, then used this data to steal the personal information of more than 100 million Capital One customers.