COMMON CLOUD THREATS: CREDENTIAL THEFT

REQUEST CLOUD SECURITY ASSESSMENT

David Puzas - January 12, 2023

What is Credential Theft?

Credential theft is the act of stealing personal information such as usernames, passwords and financial information in order to gain access to an online account or system. It is a form of identity theft and can involve the use of malicious software or phishing techniques.

In cloud environments, identity is the new perimeter. Threat actors are well aware of this and target credentials to compromise cloud environments and steal enterprise data. Controlling access to cloud workloads and services is fundamental to cloud security, and organizations must prioritize the prevention of credential theft to secure access to cloud assets.

Gaining credentials allows attackers to impersonate the account owner and appear as someone who has legitimate access, such as an employee, contractor, service account or third-party supplier. Because the attacker looks like a legitimate user, this type of attack is challenging for defenses to detect. Threat actors can then use their access to expand their foothold in the targeted organization.

Common Causes of Credential Theft

1. Malware

Malicious programs can infect users' devices and steal credentials. Malware can be installed on the machines of unsuspecting users via techniques such as drive-by downloads and social engineering.

2. Phishing

Phishing attacks often abuse trust in popular brands to trick victims into giving up their credentials. Typically, they will use an enticing email to lure the recipient into visiting a malicious website where they enter their credentials.

3. Weak passwords or password reuse

Attackers take advantage of poor password security practices to gain access to systems, applications and data. Weak passwords are easier for attackers to crack, and reusing passwords increases the risk that a single stolen password could lead to a broader compromise.

4. Attacks on cloud services leading to lateral movement

Attacks against the cloud environment can lead to threat actors gaining access to on-premises systems and resources. These attacks can leverage accounts with excessive permissions to broaden their reach inside the victim's IT infrastructure.

5. Man-in-the-middle (MitM) attacks

These attacks occur when a threat actor is able to intercept and relay communications between two parties that believe they are communicating with each other. MitM attacks allow attackers to steal credentials and eavesdrop on that communication.

LEARN MORE

A complete cloud security strategy must mitigate risk, defend against threats, and overcome challenges for your business to use the cloud to grow securely.

12 Cloud Security Challenges, Risks, Threats >

Credential Theft Attack Example

In an age of remote workers and cloud computing, credential theft has emerged as **a common tactic for initial entry** as well as a means to pivot around a compromised network after threat actors are already inside.

Threat actors routinely host fake authentication pages to harvest legitimate authentication credentials for cloud services such as Microsoft Office 365 (O365), Okta or webmail accounts. They then use these credentials to attempt to access victim accounts.

Access to cloud-hosted email or file-hosting services can also facilitate espionage and theft of information. In April 2021, CrowdStrike observed **COSMIC WOLF (a Turkey-affiliated threat actor) targeting victim data stored within a large cloud service provider (CSP) environment.** The adversary compromised the environment via a stolen credential that allowed the operator to interact with the CSP using the command line. Employing this technique, the adversary altered security group settings to allow direct SSH access from malicious infrastructure.

What You Can Do TO Prevent Credential Theft

1. Enable and require multifactor authentication (MFA)

MFA requires a user to present two or more pieces of evidence to verify and authenticate their identity before they are granted the access they are requesting. MFA techniques raise the barrier to entry for attackers by preventing them from compromising applications and systems with a single password.

2. Conduct security awareness training against phishing

Knowledge is power. By training users to recognize phishing attacks and social engineering schemes, organizations can turn their employees into a critical layer of defense for their IT environment.

3. Maintain good password hygiene

Strong passwords are more difficult for attackers to crack. These passwords should be rotated regularly and should not be shared between users. Additionally, users should refrain from using the same password across multiple sites or services.

4. Use a cloud infrastructure entitlement management (CIEM) solution

CIEM solutions help enterprises manage entitlements across all of their cloud infrastructure resources. The primary goal of tools like CrowdStrike Falcon Cloud Security™ which includes CIEM capabilities, is to mitigate the risk that comes from the unintentional and unchecked granting of excessive permissions to cloud resources. By removing unnecessary privileges, organizations can reduce the threat posed by a compromised account.

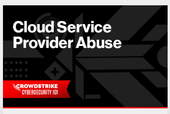
5. Properly scope permissions across users and machines

It is critical for organizations to understand the privileged access that users and devices have. Accounts that can be used to access sensitive systems, data and applications must be tightly managed to meet the security and compliance mandates of the modern enterprise.

GET TO KNOW THE AUTHOR

David Puzas is a proven cybersecurity, cloud and IT services marketer and business leader with over two decades of experience. Charged with building client value and innovative outcomes for companies such as CrowdStrike, Dell SecureWorks and IBM clients world-wide. He focuses on the optimization of computing innovation, trends, and their business implications for market expansion and growth. David is responsible for strategically bringing to market CrowdStrike's global cloud security portfolio as well as driving customer retention.

Featured Articles

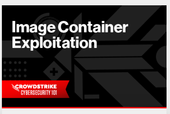


Common Cloud Threats: Cloud Service Provider Abuse

REQUEST CLOUD SECURITY ASSESSMENT

Common Cloud Threats: Cloud Vulnerability Exploitation

REQUEST CLOUD SECURITY ASSESSMENT



Common Cloud Threats: Exploitation of Misconfigured Image Containers

CLOUD THREAT REPORT