Forge Web Credentials, Technique T1606 - Enterprise

Archived: 2026-04-05 15:13:47 UTC

Adversaries may forge credential materials that can be used to gain access to web applications or Internet services. Web applications and services (hosted in cloud SaaS environments or on-premise servers) often use session cookies, tokens, or other materials to authenticate and authorize user access.

Adversaries may generate these credential materials in order to gain access to web resources. This differs from Steal Web Session Cookie, Steal Application Access Token, and other similar behaviors in that the credentials are new and forged by the adversary, rather than stolen or intercepted from legitimate users.

The generation of web credentials often requires secret values, such as passwords, Private Keys, or other cryptographic seed values.[1] Adversaries may also forge tokens by taking advantage of features such as the `AssumeRole` and `GetFederationToken` APIs in AWS, which allow users to request temporary security credentials (i.e., Temporary Elevated Cloud Access), or the `zmprov gdpak` command in Zimbra, which generates a pre-authentication key that can be used to generate tokens for any user in the domain.[2][3]

Once forged, adversaries may use these web credentials to access resources (ex: Use Alternate Authentication Material), which may bypass multi-factor and other authentication protection mechanisms.[4][5][6]

Source: https://attack.mitre.org/techniques/T1606