Steal Web Session Cookie, Technique T1539 - Enterprise

Archived: 2026-04-05 18:27:57 UTC

An adversary may steal web application or service session cookies and use them to gain access to web applications or Internet services as an authenticated user without needing credentials. Web applications and services often use session cookies as an authentication token after a user has authenticated to a website.

Cookies are often valid for an extended period of time, even if the web application is not actively used. Cookies can be found on disk, in the process memory of the browser, and in network traffic to remote systems. Additionally, other applications on the targets machine might store sensitive authentication cookies in memory (e.g. apps which authenticate to cloud services). Session cookies can be used to bypasses some multi-factor authentication protocols.[1]

There are several examples of malware targeting cookies from web browsers on the local system.[2][3] Adversaries may also steal cookies by injecting malicious JavaScript content into websites or relying on User Execution by tricking victims into running malicious JavaScript in their browser.[4][5]

There are also open source frameworks such as `Evilginx2` and `Muraena` that can gather session cookies through a malicious proxy (e.g., Adversary-in-the-Middle) that can be set up by an adversary and used in phishing campaigns.[6][7]

After an adversary acquires a valid cookie, they can then perform a Web Session Cookie technique to login to the corresponding web application.

Source: https://attack.mitre.org/techniques/T1539