Stage Capabilities: Drive-by Target, Sub-technique T1608.004 - Enterprise

Archived: 2026-04-02 10:36:10 UTC

Adversaries may prepare an operational environment to infect systems that visit a website over the normal course of browsing. Endpoint systems may be compromised through browsing to adversary controlled sites, as in Drive-by Compromise. In such cases, the user's web browser is typically targeted for exploitation (often not requiring any extra user interaction once landing on the site), but adversaries may also set up websites for non-exploitation behavior such as Application Access Token. Prior to Drive-by Compromise, adversaries must stage resources needed to deliver that exploit to users who browse to an adversary controlled site. Drive-by content can be staged on adversary controlled infrastructure that has been acquired (Acquire Infrastructure) or previously compromised (Compromise Infrastructure).

Adversaries may upload or inject malicious web content, such as JavaScript, into websites.[1][2] This may be done in a number of ways, including:

- Inserting malicious scripts into web pages or other user controllable web content such as forum posts
- Modifying script files served to websites from publicly writeable cloud storage buckets
- Crafting malicious web advertisements and purchasing ad space on a website through legitimate ad providers (i.e., Malvertising)

In addition to staging content to exploit a user's web browser, adversaries may also stage scripting content to profile the user's browser (as in Gather Victim Host Information) to ensure it is vulnerable prior to attempting exploitation.[3]

Websites compromised by an adversary and used to stage a drive-by may be ones visited by a specific community, such as government, a particular industry, or region, where the goal is to compromise a specific user or set of users based on a shared interest. This kind of targeted campaign is referred to a strategic web compromise or watering hole attack.

Adversaries may purchase domains similar to legitimate domains (ex: homoglyphs, typosquatting, different top-level domain, etc.) during acquisition of infrastructure (Domains) to help facilitate Drive-by Compromise.

Source: https://attack.mitre.org/techniques/T1608/004