

Browser Bookmark Discovery Mitigation, Mitigation T1217 - Enterprise

Archived: 2026-04-05 12:43:28 UTC

File system activity is a common part of an operating system, so it is unlikely that mitigation would be appropriate for this technique. For example, mitigating accesses to browser bookmark files will likely have unintended side effects such as preventing legitimate software from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identification of subsequent malicious behavior. It may still be beneficial to identify and block unnecessary system utilities or potentially malicious software by using whitelisting tools, like AppLocker, or Software Restriction Policies where appropriate.

Source: <https://attack.mitre.org/mitigations/T1217>