

Hooking Mitigation, Mitigation T1179 - Enterprise

By Authorization Enforcement

Archived: 2026-04-05 17:26:30 UTC

Deprecation Warning

This type of attack technique cannot be easily mitigated with preventive controls since it is based on the abuse of operating system design features. For example, mitigating all hooking will likely have unintended side effects, such as preventing legitimate software (i.e., security products) from operating properly. Efforts should be focused on preventing adversary tools from running earlier in the chain of activity and on identifying subsequent malicious behavior.

Source: <https://attack.mitre.org/mitigations/T1179>