Compile After Delivery Mitigation, Mitigation T1500 - Enterprise

Archived: 2026-04-02 10:35:57 UTC

This type of technique cannot be easily mitigated with preventive controls or patched since it is based on the abuse of operating system design features. For example, blocking all file compilation may have unintended side effects, such as preventing legitimate OS frameworks and code development mechanisms from operating properly. Consider removing compilers if not needed, otherwise 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/T1500