Boot or Logon Autostart Execution: Shortcut Modification, Sub-technique T1547.009 - Enterprise

Archived: 2026-04-05 17:02:12 UTC

Adversaries may create or modify shortcuts that can execute a program during system boot or user login. Shortcuts or symbolic links are used to reference other files or programs that will be opened or executed when the shortcut is clicked or executed by a system startup process.

Adversaries may abuse shortcuts in the startup folder to execute their tools and achieve persistence.[1] Although often used as payloads in an infection chain (e.g. Spearphishing Attachment), adversaries may also create a new shortcut as a means of indirection, while also abusing Masquerading to make the malicious shortcut appear as a legitimate program. Adversaries can also edit the target path or entirely replace an existing shortcut so their malware will be executed instead of the intended legitimate program.

Shortcuts can also be abused to establish persistence by implementing other methods. For example, LNK browser extensions may be modified (e.g. Browser Extensions) to persistently launch malware.

Source: https://attack.mitre.org/techniques/T1547/009