Command and Scripting Interpreter: AutoHotKey & AutoIT, Sub-technique T1059.010 - Enterprise

Archived: 2026-04-05 16:27:46 UTC

Adversaries may execute commands and perform malicious tasks using AutoIT and AutoHotKey automation scripts. AutoIT and AutoHotkey (AHK) are scripting languages that enable users to automate Windows tasks. These automation scripts can be used to perform a wide variety of actions, such as clicking on buttons, entering text, and opening and closing programs.[1][2]

Adversaries may use AHK (`.ahk`) and AutoIT (`.au3`) scripts to execute malicious code on a victim's system. For example, adversaries have used for AHK to execute payloads and other modular malware such as keyloggers. Adversaries have also used custom AHK files containing embedded malware as Phishing payloads.[3]

These scripts may also be compiled into self-contained executable payloads (`.exe`).[1][2]

Source: https://attack.mitre.org/techniques/T1059/010