Obtain Capabilities: Code Signing Certificates, Sub-technique T1588.003 - Enterprise

Archived: 2026-04-05 16:24:23 UTC

Adversaries may buy and/or steal code signing certificates that can be used during targeting. Code signing is the process of digitally signing executables and scripts to confirm the software author and guarantee that the code has not been altered or corrupted. Code signing provides a level of authenticity for a program from the developer and a guarantee that the program has not been tampered with.[1] Users and/or security tools may trust a signed piece of code more than an unsigned piece of code even if they don't know who issued the certificate or who the author is.

Prior to Code Signing, adversaries may purchase or steal code signing certificates for use in operations. The purchase of code signing certificates may be done using a front organization or using information stolen from a previously compromised entity that allows the adversary to validate to a certificate provider as that entity. Adversaries may also steal code signing materials directly from a compromised third-party.

Source: https://attack.mitre.org/techniques/T1588/003