System Location Discovery, Technique T1614 - Enterprise

Archived: 2026-04-05 18:05:50 UTC

Adversaries may gather information in an attempt to calculate the geographical location of a victim host. Adversaries may use the information from System Location Discovery during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

Adversaries may attempt to infer the location of a system using various system checks, such as time zone, keyboard layout, and/or language settings.[1][2][3] Windows API functions such as `GetLocaleInfoW` can also be used to determine the locale of the host.[1] In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.[4][5]

Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.[6][2]

Source: https://attack.mitre.org/techniques/T1614