# Detection Strategy for System Location Discovery, Detection Strategy DET0043

Archived: 2026-04-05 14:49:39 UTC

### AN0119

Unusual process or API usage attempting to query system locale, timezone, or keyboard layout (e.g., calls to GetLocaleInfoW, GetTimeZoneInformation). Detection can be enhanced by correlating with processes not typically associated with system configuration queries, such as unknown binaries or scripts.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| ParentProcessAllowList | Defines trusted processes expected to call locale APIs. Deviations may indicate adversarial activity. |
| TimeWindow | Specifies correlation window for API calls and suspicious process execution (e.g., 2m). |

### AN0120

Detection of commands accessing locale, timezone, or language settings such as 'locale', 'timedatectl', or parsing /etc/timezone. Anomalous execution by unusual users or automation scripts should be flagged.

#### Log Sources

#### Mutable Elements

| Field | Description |
| --- | --- |
| UserContext | Unexpected users running location discovery commands may indicate malicious behavior. |

### AN0121

Detection of system calls or commands accessing system locale (e.g., 'defaults read -g AppleLocale', 'systemsetup -gettimezone'). Correlate with unusual parent processes or execution contexts.

#### Log Sources

**Mutable Elements**

| Field | Description |
| --- | --- |
| ExecutionPath | Restrict known binaries allowed to query system locale on macOS. |

### AN0122

Detection of queries to instance metadata services (e.g., AWS IMDS, Azure Metadata Service) for availability zone, region, or network geolocation details. Correlation with non-management accounts or non-standard workloads may indicate adversary reconnaissance.

**Log Sources**

**Mutable Elements**

| Field | Description |
| --- | --- |
| MetadataQueryAllowList | Expected services that query cloud metadata APIs. Any additional sources may be malicious. |

---