# TTP Detail – T1614.001

## TTP Information

Name: System Language Discovery

Description: Adversaries may attempt to gather information about the system language of a victim in order to infer the geographical location of that host. This information may be used to shape follow-on behaviors, including whether the adversary infects the target and/or attempts specific actions. This decision may be employed by malware developers and operators to reduce their risk of attracting the attention of specific law enforcement agencies or prosecution/scrutiny from other entities.(Citation: Malware System Language Check)

There are various sources of data an adversary could use to infer system language, such as system defaults and keyboard layouts. Specific checks will vary based on the target and/or adversary, but may involve behaviors such as [Query Registry](https://attack.mitre.org/techniques/T1012) and calls to [Native API](https://attack.mitre.org/techniques/T1106) functions.(Citation: CrowdStrike Ryuk January 2019)

For example, on a Windows system adversaries may attempt to infer the language of a system by querying the registry key <code>HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\Language</code> or parsing the outputs of Windows API functions <code>GetUserDefaultUILanguage</code>, <code>GetSystemDefaultUILanguage</code>, <code>GetKeyboardLayoutList</code> and <code>GetUserDefaultLangID</code>.(Citation: Darkside Ransomware Cybereason)(Citation: Securelist JSWorm)(Citation: SecureList SynAck Doppelgänging May 2018)

On a macOS or Linux system, adversaries may query <code>locale</code> to retrieve the value of the <code>$LANG</code> environment variable.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Avaddon
* Bazar
* BlackByte Ransomware
* Clop
* Cuba
* Cuckoo Stealer
* DEATHRANSOM
* DropBook
* Flagpro
* Gootloader
* GrimAgent
* IcedID
* LockBit 2.0
* LockBit 3.0
* MarkiRAT
* Maze
* Misdat
* Mispadu
* Neoichor
* REvil
* Ryuk
* S-Type
* SharpStage
* Spark
* StealBit
* StrelaStealer
* SynAck
* XCSSET
* Zeus Panda

## APTs (Intrusion Sets)

* BlackByte
* Ke3chang
* Malteiro