# TTP Detail – T1614

## TTP Information

Name: System Location Discovery

Description:
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](https://attack.mitre.org/techniques/T1614) 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.(Citation: FBI Ragnar Locker 2020)(Citation: Sophos Geolocation 2016)(Citation: Bleepingcomputer RAT malware 2020) Windows API functions such as <code>GetLocaleInfoW</code> can also be used to determine the locale of the host.(Citation: FBI Ragnar Locker 2020) In cloud environments, an instance's availability zone may also be discovered by accessing the instance metadata service from the instance.(Citation: AWS Instance Identity Documents)(Citation: Microsoft Azure Instance Metadata 2021)

Adversaries may also attempt to infer the location of a victim host using IP addressing, such as via online geolocation IP-lookup services.(Citation: Securelist Trasparent Tribe 2020)(Citation: Sophos Geolocation 2016)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Amadey
* Crimson
* Cuckoo Stealer
* DarkGate
* DarkWatchman
* Gootloader
* GrimAgent
* Raccoon Stealer
* Ragnar Locker
* SDBbot
* Saint Bot
* SocGholish

## Tools

* QuasarRAT

## APTs (Intrusion Sets)

* SideCopy
* Volt Typhoon