# TTP Detail – T1480

## TTP Information

Name: Execution Guardrails

Description: Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary’s campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019)  
  
Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.  
  
Adversaries may identify and block certain user-agents to evade defenses and narrow the scope of their attack to victims and platforms on which it will be most effective. A user-agent self-identifies data such as a user's software application, operating system, vendor, and version. Adversaries may check user-agents for operating system identification and then only serve malware for the exploitable software while ignoring all other operating systems.(Citation: Trellix-Qakbot)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Akira \_v2
* Anchor
* Apostle
* BOLDMOVE
* BPFDoor
* BitPaymer
* BlackByte Ransomware
* BoomBox
* CHIMNEYSWEEP
* DEADEYE
* DarkGate
* EnvyScout
* Exbyte
* LightSpy
* LockBit 2.0
* LockBit 3.0
* LunarLoader
* NativeZone
* ROADSWEEP
* RansomHub
* Raspberry Robin
* SUNSPOT
* Sagerunex
* ShrinkLocker
* Small Sieve
* StealBit
* StrelaStealer
* Stuxnet
* Torisma
* VaporRage

## APTs (Intrusion Sets)

* BlackByte
* Gamaredon Group