# TTP Detail – T1497

## TTP Information

Name: Virtualization/Sandbox Evasion

Description: Adversaries may employ various means to detect and avoid virtualization and analysis environments. This may include changing behaviors based on the results of checks for the presence of artifacts indicative of a virtual machine environment (VME) or sandbox. If the adversary detects a VME, they may alter their malware to disengage from the victim or conceal the core functions of the implant. They may also search for VME artifacts before dropping secondary or additional payloads. Adversaries may use the information learned from [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) during automated discovery to shape follow-on behaviors.(Citation: Deloitte Environment Awareness)

Adversaries may use several methods to accomplish [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) such as checking for security monitoring tools (e.g., Sysinternals, Wireshark, etc.) or other system artifacts associated with analysis or virtualization. Adversaries may also check for legitimate user activity to help determine if it is in an analysis environment. Additional methods include use of sleep timers or loops within malware code to avoid operating within a temporary sandbox.(Citation: Unit 42 Pirpi July 2015)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: discovery

## Malware

* Agent Tesla
* Bazar
* Bisonal
* Black Basta
* Bumblebee
* CHOPSTICK
* Carberp
* CozyCar
* Egregor
* Gelsemium
* Hancitor
* IcedID
* Kevin
* Metamorfo
* Pteranodon
* RTM
* Raspberry Robin
* Squirrelwaffle
* StoneDrill
* StrelaStealer
* XLoader

## APTs (Intrusion Sets)

* Darkhotel
* Saint Bear