# TTP Detail – T1497.001

## TTP Information

Name: System Checks

Description: Adversaries may employ various system checks 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)

Specific checks will vary based on the target and/or adversary, but may involve behaviors such as [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047), [PowerShell](https://attack.mitre.org/techniques/T1059/001), [System Information Discovery](https://attack.mitre.org/techniques/T1082), and [Query Registry](https://attack.mitre.org/techniques/T1012) to obtain system information and search for VME artifacts. Adversaries may search for VME artifacts in memory, processes, file system, hardware, and/or the Registry. Adversaries may use scripting to automate these checks into one script and then have the program exit if it determines the system to be a virtual environment.

Checks could include generic system properties such as host/domain name and samples of network traffic. Adversaries may also check the network adapters addresses, CPU core count, and available memory/drive size. Once executed, malware may also use [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) to check if it was saved in a folder or file with unexpected or even analysis-related naming artifacts such as `malware`, `sample`, or `hash`.

Other common checks may enumerate services running that are unique to these applications, installed programs on the system, manufacturer/product fields for strings relating to virtual machine applications, and VME-specific hardware/processor instructions.(Citation: McAfee Virtual Jan 2017) In applications like VMWare, adversaries can also use a special I/O port to send commands and receive output.

Hardware checks, such as the presence of the fan, temperature, and audio devices, could also be used to gather evidence that can be indicative a virtual environment. Adversaries may also query for specific readings from these devices.(Citation: Unit 42 OilRig Sept 2018)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: discovery

## Malware

* Astaroth
* Attor
* BLUELIGHT
* BadPatch
* Black Basta
* BlackByte Ransomware
* Bumblebee
* DUSTTRAP
* DarkGate
* DarkTortilla
* Denis
* Dyre
* EvilBunny
* Exbyte
* Ferocious
* FinFisher
* GoldMax
* Grandoreiro
* GravityRAT
* GuLoader
* InvisiMole
* Latrodectus
* Lucifer
* Lumma Stealer
* MegaCortex
* Mispadu
* NativeZone
* Nightdoor
* OSX\_OCEANLOTUS.D
* ObliqueRAT
* Okrum
* OopsIE
* P8RAT
* Pikabot
* PlugX
* PoetRAT
* QakBot
* ROKRAT
* Raspberry Robin
* RogueRobin
* SUNBURST
* SVCReady
* Saint Bot
* Shark
* Smoke Loader
* Snip3
* SodaMaster
* SynAck
* Trojan.Karagany
* UBoatRAT
* WastedLocker
* WhisperGate
* XLoader
* macOS.OSAMiner
* yty

## Tools

* AsyncRAT
* CSPY Downloader
* Pupy
* Remcos

## APTs (Intrusion Sets)

* Darkhotel
* Evilnum
* OilRig
* Volt Typhoon