# TTP Detail – T1497.003

## TTP Information

Name: Time Based Evasion

Description: Adversaries may employ various time-based methods to detect and avoid virtualization and analysis environments. This may include enumerating time-based properties, such as uptime or the system clock, as well as the use of timers or other triggers to avoid a virtual machine environment (VME) or sandbox, specifically those that are automated or only operate for a limited amount of time.  
  
Adversaries may employ various time-based evasions, such as delaying malware functionality upon initial execution using programmatic sleep commands or native system scheduling functionality (ex: [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)). Delays may also be based on waiting for specific victim conditions to be met (ex: system time, events, etc.) or employ scheduled [Multi-Stage Channels](https://attack.mitre.org/techniques/T1104) to avoid analysis and scrutiny.(Citation: Deloitte Environment Awareness)  
  
Benign commands or other operations may also be used to delay malware execution. Loops or otherwise needless repetitions of commands, such as [Ping](https://attack.mitre.org/software/S0097)s, may be used to delay malware execution and potentially exceed time thresholds of automated analysis environments.(Citation: Revil Independence Day)(Citation: Netskope Nitol) Another variation, commonly referred to as API hammering, involves making various calls to [Native API](https://attack.mitre.org/techniques/T1106) functions in order to delay execution (while also potentially overloading analysis environments with junk data).(Citation: Joe Sec Nymaim)(Citation: Joe Sec Trickbot)  
  
Adversaries may also use time as a metric to detect sandboxes and analysis environments, particularly those that attempt to manipulate time mechanisms to simulate longer elapses of time. For example, an adversary may be able to identify a sandbox accelerating time by sampling and calculating the expected value for an environment's timestamp before and after execution of a sleep function.(Citation: ISACA Malware Tricks)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

**•** mitre-attack: discovery

## Malware

* AppleJeus
* BADFLICK
* Bazar
* BendyBear
* Bisonal
* Bumblebee
* Clambling
* Clop
* Crimson
* DRATzarus
* DarkTortilla
* Egregor
* EvilBunny
* FatDuke
* GoldMax
* GoldenSpy
* Gootloader
* GrimAgent
* GuLoader
* HermeticWiper
* IPsec Helper
* LiteDuke
* Lokibot
* LunarWeb
* Okrum
* P8RAT
* Pony
* QakBot
* Raindrop
* RansomHub
* SUNBURST
* SVCReady
* Saint Bot
* Snip3
* SodaMaster
* StrifeWater
* ThiefQuest
* Tomiris
* TrickBot
* Ursnif
* WhisperGate
* XCSSET
* metaMain

## Tools

* Brute Ratel C4