# TTP Detail – T1124

## TTP Information

Name: System Time Discovery

Description: An adversary may gather the system time and/or time zone settings from a local or remote system. The system time is set and stored by services, such as the Windows Time Service on Windows or <code>systemsetup</code> on macOS.(Citation: MSDN System Time)(Citation: Technet Windows Time Service)(Citation: systemsetup mac time) These time settings may also be synchronized between systems and services in an enterprise network, typically accomplished with a network time server within a domain.(Citation: Mac Time Sync)(Citation: linux system time)  
  
System time information may be gathered in a number of ways, such as with [Net](https://attack.mitre.org/software/S0039) on Windows by performing <code>net time \\hostname</code> to gather the system time on a remote system. The victim's time zone may also be inferred from the current system time or gathered by using <code>w32tm /tz</code>.(Citation: Technet Windows Time Service) In addition, adversaries can discover device uptime through functions such as <code>GetTickCount()</code> to determine how long it has been since the system booted up.(Citation: Virtualization/Sandbox Evasion)  
  
On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show clock detail` can be used to see the current time configuration.(Citation: show\_clock\_detail\_cisco\_cmd) On ESXi servers, `esxcli system clock get` can be used for the same purpose.  
  
In addition, system calls – such as <code>time()</code> – have been used to collect the current time on Linux devices.(Citation: MAGNET GOBLIN) On macOS systems, adversaries may use commands such as <code>systemsetup -gettimezone</code> or <code>timeIntervalSinceNow</code> to gather current time zone information or current date and time.(Citation: System Information Discovery Technique)(Citation: ESET DazzleSpy Jan 2022)  
  
This information could be useful for performing other techniques, such as executing a file with a [Scheduled Task/Job](https://attack.mitre.org/techniques/T1053)(Citation: RSA EU12 They're Inside), or to discover locality information based on time zone to assist in victim targeting (i.e. [System Location Discovery](https://attack.mitre.org/techniques/T1614)). Adversaries may also use knowledge of system time as part of a time bomb, or delaying execution until a specified date/time.(Citation: AnyRun TimeBomb)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: discovery

## Malware

* Agent Tesla
* AppleSeed
* Astaroth
* AvosLocker
* Azorult
* BADHATCH
* BISCUIT
* BLUELIGHT
* Bazar
* BendyBear
* Bisonal
* Cannon
* Carbon
* Clambling
* ComRAT
* Conficker
* Crimson
* DCSrv
* DEADWOOD
* DRATzarus
* DUSTTRAP
* DarkGate
* DarkWatchman
* Egregor
* Epic
* EvilBunny
* FELIXROOT
* FunnyDream
* GRIFFON
* GoldMax
* Grandoreiro
* GravityRAT
* Green Lambert
* HOPLIGHT
* InvisiMole
* KEYPLUG
* Metamorfo
* MoonWind
* NOKKI
* Nightdoor
* Okrum
* OopsIE
* PipeMon
* PowerDuke
* Proxysvc
* QakBot
* RTM
* Raccoon Stealer
* SHARPSTATS
* SUNBURST
* SVCReady
* ShadowPad
* Shamoon
* ShrinkLocker
* SombRAT
* StoneDrill
* StrifeWater
* Stuxnet
* T9000
* TAINTEDSCRIBE
* Taidoor
* TajMahal
* Torisma
* UPPERCUT
* WindTail
* Zebrocy
* Zeus Panda
* build\_downer
* ccf32

## Tools

* Net
* SILENTTRINITY

## APTs (Intrusion Sets)

* BRONZE BUTLER
* CURIUM
* Chimera
* Darkhotel
* Higaisa
* Lazarus Group
* Sidewinder
* The White Company
* Turla
* Volt Typhoon
* ZIRCONIUM