# TTP Detail – T1053.002

## TTP Information

Name: At

Description: Adversaries may abuse the [at](https://attack.mitre.org/software/S0110) utility to perform task scheduling for initial or recurring execution of malicious code. The [at](https://attack.mitre.org/software/S0110) utility exists as an executable within Windows, Linux, and macOS for scheduling tasks at a specified time and date. Although deprecated in favor of [Scheduled Task](https://attack.mitre.org/techniques/T1053/005)'s [schtasks](https://attack.mitre.org/software/S0111) in Windows environments, using [at](https://attack.mitre.org/software/S0110) requires that the Task Scheduler service be running, and the user to be logged on as a member of the local Administrators group. In addition to explicitly running the `at` command, adversaries may also schedule a task with [at](https://attack.mitre.org/software/S0110) by directly leveraging the [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) `Win32\_ScheduledJob` WMI class.(Citation: Malicious Life by Cybereason)

On Linux and macOS, [at](https://attack.mitre.org/software/S0110) may be invoked by the superuser as well as any users added to the <code>at.allow</code> file. If the <code>at.allow</code> file does not exist, the <code>at.deny</code> file is checked. Every username not listed in <code>at.deny</code> is allowed to invoke [at](https://attack.mitre.org/software/S0110). If the <code>at.deny</code> exists and is empty, global use of [at](https://attack.mitre.org/software/S0110) is permitted. If neither file exists (which is often the baseline) only the superuser is allowed to use [at](https://attack.mitre.org/software/S0110).(Citation: Linux at)

Adversaries may use [at](https://attack.mitre.org/software/S0110) to execute programs at system startup or on a scheduled basis for [Persistence](https://attack.mitre.org/tactics/TA0003). [at](https://attack.mitre.org/software/S0110) can also be abused to conduct remote [Execution](https://attack.mitre.org/tactics/TA0002) as part of [Lateral Movement](https://attack.mitre.org/tactics/TA0008) and/or to run a process under the context of a specified account (such as SYSTEM).

In Linux environments, adversaries may also abuse [at](https://attack.mitre.org/software/S0110) to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, [at](https://attack.mitre.org/software/S0110) may also be used for [Privilege Escalation](https://attack.mitre.org/tactics/TA0004) if the binary is allowed to run as superuser via <code>sudo</code>.(Citation: GTFObins at)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: execution

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

## Malware

* MURKYTOP

## Tools

* CrackMapExec
* at

## APTs (Intrusion Sets)

* APT18
* BRONZE BUTLER
* Threat Group-3390