T1053.002 - At

Description from ATT&CK

> 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. On Linux and macOS, at may be invoked by the superuser as well as any users added to the `at.allow` file. If the `at.allow` file does not exist, the `at.deny` file is checked. Every username not listed in `at.deny` is allowed to invoke at. If the `at.deny` exists and is empty, global use of at is permitted. If neither file exists (which is often the baseline) only the superuser is allowed to use at.(Citation: Linux at)
>
> Adversaries may use at to execute programs at system startup or on a scheduled basis for Persistence. at can also be abused to conduct remote Execution as part of Lateral Movement and/or to run a process under the context of a specified account (such as SYSTEM).
>
> In Linux environments, adversaries may also abuse at to break out of restricted environments by using a task to spawn an interactive system shell or to run system commands. Similarly, at may also be used for Privilege Escalation if the binary is allowed to run as superuser via `sudo`.(Citation: GTFObins at)

Atomic Tests

- Atomic Test #1 - At.exe Scheduled task
- Atomic Test #2 - At - Schedule a job

Atomic Test #1 - At.exe Scheduled task

Executes cmd.exe Note: deprecated in Windows 8+

Upon successful execution, cmd.exe will spawn at.exe and create a scheduled task that will spawn cmd at a specific time.

Supported Platforms: Windows

- T1037.001
- T1037.002
- T1037.004
- T1037.005
- T1039
- T1040

auto_generated_guid: 4a6c0dc4-0f2a-4203-9298-a5a9bdc21ed8

Attack Commands: Run with `command_prompt`!

```
at 13:20 /interactive cmd
```

Atomic Test #2 - At - Schedule a job

This test submits a command to be run in the future by the `at` daemon.

Supported Platforms: Linux

auto_generated_guid: 7266d898-ac82-4ec0-97c7-436075d0d08e

Inputs:

Name	Description	Type	Default Value
time_spec	Time specification of when the command should run	String	now + 1 minute
at_command	The command to be run	String	echo Hello from Atomic Red Team

Attack Commands: Run with `sh`!

```
echo "#{at_command}" | at #{time_spec}
```

Dependencies: Run with `sh`!

Description: The `at` and `atd` executables must exist in the PATH

Check Prereq Commands:

```
which at && which atd
```

Get Prereq Commands:

```
echo 'Please install `at` and `atd`; they were not found in the PATH (Pa
```

Description: The `atd` daemon must be running

Check Prereq Commands:

```
systemctl status atd || service atd status
```

Get Prereq Commands:

```
echo 'Please start the `atd` daemon (sysv: `service atd start` ; systemd
```