

## T1489 - Service Stop

### **Description from ATT&CK**

Adversaries may stop or disable services on a system to render those services unavailable to legitimate users. Stopping critical services or processes can inhibit or stop response to an incident or aid in the adversary's overall objectives to cause damage to the environment.(Citation: Talos Olympic Destroyer 2018)(Citation: Novetta Blockbuster)

Adversaries may accomplish this by disabling individual services of high importance to an organization, such as MSExchangeIS, which will make Exchange content inaccessible (Citation: Novetta Blockbuster). In some cases, adversaries may stop or disable many or all services to render systems unusable.(Citation: Talos Olympic Destroyer 2018) Services or processes may not allow for modification of their data stores while running. Adversaries may stop services or processes in order to conduct Data Destruction or Data Encrypted for Impact on the data stores of services like Exchange and SQL Server.(Citation: SecureWorks WannaCry Analysis)

#### **Atomic Tests**

- Atomic Test #1 Windows Stop service using Service Controller
- Atomic Test #2 Windows Stop service using net.exe
- Atomic Test #3 Windows Stop service by killing process

# Atomic Test #1 - Windows - Stop service using Service Controller

Stops a specified service using the sc.exe command. Upon execution, if the spooler service was running information will be displayed saying it has changed to a state of STOP\_PENDING. If the spooler service was not running "The service has not been started." will be displayed and it can be started by running the cleanup command.

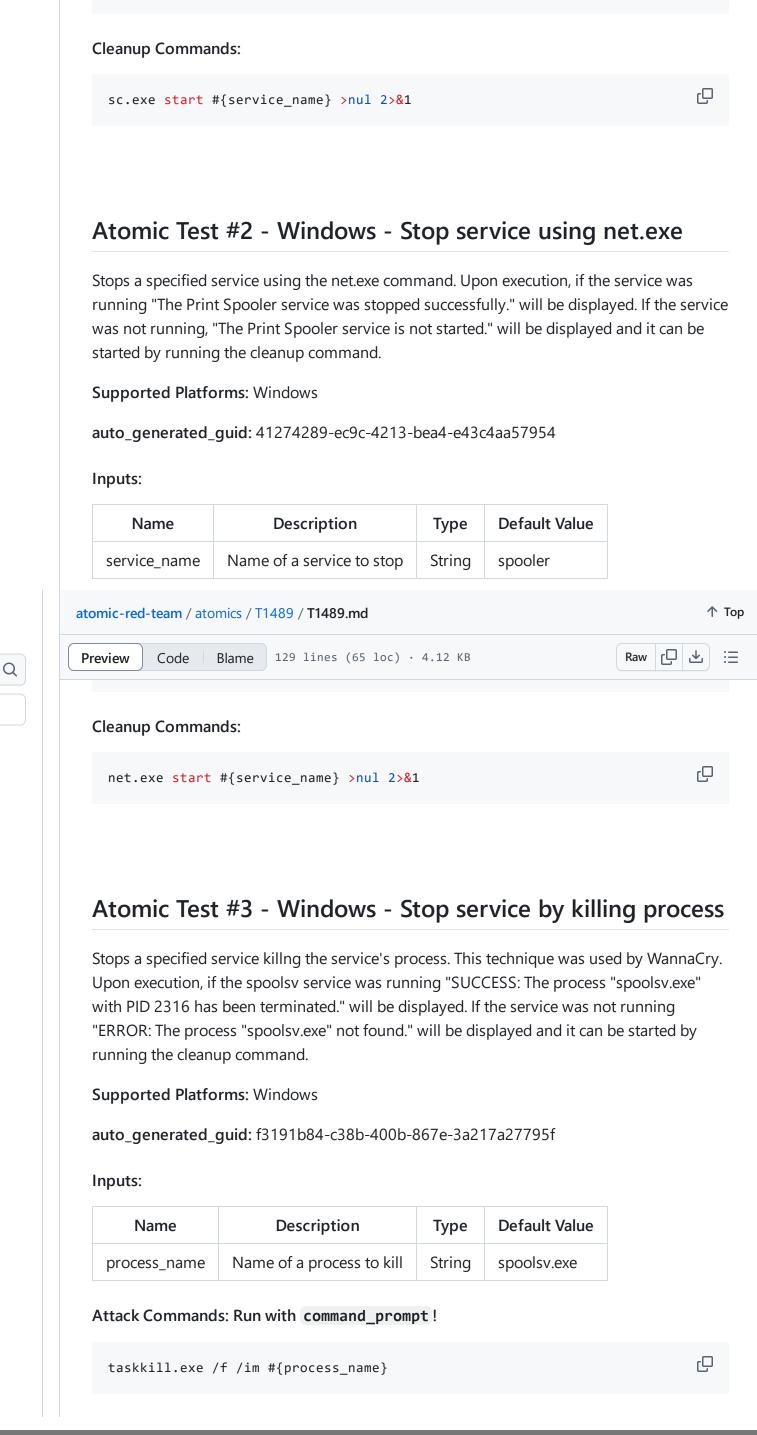
Supported Platforms: Windows

auto\_generated\_guid: 21dfb440-830d-4c86-a3e5-2a491d5a8d04

#### Inputs:

Name	Description	Туре	Default Value
service_name	Name of a service to stop	String	spooler

sc.exe stop #{service\_name}



Page 2 of 3

Attack Commands: Run with command\_prompt! Elevation Required (e.g. root or admin)

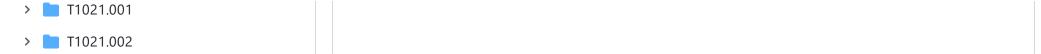
Q

Files

**ያ** f339e7d

Q Go to file

> T1020



- > T1021.003
- > T1021.006
- > T1027.001
- > T1027.002
- > T1027.004
- > T1027
- > T1030
- > T1033
- > T1036.003
- > T1036.004
- > T1036.005
- > **T1036.006**
- > **T1036**
- > T1037.001
- > T1037.002
- > T1037.004
- > T1037.005
- > T1039
- > T1040