Product Solutions Resources Open Source Enterprise Pricing Sign in Sign up

redcanaryco / atomic-red-team Public Notifications Fork 2.8k Star 9.7k

Code Issues 6 Pull requests 5 Actions Wiki Security Insights

atomic-red-team / atomics / T1489 / T1489.md

CircleCI Atomic Red Team doc... Generate docs from job=gener... 36d49de · 3 years ago History

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 infomration 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	Type	Default Value
service_name	Name of a service to stop	String	spooler

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

```
sc.exe stop #{service_name}
```

Cleanup Commands:

```
sc.exe start #{service_name} >nul 2>&1
```

Atomic Test #2 - Windows - Stop service using net.exe

Stops a specified service using the net.exe command. Upon execution, if the service was running "The Print Spooler service was stopped successfully." will be displayed. If the service was not running, "The Print Spooler service is not started." will be displayed and it can be started by running the cleanup command.

Supported Platforms: Windows

auto_generated_guid: 41274289-ec9c-4213-bea4-e43c4aa57954

Inputs:

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

atomic-red-team / atomics / T1489 / T1489.md   Top
Preview Code Blame 129 lines (65 loc) · 4.12 KB   Raw

Cleanup Commands:

```
net.exe start #{service_name} >nul 2>&1
```

Atomic Test #3 - Windows - Stop service by killing process

Stops a specified service killng the service's process. This technique was used by WannaCry. Upon execution, if the spoolsv service was running "SUCCESS: The process "spoolsv.exe" with PID 2316 has been terminated." will be displayed. If the service was not running "ERROR: The process "spoolsv.exe" not found." will be displayed and it can be started by running the cleanup command.

Supported Platforms: Windows

auto_generated_guid: f3191b84-c38b-400b-867e-3a217a27795f

Inputs:

Name	Description	Type	Default Value
process_name	Name of a process to kill	String	spoolsv.exe

Attack Commands: Run with `command_prompt`!

```
taskkill.exe /f /im #{process_name}
```

Files
f339e7d
Go to file
.github
atomic_red_team
atomics
Indexes
T1003.001
T1003.002
T1003.003
T1003.004
T1003.005
T1003.006
T1003.007
T1003.008
T1003
T1006
T1007
T1010
T1012
T1014
T1016
T1018
T1020

- T1021.001
- T1021.002
- 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