T1119 - Automated Collection

Description from ATT&CK

> Once established within a system or network, an adversary may use automated techniques for collecting internal data. Methods for performing this technique could include use of a [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059) to search for and copy information fitting set criteria such as file type, location, or name at specific time intervals. In cloud-based environments, adversaries may also use cloud APIs, command line interfaces, or extract, transform, and load (ETL) services to automatically collect data. This functionality could also be built into remote access tools.
> This technique may incorporate use of other techniques such as File and Directory Discovery and Lateral Tool Transfer to identify and move files, as well as Cloud Service Dashboard and Cloud Storage Object Discovery to identify resources in cloud environments.

Atomic Tests

- Atomic Test #1 - Automated Collection Command Prompt

Atomic Test #1 - Automated Collection Command Prompt

Automated Collection. Upon execution, check the users temp directory (%temp%) for the folder T1119_command_prompt_collection to see what was collected.

Supported Platforms: Windows

auto_generated_guid: cb379146-53f1-43e0-b884-7ce2c635ff5b

Attack Commands: Run with `command_prompt`!

```
mkdir %temp%\T1119_command_prompt_collection >nul 2>&1
dir c: /b /s .docx | findstr /e .docx
for /R c: %f in (*.docx) do copy %f %temp%\T1119_command_prompt_collection
```

Cleanup Commands:

```
del %temp%\T1119_command_prompt_collection /F /Q >nul 2>&1
```

Atomic Test #2 - Automated Collection PowerShell

Automated Collection. Upon execution, check the users temp directory (%temp%) for the folder T1119_powershell_collection to see what was collected.

Supported Platforms: Windows

auto_generated_guid: 634bd9b9-dc83-4229-b19f-7f83ba9ad313

Attack Commands: Run with `powershell`!

```
New-Item -Path $env:TEMP\T1119_powershell_collection -ItemType Directory -Force | (
Get-ChildItem -Recurse -Include *.doc | % {Copy-Item $_.FullName -destination $env
```

Cleanup Commands:

```
Remove-Item $env:TEMP\T1119_powershell_collection -Force -ErrorAction Ignore | Out
```

Atomic Test #3 - Recon information for export with PowerShell

collect information for exfiltration. Upon execution, check the users temp directory (%temp%) for files T1119_*.txt to see what was collected.

Supported Platforms: Windows

auto_generated_guid: c3f6d794-50dd-482f-b640-0384fbb7db26

Attack Commands: Run with `powershell`!

```
Get-Service > $env:TEMP\T1119_1.txt
Get-ChildItem Env: > $env:TEMP\T1119_2.txt
Get-Process > $env:TEMP\T1119_3.txt
```

Cleanup Commands:

```
Remove-Item $env:TEMP\T1119_1.txt -ErrorAction Ignore
Remove-Item $env:TEMP\T1119_2.txt -ErrorAction Ignore
Remove-Item $env:TEMP\T1119_3.txt -ErrorAction Ignore
```

Atomic Test #4 - Recon information for export with Command Prompt

collect information for exfiltration. Upon execution, check the users temp directory (%temp%) for files T1119_*.txt to see what was collected.

Supported Platforms: Windows

auto_generated_guid: aa1180e2-f329-4e1e-8625-2472ec0bfaf3

Attack Commands: Run with `command_prompt`!

```
sc query type=service > %TEMP%\T1119_1.txt
doskey /history > %TEMP%\T1119_2.txt
wmic process list > %TEMP%\T1119_3.txt
tree C:\AtomicRedTeam\atomics > %TEMP%\T1119_4.txt
```

Cleanup Commands:

```
del %TEMP%\T1119_1.txt >nul 2>&1
del %TEMP%\T1119_2.txt >nul 2>&1
del %TEMP%\T1119_3.txt >nul 2>&1
del %TEMP%\T1119_4.txt >nul 2>&1
```