

## Day 4 Advent of Cyber 2024 Atomic Red Team

What are we going to learn on this day?

- Learn how to identify malicious techniques using the MITRE ATT&CK framework.
- Learn about how to use Atomic Red Team tests to conduct attack simulations.
- Understand how to create alerting and detection rules from the attack tests.

Defining a proper boundary between false positive and true positive is a challenging task, especially when we look into some cases, for example we try to expect the IP and log generated should be from the country we have our company, but we will get log which says someone logged in from dddddd out of the country, which may be concerning.

But it may also be my boss travelling abroad for develop the business. So understanding the game starts there.

Cyber attack kill chain



Blue teamers can't be perfect but they want to stop the initial recon, which is not possible in a lot of cases, but we have a chance to stop them in later stages before they take over completely (last stage).

This framework completely aligns with the mitre framework which details about the cyberkill chain in 14 different columns.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
10 techniques	8 techniques	10 techniques	14 techniques	20 techniques	14 techniques	44 techniques	17 techniques	32 techniques	9 techniques	17 techniques	18 techniques

Last two columns are exfiltration and impact.

But keeping track of all the steps and trying to find the TTPs are difficult so what can we do about that?

There comes an important framework or library you want to call is **Atomic Red**. The library consists of simple test cases that can be executed by any blue team to test for detection gaps and help close them down. The library also supports automation, where the techniques can be automatically executed. However, it is also possible to execute them manually.

Perpetrator: Someone carries out an immoral or ethical act.

Simulation of the phishing to be specific spear phishing in this case

Below screenshot shows the options and parameters that we can use for the atomic test.

```
Loading personal and system profiles took 1302ms.
PS C:\Users\Administrator> Get-Help Invoke-AtomicTest

NAME
    Invoke-AtomicTest

SYNTAX
    Invoke-AtomicTest [-AtomicTechnique] <string[]> [-ShowDetails] [-ShowDetailsBrief]
    [-TestNumbers <string[]>] [-TestNames <string[]>] [-TestGuids <string[]>]
    [-PathToAtomicsFolder <string>] [-CheckPrereqs] [-PromptForInputArgs] [-GetPrereqs]
    [-Cleanup] [-NoExecutionLog] [-ExecutionLogPath <string>] [-Force] [-InputArgs <hashtable>]
    [-TimeoutSeconds <int>] [-Session <PSSession[]>] [-Interactive] [-KeepStdOutStdErrFiles]
    [-LoggingModule <string>] [-WhatIf] [-Confirm] [<CommonParameters>]

ALIASES
    None

REMARKS
    None
```

I just gave a request to know more about the particular attack ID which in our case seems like Spear Phishing.

```

PS C:\Users\Administrator> Invoke-AtomicTest T1566.001 -ShowDetails
PathToAtomicsFolder = C:\Tools\AtomicRedTeam\atomics

[*****BEGIN TEST*****]
Technique: Phishing: Spearphishing Attachment T1566.001
Atomic Test Name: Download Macro-Enabled Phishing Attachment
Atomic Test Number: 1
Atomic Test GUID: 114ccff9-ae6d-4547-9ead-4cd69f687306
Description: This atomic test downloads a macro enabled document from the Atomic Red Team GitHub repository, simulating an end user clicking a phishing link to download the file. The file "PhishingAttachment.xlsm" and PhishingAttachment.txt are downloaded to the %temp% directory.

Attack Commands:
Executor: powershell
ElevationRequired: False
Command:
$url = 'http://localhost/PhishingAttachment.xlsm'
$url2 = 'http://localhost/PhishingAttachment.txt'
Invoke-WebRequest -Uri $url -OutFile $env:TEMP\PhishingAttachment.xlsm
Invoke-WebRequest -Uri $url2 -OutFile $env:TEMP\PhishingAttachment.txt

Cleanup Commands:
Command:
Remove-Item $env:TEMP\PhishingAttachment.xlsm -ErrorAction Ignore
Remove-Item $env:TEMP\PhishingAttachment.txt -ErrorAction Ignore
[!!!!!!END TEST!!!!!!]

```

Go through the complete information after running the command, and we can understand the complete usage of this test and its outcome.

We are going to simulate a spear phishing attack using the command which will download a file, in the sense that somebody clicked a phishing link and the file is downloaded for us.

```

PS C:\Users\Administrator> Invoke-AtomicTest T1566.001 -TestNumbers 1 -CheckPrereq
PathToAtomicsFolder = C:\Tools\AtomicRedTeam\atomics

CheckPrereq's for: T1566.001-1 Download Macro-Enabled Phishing Attachment
Prerequisites met: T1566.001-1 Download Macro-Enabled Phishing Attachment
PS C:\Users\Administrator>

```

We successfully verified the prerequisite and it downloaded a phishing attachment.

```

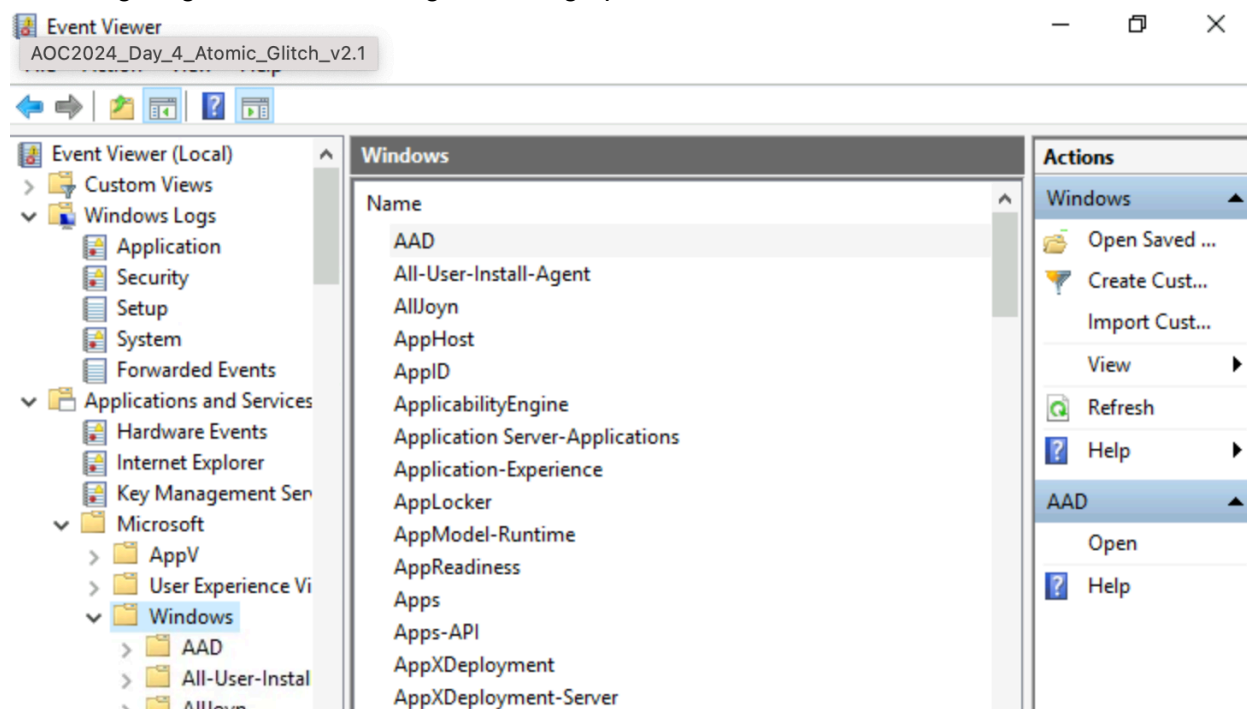
PS C:\Users\Administrator> Invoke-AtomicTest T1566.001 -TestNumbers 1
PathToAtomicsFolder = C:\Tools\AtomicRedTeam\atomics

Executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
Done executing test: T1566.001-1 Download Macro-Enabled Phishing Attachment
PS C:\Users\Administrator>

```

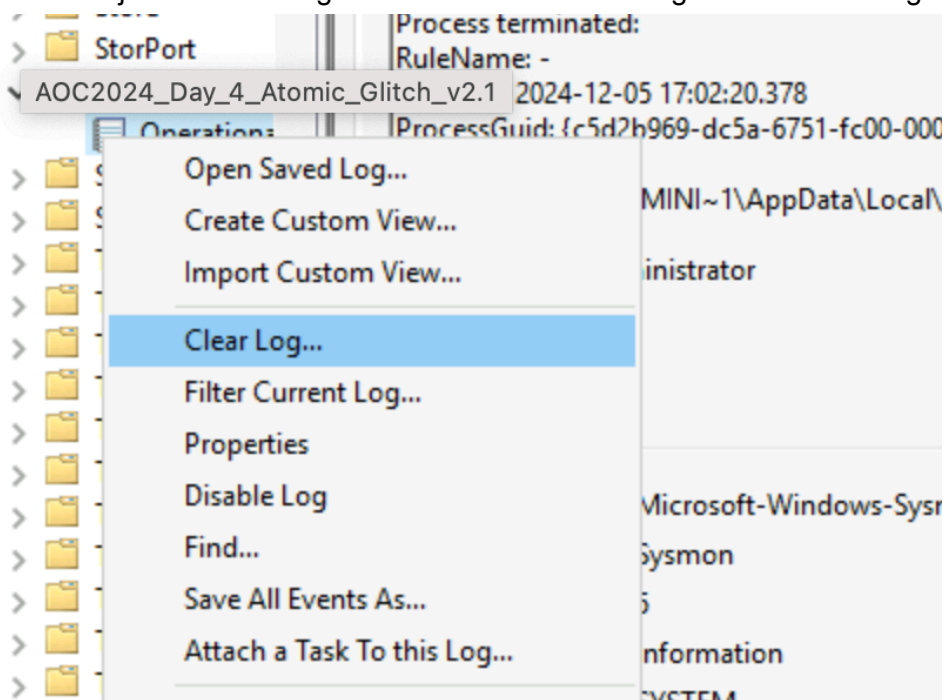
Remove the CheckPrereq and execute the command will run the test and download the macro enabled phishing attachment.

We will find the logs that must be stored in the registry, which we can view using the eventview and navigating to windows through following options below in the screenshot.



After windows look for a folder called sysmon which is one of tools from sysinternals for monitoring the windows via logs.

Now we will just clear the log and run the attack once again to view the logs.

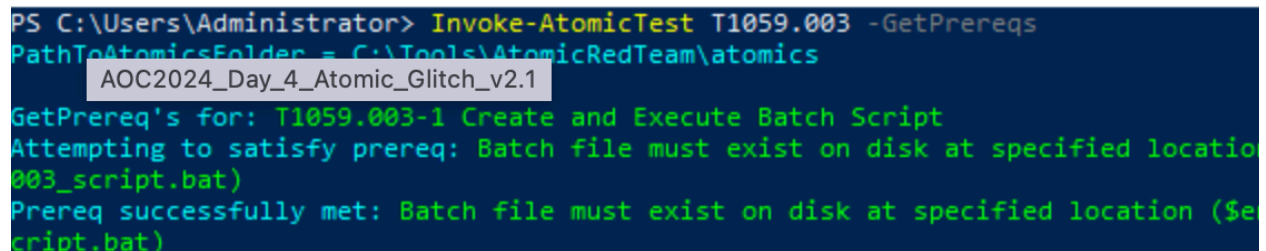


Once we clear the log we will get our first flag at \AppData\Local\Temp\ and record the flag and enter for the first question (.txt file)

Now our time to produce an attack for simulating ransomware using scriptor which is mitre attack Command and scripting interpreter.

Find the appropriate attack ID and find the subID based on that attack we are going to do. (Hint: Windows Command shell for subid)

Running the below Getprereqs command will help the prereqs to download and ready to execute the command.



```
PS C:\Users\Administrator> Invoke-AtomicTest T1059.003 -GetPrereqs
PathToAtomicFolder = C:\Tools\AtomicRedTeam\atomics
AOC2024_Day_4_Atomic_Glitch_v2.1
GetPrereq's for: T1059.003-1 Create and Execute Batch Script
Attempting to satisfy prereq: Batch file must exist on disk at specified location
003_script.bat)
Prereq successfully met: Batch file must exist on disk at specified location ($e
cript.bat)
```

The final flag is in the pdf file that is downloaded now.

Hint, this is the final attack simulation command, you will get the output in the pdf file.

“Invoke-AtomicTest 1059.003-4”

You will see the final flag in the file.