

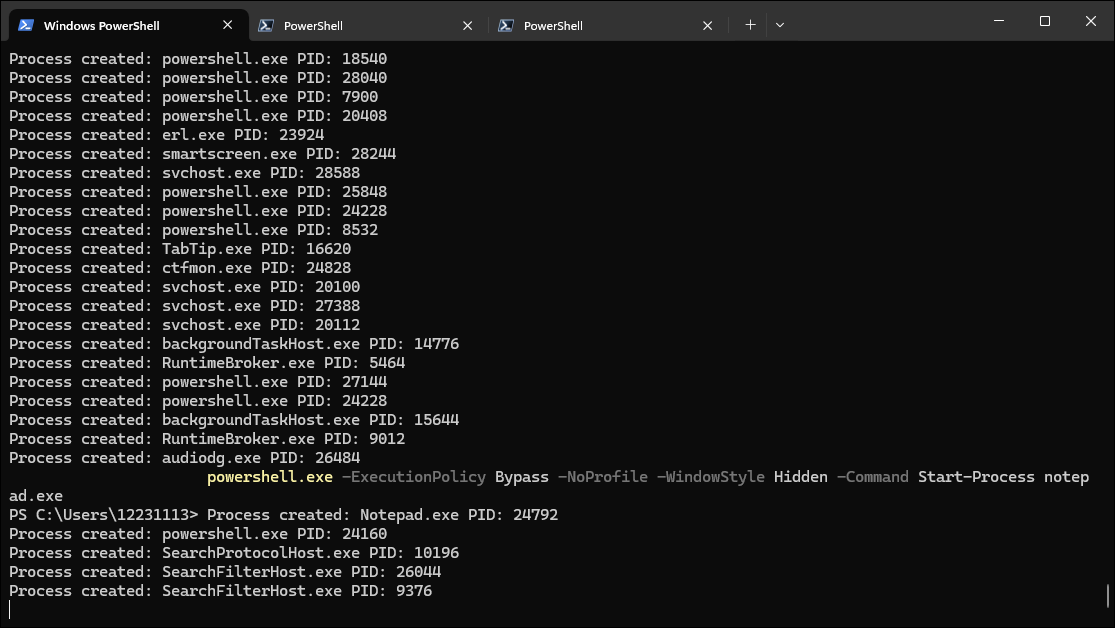
* This command simulates a malicious actor creating a new process (in this case, notepad.exe) in a hidden PowerShell window.

What This Represents:

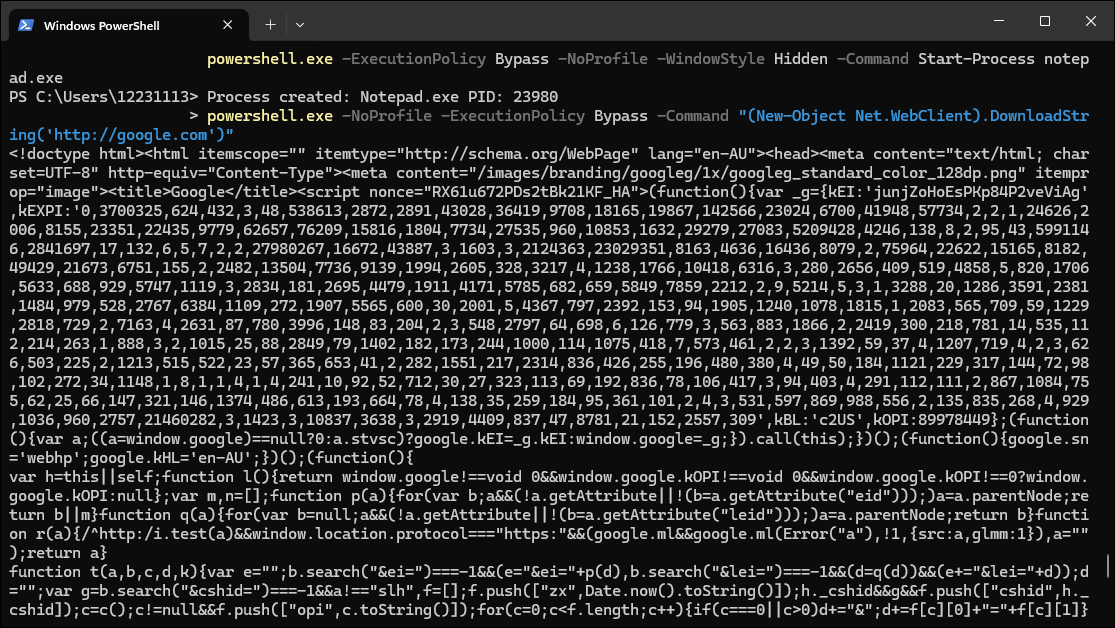
* This command mimics process creation using PowerShell with parameters that hide the execution window. In real attacks, threat actors often use such commands to launch malicious processes while attempting to evade detection.

MITRE ATT&CK Category:

* T1055: Process Injection
  + Tactic: Defense Evasion, Execution
  + Description: Attackers can use process injection techniques to run malicious code in the context of another process or to create new processes with malicious payloads.



Second attack

****

* This command simulates a network connection that attackers might use to communicate with a Command-and-Control (C2) server.

**What This Represents:**

* In real-world attacks, malware often uses PowerShell or other scripting languages to connect to an external server and either download malicious payloads or exfiltrate data. This simulation shows how a threat actor might connect to a remote server using PowerShell.

**MITRE ATT&CK Category:**

* **T1071: Application Layer Protocol**
  + **Tactic**: Command and Control
  + **Description**: This technique involves using standard application layer protocols (like HTTP) to communicate with external servers (often Command-and-Control servers) without raising alarms.

