Microsoft 365 Defender (KQL)

Query to detect creation of the `spinstall0.aspx` web shell:

Code snippet
```
DeviceFileEvents

| where InitiatingProcessParentFileName == "w3wp.exe"
| where InitiatingProcessFileName in ("cmd.exe", "powershell.exe")
| where FileName contains "spinstall" and FileName endswith ".aspx"
| where FolderPath contains @"\Web Server Extensions\" and FolderPath contains
@"\TEMPLATE\LAYOUTS\"
| project Timestamp, DeviceName, FileName, FolderPath, InitiatingProcessCommandLine,
SHA256
```

This query, adapted from Microsoft's guidance , looks for the specific process chain and file creation event that signifies the web shell drop.

Generic SIEM/Log Query (Splunk/ELK)

Query to detect suspicious process chains from the IIS worker process:

```
source="WinEventLog:Security" OR source="sysmon"
(ParentProcessName="w3wp.exe" OR ParentImage="*\\w3wp.exe")
AND (ProcessName IN ("cmd.exe", "powershell.exe", "rundll32.exe", "mshta.exe") OR
Image IN ("*\\cmd.exe", "*\\powershell.exe", "*\\rundll32.exe", "*\\mshta.exe"))
```

This query, based on the logic from multiple security vendors , is a high-fidelity indicator of web shell activity, as the IIS worker process should not normally be spawning command shells or other LOLBINs.

Query to detect suspicious file drops in SharePoint LAYOUTS directories:

```
source="WinEventLog:Security" OR source="sysmon" OR source="edr"
(EventCode="4663" OR EventID="11")
AND (TargetFileName ENDSWITH ".aspx" OR TargetFileName ENDSWITH ".js")
AND TargetFileName CONTAINS "\\Web Server Extensions\\"
AND TargetFileName CONTAINS "\\TEMPLATE\\LAYOUTS\\"
```

This query hunts for any new `.aspx` or `.js` files being written to the sensitive LAYOUTS directories, which are directly served to clients and are a common location for attackers to place backdoors.

PowerShell Log Query

Query to detect suspicious encoded PowerShell commands:

```
source="WinEventLog:Microsoft-Windows-PowerShell/Operational"
EventID="4104"
(ScriptBlockText CONTAINS "-enc" OR ScriptBlockText CONTAINS "-EncodedCommand" OR
ScriptBlockText CONTAINS "Invoke-Obfuscation")
```

This query targets PowerShell Script Block Logging (Event ID 4104) to find the use of encoded commands, a technique heavily favored by attackers to obfuscate their payloads and evade simple signature-based detection.