3B4E5808-3C71-406A-B181-17B0CE3178C9

Data Sources

- Microsoft-Windows-Sysmon/Operational

Logic

```
SELECT Message
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessGuid, d.ParentProcessGuid
    FROM apt29Host d
    INNER JOIN (
      SELECT a.ProcessGuid, a.ParentProcessGuid
      FROM apt29Host a
      INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
```

```
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(Image) LIKE "%control.exe"
            AND LOWER(ParentImage) LIKE "%sdclt.exe"
      ) b
      ON a.ParentProcessGuid = b.ProcessGuid
      WHERE a.Channel = "Microsoft-Windows-Sysmon/Operational"
        AND a.EventID = 1
        AND a.IntegrityLevel = "High"
    ) c
    ON d.ParentProcessGuid= c.ProcessGuid
    WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
) e
ON f.ProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND f.EventID = 7
    AND LOWER(f.ImageLoaded) LIKE "%system.drawing.ni.dll"
```

Output

```
Image loaded:
RuleName: -
UtcTime: 2020-05-02 03:06:42.583
ProcessGuid: {47ab858c-e374-5eac-d803-000000000400}
ProcessId: 3852
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ImageLoaded: C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawing\333e2b2
FileVersion: 4.8.3752.0 built by: NET48REL1
Description: .NET Framework
Product: Microsoft® .NET Framework
Company: Microsoft Corporation
OriginalFileName: System.Drawing.dll
Hashes: SHA1=388B289E2FD96234E2C1E8AE777248BE2C3D327B,MD5=30588BB4DCBF9940A1B1ECD6
Signed: false
Signature: -
SignatureStatus: Unavailable
```