

F4609F7E-C4DB-4327-91D4-59A58C962A02

Data Sources

- Microsoft-Windows-Sysmon/Operational
 - * Microsoft-Windows-PowerShell/Operational

Logic

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT d.ProcessId, d.ParentProcessId
  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.ExecutionProcessID = e.ProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
      AND f.EventID = 4103
      AND LOWER(f.Payload) LIKE "%get-clipboard%"
```

Output

```
CommandInvocation(Get-Clipboard): "Get-Clipboard"
Context:
Severity = Informational
Host Name = ConsoleHost
Host Version = 5.1.18362.628
Host ID = b802b425-c255-486e-81a2-6d10f7563af8
Host Application = powershell.exe
Engine Version = 5.1.18362.628
Runspace ID = f703f141-62e0-4a88-967c-42505edb0ce4
Pipeline ID = 21
Command Name = Get-Clipboard
Command Type = Cmdlet
Script Name =
Command Path =
Sequence Number = 62
User = DMEVALS\pbeesly
Connected User =
Shell ID = Microsoft.PowerShell
```



