



Cyb3rWard0g commented on May 13, 2020 • edited ▼



1 participant

Milestone

```
Sysmon Logs
                                                     Q
  SELECT Message
  FROM apt29Host d
  INNER JOIN (
      SELECT b.ProcessGuid
      FROM apt29Host b
      INNER JOIN (
          SELECT ProcessGuid
          FROM apt29Host
          WHERE Channel = "Microsoft-Windows-Sysmon/Operat
              AND EventID = 1
              AND LOWER(ParentImage) RLIKE '.*\\‎|â€|‪
      ) a
      ON b.ParentProcessGuid = a.ProcessGuid
      WHERE b.Channel = "Microsoft-Windows-Sysmon/Operation"
          AND b.EventID = 1
  ) c
  ON d.ProcessGuid = c.ProcessGuid
  WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND d.EventID = 11
    AND LOWER(d.TargetFilename) LIKE '%.zip'
Results
                                                     Q
  File created:
  RuleName: -
  UtcTime: 2020-05-02 02:56:18.032
  ProcessGuid: {47ab858c-e14e-5eac-ac03-000000000400}
  ProcessId: 5944
  Image: C:\windows\System32\WindowsPowerShell\v1.0\powers
  TargetFilename: C:\Users\pbeesly\AppData\Roaming\Draft.Z
  CreationUtcTime: 2020-05-02 02:56:18.032
```



Cyb3rWard0g commented on May 13, 2020 Contributor Author ···

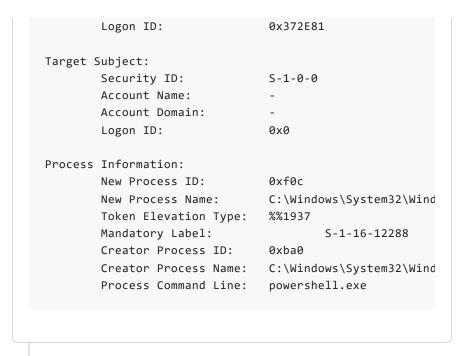
4.A.2 PowerShell

Procedure: Spawned interactive powershell.exe Criteria: powershell.exe spawning from powershell.exe



```
Cyb3rWard0g commented
                                    Contributor (Author) •••
on May 13, 2020
Powershell spawned after BypassUAC #6 (comment)
Sysmon
                                                      Q
  SELECT Message
  FROM apt29Host d
  INNER JOIN (
      SELECT a.ProcessGuid, a.ParentProcessGuid
      FROM apt29Host a
      INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operation
            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/Operatio"
        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'
Results
  Process Create:
                                                      Q
  RuleName: -
  UtcTime: 2020-05-02 03:00:13.551
  ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}
  ProcessId: 3876
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powers
  FileVersion: 10.0.18362.1 (WinBuild.160101.0800)
  Description: Windows PowerShell
  Product: Microsoft® Windows® Operating System
  Company: Microsoft Corporation
  OriginalFileName: PowerShell.EXE
  CommandLine: powershell.exe
  CurrentDirectory: C:\windows\system32\
  User: DMEVALS\pbeesly
  LogonGuid: {47ab858c-dabe-5eac-812e-370000000000}
  LogonId: 0x372E81
```

```
TerminalSessionId: 2
  IntegrityLevel: High
  Hashes: SHA1=36C5D12033B2EAF251BAE61C00690FFB17FDDC87,MD
  ParentProcessId: 2976
  ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\
  ParentCommandLine: "PowerShell.exe" -noni -noexit -ep by
Cyb3rWard0g commented
                                 (Contributor) (Author) •••
on May 13, 2020
Security Logs
                                                   Q
  SELECT Message
  FROM apt29Host d
  INNER JOIN(
     SELECT a.ProcessId, a.NewProcessId
      FROM apt29Host a
     INNER JOIN (
        SELECT NewProcessId
        FROM apt29Host
       WHERE LOWER(Channel) = "security"
           AND EventID = 4688
           AND LOWER(NewProcessName) LIKE "%control.exe"
           AND LOWER(ParentProcessName) LIKE "%sdclt.exe"
      ) b
     ON a.ProcessId = b.NewProcessId
     WHERE LOWER(a.Channel) = "security"
        AND a.EventID = 4688
       AND a.MandatoryLabel = "S-1-16-12288"
       AND a.TokenElevationType = "%%1937"
  ) c
  ON d.ProcessId = c.NewProcessId
  WHERE LOWER(d.Channel) = "security"
     AND d.EventID = 4688
     AND d.NewProcessName LIKE '%powershell.exe'
Results
                                                   Q
  A new process has been created.
  Creator Subject:
         Security ID:
                                 S-1-5-21-1830255721-3727
         Account Name:
                                 pbeesly
         Account Domain:
                                 DMEVALS
```





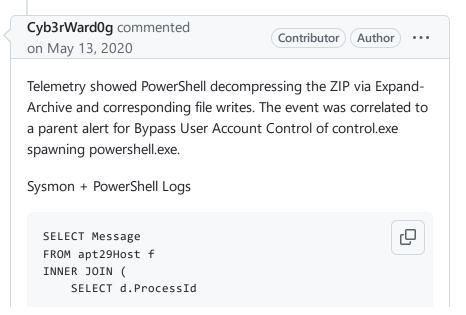
Cyb3rWard0g commented on May 13, 2020 Contributor Author ···

4.A.3 Deobfuscate/Decode Files or Information

Procedure: Decompressed ZIP (SysinternalsSuite.zip) file using PowerShell

Criteria: powershell.exe executing Expand-Archive





```
FROM apt29Host d
      INNER JOIN (
        SELECT a.ProcessGuid, a.ParentProcessGuid
        FROM apt29Host a
        INNER JOIN (
          SELECT ProcessGuid
          FROM apt29Host
          WHERE Channel = "Microsoft-Windows-Sysmon/Operat
              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/Operat
          AND a.EventID = 1
          AND a.IntegrityLevel = "High"
      ) c
      ON d.ParentProcessGuid= c.ProcessGuid
      WHERE d.Channel = "Microsoft-Windows-Sysmon/Operation"
        AND d.EventID = 1
        AND d.Image LIKE '%powershell.exe'
  ) e
  ON f.ExecutionProcessID = e.ProcessId
  WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatic
      AND f.EventID = 4104
      AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
Results
  Creating Scriptblock text (1 of 1):
  Expand-Archive -LiteralPath "$env:USERPROFILE\Down ____s\
  ScriptBlock ID: 63fc6cf4-cd9f-4134-9231-51ccb5c7d247
Security Logs + PowerShell
                                                      Q
  SELECT Message
  FROM apt29Host f
  INNER JOIN (
      SELECT split(d.NewProcessId, '0x')[1] as NewProcessI
      FROM apt29Host d
      INNER JOIN(
        SELECT a.ProcessId, a.NewProcessId
        FROM apt29Host a
        INNER JOIN (
          SELECT NewProcessId
          FROM apt29Host
          WHERE LOWER(Channel) = "security"
              AND EventID = 4688
```

```
AND LOWER(NewProcessName) LIKE "%control.exe
              AND LOWER(ParentProcessName) LIKE "%sdclt.ex
        ) b
        ON a.ProcessId = b.NewProcessId
        WHERE LOWER(a.Channel) = "security"
          AND a.EventID = 4688
          AND a.MandatoryLabel = "S-1-16-12288"
          AND a.TokenElevationType = "%%1937"
      ON d.ProcessId = c.NewProcessId
      WHERE LOWER(d.Channel) = "security"
        AND d.EventID = 4688
        AND d.NewProcessName LIKE '%powershell.exe'
  ) e
  ON LOWER(hex(f.ExecutionProcessID)) = e.NewProcessId
  WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatic
      AND f.EventID = 4104
      AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
Results
  Creating Scriptblock text (1 of 1):
  Expand-Archive -LiteralPath "$env:USERPROFILE\Down =====s\
  ScriptBlock ID: 63fc6cf4-cd9f-4134-9231-51ccb5c7d247
```

Sign up for free

to join this conversation on GitHub. Already have an

account? Sign in to comment

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information