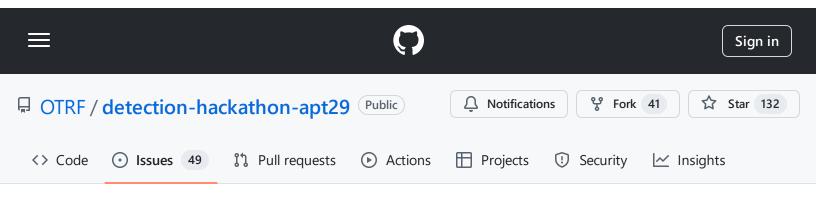
3.B) Component Object Model Hijacking, Bypass User Account Control, Commonly Used Port, Standard Application Layer Protocol, Standard Cryptographic Protocol · Issue #6 · OTRF/detection-hackathon-apt29 · GitHub - 31/10/2024 19:16 https://github.com/OTRF/detection-hackathon-apt29/issues/6

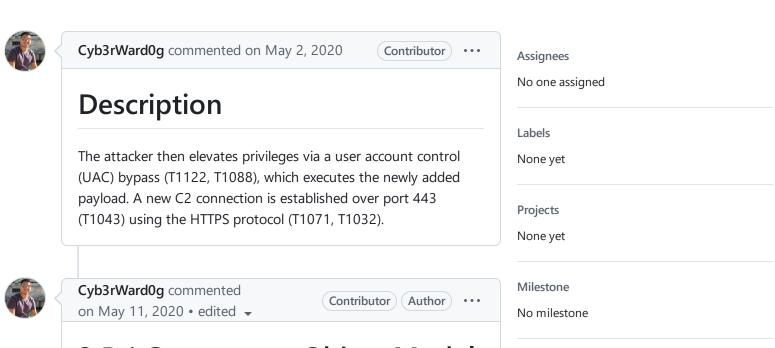


## 3.B) Component Object Model Hijacking, Bypass User Account Control, Commonly Used Port, Standard Application Layer Protocol, Standard Cryptographic Protocol #6





Cyb3rWard0g opened this issue on May 2, 2020 · 7 comments



## 3.B.1 Component Object Model Hijacking

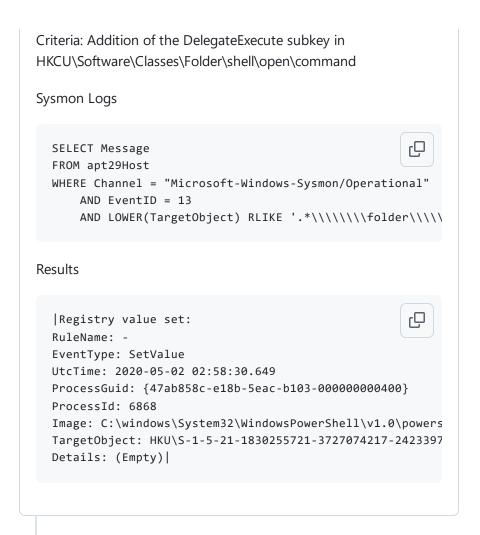
Procedure: Modified the Registry to enable COM hijacking of sdclt.exe using PowerShell

No branches or pull requests

1 participant



Development





Cyb3rWard0g commented on May 11, 2020

3.B.2 Bypass User Account Control

Detection Category (Telemetry)

Procedure: Executed elevated PowerShell payload Criteria: High integrity powershell.exe spawning from control.exe (spawned from sdclt.exe)

bypassUAC = spark.sql(

SELECT a.Image, a.CommandLine FROM apt29Table a INNER JOIN (

```
SELECT ProcessGuid
      FROM apt29Table
      WHERE Channel = "Microsoft-Windows-Sysmon/Operationa
          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"
  ''')
  bypassUAC.show(truncate = False, vertical = True)
Results
               | C:\Windows\System32\WindowsPowerShe [ ...
   CommandLine | "PowerShell.exe" -noni -noexit -ep bypass
```





```
Cyb3rWard0g commented on May 13, 2020

Security Event Logs

Contributor Author ...
```

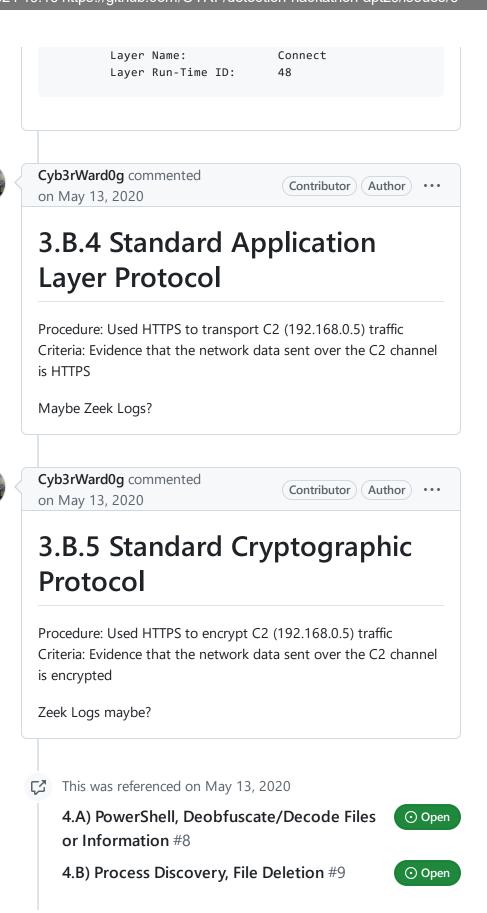
```
Q
  SELECT Message
  FROM apt29Host a
  INNER JOIN (
      SELECT NewProcessId
      FROM apt29Host
      WHERE LOWER(Channel) = "security"
          AND EventID = 4688
          AND LOWER(NewProcessName) LIKE "%control.exe"
          AND LOWER(ParentProcessName) LIKE "%sdclt.exe"
  ) b
  ON a.ProcessId = b.NewProcessId
  WHERE LOWER(a.Channel) = "security"
      AND a.EventID = 4688
      AND a.MandatoryLabel = "S-1-16-12288"
      AND a.TokenElevationType = "%%1937"
Output:
  A new process has been created.
                                                     Q
  Creator Subject:
          Security ID:
                                  S-1-5-21-1830255721-3727
          Account Name:
                                  pbeesly
          Account Domain:
                                  DMEVALS
          Logon ID:
                                  0x372E81
  Target Subject:
          Security ID:
                                  S-1-0-0
          Account Name:
          Account Domain:
          Logon ID:
                                  0x0
  Process Information:
          New Process ID:
                                  0xba0
          New Process Name:
                                 C:\Windows\System32\Wind
          Token Elevation Type: %%1937
          Mandatory Label:
                                          S-1-16-12288
          Creator Process ID: 0x131c
          Creator Process Name: C:\Windows\System32\cont
          Process Command Line: "PowerShell.exe" -noni -
```



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

```
3.B.3 Commonly Used Port
Procedure: Established C2 channel (192.168.0.5) via PowerShell
payload over TCP port 443
Criteria: Established network channel over port 443
Sysmon Event Logs
                                                      Q
  SELECT Message
  FROM apt29Host d
  INNER JOIN (
    SELECT a.ProcessGuid
    FROM apt29Host a
    INNER JOIN (
      SELECT ProcessGuid
      FROM apt29Host
      WHERE Channel = "Microsoft-Windows-Sysmon/Operationa
          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/Operationa
      AND a.EventID = 1
      AND a.IntegrityLevel = "High"
  ) c
  ON d.ProcessGuid = c.ProcessGuid
  WHERE d.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND d.EventID = 3
Results:
                                                      Q
  Network connection detected:
  RuleName: -
  UtcTime: 2020-05-02 02:58:46.099
  ProcessGuid: {47ab858c-e1e4-5eac-b803-000000000400}
  ProcessId: 2976
  Image: C:\Windows\System32\WindowsPowerShell\v1.0\powers
  User: DMEVALS\pbeesly
  Protocol: tcp
  Initiated: true
  SourceIsIpv6: false
  SourceIp: 10.0.1.4
  SourceHostname: -
  SourcePort: 59846
  SourcePortName: -
  DestinationIsIpv6: false
  DestinationIp: 192.168.0.5
```

```
DestinationHostname: -
  DestinationPort: 443
  DestinationPortName: -
Security Logs
                                                     Q
  SELECT Message
  FROM apt29Host d
  INNER JOIN (
      SELECT split(a.NewProcessId, '0x')[1] as NewProcessI
      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"
  ON LOWER(hex(CAST(ProcessId as INT))) = c.NewProcessId
  WHERE LOWER(Channel) = "security"
      AND d.EventID = 5156
Results
  The Windows Filtering Platform has permitted a con [ c
  Application Information:
          Process ID:
                                 2976
          Application Name:
                                \device\harddiskvolume2\
  Network Information:
         Direction:
                                 Outbound
          Source Address:
                                10.0.1.4
          Source Port:
                                59846
         Destination Address: 192.168.0.5
         Destination Port:
                                        443
          Protocol:
  Filter Information:
          Filter Run-Time ID:
                                 68659
```



3.B) Component Object Model Hijacking, Bypass User Account Control, Commonly Used Port, Standard Application Layer Protocol, Standard Cryptographic Protocol · Issue #6 · OTRF/detection-hackathon-apt29 · GitHub - 31/10/2024 19:16 https://github.com/OTRF/detection-hackathon-apt29/issues/6

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 © 2024 GitHub, Inc.