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

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

Cyb3rWard0g commented on May 2, 2020 Contributor

Description

The attacker then elevates privileges via a user account control (UAC) bypass (T1122, T1088), which executes the newly added payload. A new C2 connection is established over port 443 (T1043) using the HTTPS protocol (T1071, T1032).

Cyb3rWard0g commented on May 11, 2020 • edited Contributor Author

3.B.1 Component Object Model Hijacking

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

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant

Criteria: Addition of the DelegateExecute subkey in HKCU\Software\Classes\Folder\shell\open\command

Sysmon Logs

```
SELECT Message
FROM apt29Host
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
    AND EventID = 13
    AND LOWER(TargetObject) RLIKE '.*\\\\\\\\folder\\\\\
```

Results

```
|Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2020-05-02 02:58:30.649
ProcessGuid: {47ab858c-e18b-5eac-b103-000000000400}
ProcessId: 6868
Image: C:\windows\System32\WindowsPowerShell\v1.0\powers
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
Details: (Empty)|
```

Cyb3rWard0g commented on May 11, 2020 — Contributor, Author

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

```
Image       | C:\Windows\System32\WindowsPowerShe
CommandLine | "PowerShell.exe" -noni -noexit -ep bypass
```

Cyb3rWard0g commented on May 11, 2020 — Contributor, Author

This could also work:

```
test = spark.sql(
    '''
SELECT Image, CommandLine
FROM apt29Table
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
    AND EventID = 1
    AND IntegrityLevel = "High"
    AND LOWER(ParentImage) LIKE "%control.exe"
''')
test.show(truncate = False, vertical = True)
```

Cyb3rWard0g commented on May 13, 2020 — Contributor, Author

Security Event Logs

```
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.

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

```
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:

```
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

```
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"
) c
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:               6

Filter Information:
        Filter Run-Time ID:     68659
```

```
Layer Name:             Connect
Layer Run-Time ID:      48
```

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

3.B.4 Standard Application Layer Protocol

Procedure: Used HTTPS to transport C2 (192.168.0.5) traffic
Criteria: Evidence that the network data sent over the C2 channel is HTTPS

Maybe Zeek Logs?

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

3.B.5 Standard Cryptographic Protocol

Procedure: Used HTTPS to encrypt C2 (192.168.0.5) traffic
Criteria: Evidence that the network data sent over the C2 channel is encrypted

Zeek Logs maybe?

This was referenced on May 13, 2020

4.A) PowerShell, Deobfuscate/Decode Files or Information #8 Open

4.B) Process Discovery, File Deletion #9 Open