Sign in

OTRF / **detection-hackathon-apt29** Public

Notifications | Fork 41 | Star 132

Code | Issues 49 | Pull requests | Actions | Projects | Security | Insights

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

New issue

Open **Cyb3rWard0g** opened this issue on May 2, 2020 · 12 comments

**Cyb3rWard0g** commented on May 2, 2020 Contributor ···

The attacker then enumerates running processes (T1057) to discover/terminate the initial access from Step 1 (Pupy Agent) before deleting various files (T1107) associated with that access.

**Cyb3rWard0g** commented on May 11, 2020 Contributor Author ···

# 4.b.* File Deletion

## Detection Category (Telemetry)

Deleting files with sdelete

```
sdelete = spark.sql(
    '''
SELECT EventID, Image, Archived, TargetFilename
FROM apt29Table
WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
AND (LOWER(TargetFilename) LIKE "%.zzz%")  OR (LOWER(Tar
                          ''')
sdelete.show(100,truncate = False, vertical = False)
```

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant

results;

```
+-------+----------------------------------------
|EventID|Image
+-------+-------------------------------------------
|23     |C:\Program Files\SysinternalsSuite\sdelete64.ex
|23     |C:\Program Files\SysinternalsSuite\sdelete64.ex
|23     |C:\Windows\Temp\sdelete64.exe
+-------+-------------------------------------------
```

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

# 4.B.1 Process Discovery

Procedure: Enumerated current running processes using PowerShell
Criteria: powershell.exe executing Get-Process

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

Telemetry showed powershell.exe executing Get-Process. The event was correlated to a parent alert for Bypass User Account Control of control.exe spawning powershell.exe.

Sysmon Logs + PowerShell Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
    SELECT d.ProcessId
    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/Operatio
        AND d.EventID = 1
        AND d.Image LIKE '%powershell.exe'
  ) e
  ON f.ExecutionProcessID = e.ProcessId
  WHERE f.Channel = "Microsoft-Windows-PowerShell/Operatio
      AND f.EventID = 4104
      AND LOWER(f.ScriptBlockText) LIKE "%get-process%"
```

Results

```
Creating Scriptblock text (1 of 1):
get-process

ScriptBlock ID: 66a7f650-8a84-4dcf-a0f7-41d06de51f5c
Path:
```

Security Logs + PowerShell Logs

```
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"
      ) c
      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 "%get-process%"
```

Results

```
Creating Scriptblock text (1 of 1):
get-process

ScriptBlock ID: 66a7f650-8a84-4dcf-a0f7-41d06de51f5c
```

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

# 4.B.2 File Deletion

Procedure: Deleted rcs.3aka3.doc on disk using SDelete
Criteria: sdelete64.exe deleting the file rcs.3aka3.doc

**Cyb3rWard0g** commented on May 13, 2020 • edited Contributor Author ···

Telemetry showed sdelete.exe running with command-line arguments to delete the file. The event was correlated to a parent alert for Bypass User Account Control of control.exe spawning powershell.exe.

Sysmon Logs

```
SELECT Message
FROM apt29Host f
```

```
INNER JOIN (
    SELECT d.ProcessId, d.ProcessGuid
    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/Operatio
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
) e
ON f.ParentProcessGuid = e.ProcessGuid
WHERE f.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND f.EventID = 1
    AND LOWER(f.Image) LIKE '%sdelete%'
    AND LOWER(f.CommandLine) LIKE '%3aka3%'
```

Results

```
Process Create:
RuleName: -
UtcTime: 2020-05-02 03:02:04.324
ProcessGuid: {47ab858c-e2ac-5eac-cb03-000000000400}
ProcessId: 4140
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
FileVersion: 2.02
Description: Secure file delete
Product: Sysinternals Sdelete
Company: Sysinternals - www.sysinternals.com
OriginalFileName: sdelete.exe
CommandLine: "C:\Program Files\SysinternalsSuite\sdelete
CurrentDirectory: C:\Program Files\SysinternalsSuite\
User: DMEVALS\pbeesly
LogonGuid: {47ab858c-dabe-5eac-812e-370000000000}
LogonId: 0x372E81
TerminalSessionId: 2
IntegrityLevel: High
Hashes: SHA1=7BCD946326B67F806B3DB4595EDE9FBDF29D0C36,MD
```

```
ParentProcessGuid: {47ab858c-e23d-5eac-c603-000000000400
ParentProcessId: 3876
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\
ParentCommandLine: powershell.exe
```

**Cyb3rWard0g** commented on May 13, 2020

Contributor Author ···

Another way to identify Sysinternals Sdelete tool
Sysmon

```
SELECT Message
FROM apt29Host h
INNER JOIN (
    SELECT f.ProcessGuid
    FROM apt29Host f
    INNER JOIN (
      SELECT d.ProcessId, d.ProcessGuid
      FROM apt29Host d
      INNER JOIN (
        SELECT a.ProcessGuid, a.ParentProcessGuid
        FROM apt29Host a
        INNER JOIN (
          SELECT ProcessGuid
          FROM apt29Host
          WHERE Channel = "Microsoft-Windows-Sysmon/Oper
              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/Oper
          AND a.EventID = 1
          AND a.IntegrityLevel = "High"
      ) c
      ON d.ParentProcessGuid= c.ProcessGuid
      WHERE d.Channel = "Microsoft-Windows-Sysmon/Operat
        AND d.EventID = 1
        AND d.Image LIKE '%powershell.exe'
    ) e
    ON f.ParentProcessGuid = e.ProcessGuid
    WHERE f.Channel = "Microsoft-Windows-Sysmon/Operatio
      AND f.EventID = 1
      AND LOWER(f.Image) LIKE '%sdelete%'
      AND LOWER(f.CommandLine) LIKE '%3aka3%'
) g
ON h.ProcessGuid = g.ProcessGuid
```

```
WHERE h.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND h.EventID in (12,13)
    AND LOWER(h.TargetObject) RLIKE '.*\\\\\\\\software\
```

Results

```
|Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2020-05-02 03:02:04.518
ProcessGuid: {47ab858c-e2ac-5eac-cb03-000000000400}
ProcessId: 4140
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
Details: DWORD (0x00000001)|
```

```
|Registry object added or deleted:
RuleName: -
EventType: CreateKey
UtcTime: 2020-05-02 03:02:04.518
ProcessGuid: {47ab858c-e2ac-5eac-cb03-000000000400}
ProcessId: 4140
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
|Registry object added or deleted:
RuleName: -
EventType: CreateKey
UtcTime: 2020-05-02 03:02:04.518
ProcessGuid: {47ab858c-e2ac-5eac-cb03-000000000400}
ProcessId: 4140
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
```

**Cyb3rWard0g** commented on May 13, 2020

Contributor Author ···

Security Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT d.NewProcessId
  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'
) e
ON f.ProcessId = e.NewProcessId
WHERE LOWER(f.Channel) = "security"
  AND f.EventID = 4688
  AND LOWER(f.NewProcessName) LIKE '%sdelete%'
  AND LOWER(f.CommandLine) LIKE '%3aka3%'
```

Results

```
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:         0x102c
        New Process Name:       C:\Program Files\Sysinte
        Token Elevation Type:   %%1937
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0xf24
        Creator Process Name:   C:\Windows\System32\Wind
        Process Command Line:   "C:\Program Files\Sysint
```

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

## 4.B.3 File Deletion

Procedure: Deleted Draft.zip on disk using SDelete
Criteria: sdelete64.exe deleting the file draft.zip

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

Leveraging new event 23 and a correlation from the BypassUAC detection #6

Sysmon

```
SELECT Message, g.CommandLine
FROM apt29Host h
INNER JOIN (
  SELECT f.ProcessGuid, f.CommandLine
  FROM apt29Host f
  INNER JOIN (
    SELECT d.ProcessId, d.ProcessGuid
    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/Operatio
        AND d.EventID = 1
        AND d.Image LIKE '%powershell.exe'
    ) e
    ON f.ParentProcessGuid = e.ProcessGuid
    WHERE f.Channel = "Microsoft-Windows-Sysmon/Operationa
      AND f.EventID = 1
      AND LOWER(f.Image) LIKE '%sdelete%'
      AND LOWER(f.CommandLine) LIKE '%draft.zip%'
  ) g
  ON h.ProcessGuid = g.ProcessGuid
  WHERE h.Channel = "Microsoft-Windows-Sysmon/Operational"
    AND h.EventID = 23
```

Results

```
 Message     | File Delete:
RuleName: -
UtcTime: 2020-05-02 03:03:14.765
ProcessGuid: {47ab858c-e2f2-5eac-d203-000000000400}
ProcessId: 8760
User: DMEVALS\pbeesly
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetFilename: C:\Users\pbeesly\ZZZZZZZZZZZZZZZZZZZZZ.Z
Hashes: SHA1=B639091A8FA004CAA8E2D95DF4476374D7D09221,MD
IsExecutable: false
Archived: true
 CommandLine | "C:\Program Files\SysinternalsSuite\sdele
```

**Cyb3rWard0g** commented on May 13, 2020

Contributor Author ···

Sysmon + Registry

```
SELECT Message
FROM apt29Host h
INNER JOIN (
  SELECT f.ProcessGuid
  FROM apt29Host f
  INNER JOIN (
    SELECT d.ProcessId, d.ProcessGuid
    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/Operatio
      AND d.EventID = 1
      AND d.Image LIKE '%powershell.exe'
  ) e
  ON f.ParentProcessGuid = e.ProcessGuid
  WHERE f.Channel = "Microsoft-Windows-Sysmon/Operationa
    AND f.EventID = 1
    AND LOWER(f.Image) LIKE '%sdelete%'
    AND LOWER(f.CommandLine) LIKE '%draft.zip%'
) g
ON h.ProcessGuid = g.ProcessGuid
WHERE h.Channel = "Microsoft-Windows-Sysmon/Operational"
  AND h.EventID in (12,13)
  AND LOWER(h.TargetObject) RLIKE '.*\\\\\\\\software\\\
```

Result

```
|Registry value set:
RuleName: -
EventType: SetValue
UtcTime: 2020-05-02 03:03:14.702
ProcessGuid: {47ab858c-e2f2-5eac-d203-000000000400}
ProcessId: 8760
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
Details: DWORD (0x00000001)|
|Registry object added or deleted:
RuleName: -
EventType: CreateKey
UtcTime: 2020-05-02 03:03:14.702
ProcessGuid: {47ab858c-e2f2-5eac-d203-000000000400}
ProcessId: 8760
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
|Registry object added or deleted:
RuleName: -
```

```
EventType: CreateKey
UtcTime: 2020-05-02 03:03:14.702
ProcessGuid: {47ab858c-e2f2-5eac-d203-000000000400}
ProcessId: 8760
Image: C:\Program Files\SysinternalsSuite\sdelete64.exe
TargetObject: HKU\S-1-5-21-1830255721-3727074217-2423397
```

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

Security Logs

```
SELECT Message
FROM apt29Host f
INNER JOIN (
SELECT d.NewProcessId
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'
) e
ON f.ProcessId = e.NewProcessId
WHERE LOWER(f.Channel) = "security"
AND f.EventID = 4688
AND LOWER(f.NewProcessName) LIKE '%sdelete%'
AND LOWER(f.CommandLine) LIKE '%draft.zip'
```

Results

```
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:         0x2238
        New Process Name:       C:\Program Files\Sysinte
        Token Elevation Type:   %%1937
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0xf24
        Creator Process Name:   C:\Windows\System32\Wind
        Process Command Line:   "C:\Program Files\Sysint
```

**Cyb3rWard0g** commented on May 13, 2020

Contributor Author ···

# 4.B.4 File Deletion

Procedure: Deleted SysinternalsSuite.zip on disk using SDelete
Criteria: sdelete64.exe deleting the file SysinternalsSuite.zip

Same as before but looking for sysinternalssuite.zip 😉

**hitenkoku** mentioned this issue on Apr 24, 2021

**SIGMAルール読み込み共通部分対応** Closed
Yamato-Security/hayabusa#90