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

New issue

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

Cyb3rWard0g commented on May 2, 2020 Contributor

Description

The attacker uploads additional tools (T1086) through the new, elevated access before spawning an interactive powershell.exe shell (T1086). The additional tools are decompressed (T1140) and positioned on the target for usage.

Cyb3rWard0g commented on May 13, 2020 Contributor Author

4.A.1 Remote File Copy

Procedure: Dropped additional tools (SysinternalsSuite.zip) to disk over C2 channel (192.168.0.5)
Criteria: powershell.exe creating the file SysinternalsSuite.zip

Cyb3rWard0g commented on May 13, 2020 • edited Contributor Author

Sysmon Logs

```
SELECT Message
FROM apt29Host d
INNER JOIN (
    SELECT b.ProcessGuid
    FROM apt29Host b
    INNER JOIN (
        SELECT ProcessGuid
        FROM apt29Host
        WHERE Channel = "Microsoft-Windows-Sysmon/Operational"
            AND EventID = 1
            AND LOWER(ParentImage) RLIKE '.*\\â€Ž|â€|â€ª|â€«|â€¬|â€|â€®.*'
    ) a
    ON b.ParentProcessGuid = a.ProcessGuid
    WHERE b.Channel = "Microsoft-Windows-Sysmon/Operational"
        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

```
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\powershell.exe
TargetFilename: C:\Users\pbeesly\AppData\Roaming\Draft.Zip
CreationUtcTime: 2020-05-02 02:56:18.032
```

Assignees
No one assigned

Labels
None yet

Projects
None yet

Milestone
No milestone

Development
No branches or pull requests

1 participant

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 on May 13, 2020 Contributor Author ···

Powershell spawned after BypassUAC #6 (comment)

Sysmon

```
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/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'
```

Results

```
Process Create:
RuleName: -
UtcTime: 2020-05-02 03:00:13.551
ProcessGuid: {47ab858c-e23d-5eac-c603-000000000400}
ProcessId: 3876
Image: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
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,MD5=CDA48FC75952AD12D99E526
ParentProcessGuid: {47ab858c-e1e4-5eac-b803-000000000400}
ParentProcessId: 2976
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "PowerShell.exe" -noni -noexit -ep bypass -window hidden -c "s
```

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

Security Logs

```
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

```
A new process has been created.

Creator Subject:
        Security ID:            S-1-5-21-1830255721-3727074217-2423397540-1107
        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:         0xf0c
        New Process Name:       C:\Windows\System32\WindowsPowerShell\v1.0\powers
        Token Elevation Type:   %%1937
        Mandatory Label:                S-1-16-12288
        Creator Process ID:     0xba0
        Creator Process Name:   C:\Windows\System32\WindowsPowerShell\v1.0\powers
        Process Command Line:   powershell.exe
```

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

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

Telemetry showed PowerShell decompressing the ZIP via Expand-Archive and corresponding file writes. The event was correlated to a parent alert for Bypass User Account Control of control.exe spawning powershell.exe.

Sysmon + 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/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 = 4104
  AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
```

Results

```
Creating Scriptblock text (1 of 1):
Expand-Archive -LiteralPath "$env:USERPROFILE\Downloads\SysinternalsSuite.zip" -D

ScriptBlock ID: 63fc6cf4-cd9f-4134-9231-51ccb5c7d247
```

Security Logs + PowerShell

```
SELECT Message
FROM apt29Host f
INNER JOIN (
  SELECT split(d.NewProcessId, '0x')[1] as 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 LOWER(hex(f.ExecutionProcessID)) = e.NewProcessId
WHERE f.Channel = "Microsoft-Windows-PowerShell/Operational"
  AND f.EventID = 4104
  AND LOWER(f.ScriptBlockText) LIKE "%expand-archive%"
```

Results

```
Creating Scriptblock text (1 of 1):
Expand-Archive -LiteralPath "$env:USERPROFILE\Downloads\SysinternalsSuite.zip" -D

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

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information