Files

f7a5815

Go to file

- docs
- playbooks
  - WIN-170105221010.yaml
  - WIN-180719170510.yaml
  - WIN-180815210510.yaml
  - WIN-190101151110.yaml
  - WIN-190407183310.yaml
  - WIN-190410151110.yaml
  - WIN-190510202010.yaml
  - WIN-190511223310.yaml
  - WIN-190610201010.yaml
  - WIN-190620024610.yaml
  - WIN-190625024610.yaml
  - WIN-190725024610.yaml
  - WIN-190810170510.yaml
  - WIN-190810201010.yaml
  - WIN-190811201010.yaml
  - WIN-190813181020.yaml
  - WIN-190815181010.yaml
  - WIN-190826010110.yaml
  - WIN-191030201010.yaml
  - WIN-191224222300.yaml
  - WIN-200609225055.yaml
  - WIN-200902020333.yaml
  - WIN-201009173318.yaml
  - WIN-201009183000.yaml
  - WIN-201012004336.yaml
  - WIN-201012183248.yaml
- resources
- scripts
- signatures
- .gitignore
- Dockerfile
- LICENSE
- README.md

ThreatHunter-Playbook / playbooks / WIN-201012004336.yaml

Cyb3rWard0g updated notebooks, metadata files 27f8545 · 2 years ago History

Code Blame 159 lines (159 loc) · 7.04 KB Raw

```yaml
title: SMB Create Remote File
id: WIN-201012004336
collaborators:
  - '@Cyb3rWard0g'
  - '@Cyb3rPandaH'
playbooks_related:
creation_date: 2020/10/12
modification_date: 2020/10/12
platform: Windows
attack_mappings:
  - tactics:
      - TA0008
    technique: T1021
    sub-technique: "002"
hypothesis: Adversaries might be creating a file remotely via the Server Message Block
technical_context: |-
  Client systems use the Common Internet File System (CIFS) Protocol to request file an
  The extended CIFS Protocol is known as the Server Message Block (SMB). The SMB2 CREAT
offensive_tradecraft: |-
  Adversaries leverage SMB to copy files over the network to either execute code remote
test_data:
  metadata: https://securitydatasets.com/notebooks/atomic/windows/lateral_movement/SDWI
  link: https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic
analytics:
  - name: Analytic I
    description: Look for non-system accounts SMB connecting (Tree Connect) to a file s
    data_sources:
      - name: File
        event_providers:
        - name: Microsoft-Windows-Security-Auditing
          data_model:
            - relationship: User accessed file share
              id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
              event_id: 5140
    logic: |-
      SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId,  Acces
      FROM sdTable
      WHERE LOWER(Channel) = 'security'
          AND (EventID = 5140)
          AND NOT ShareName LIKE '%IPC$'
          AND NOT SubjectUserName LIKE '%$'
  - name: Analytic II
    description: Look for non-system accounts SMB connecting (Tree Connect) to an IPC$
    data_sources:
      - name: File
        event_providers:
        - name: Microsoft-Windows-Security-Auditing
          data_model:
            - relationship: User accessed file share
              id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
              event_id: 5140
    logic: |-
      SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, b.SubjectLogonId, IpAd
      FROM sdTable b
      INNER JOIN (
          SELECT SubjectLogonId
          FROM sdTable
          FROM sdTable
          WHERE LOWER(Channel) = "security"
              AND EventID = 5140
              AND ShareName LIKE '%IPC$'
              AND NOT SubjectUserName LIKE '%$'
          ) a
      ON b.SubjectLogonId = a.SubjectLogonId
      WHERE LOWER(b.Channel) = 'security'
          AND b.EventID = 5140
          AND b.ShareName LIKE '%C$'
          AND NOT SubjectUserName LIKE '%$'
  - name: Analytic III
    description: Look for non-system accounts SMB accessing a file with write (0x2) acc
    data_sources:
      - name: File
        event_providers:
        - name: Microsoft-Windows-Security-Auditing
          data_model:
            - relationship: User accessed File
              id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
              event_id: 5145
    logic: |-
      SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId, IpAddr
      FROM sdTable
      WHERE LOWER(Channel) = "security"
          AND EventID = 5145
          AND ShareName LIKE '%C$'
          AND NOT SubjectUserName LIKE '%$'
          AND AccessMask = '0x2'
  - name: Analytic IV
    description: Look for non-system accounts SMB connecting (Tree Connect) to an IPC$
    data_sources:
      - name: File
        event_providers:
        - name: Microsoft-Windows-Security-Auditing
          data_model:
            - relationship: User accessed file share
              id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
              event_id: 5140
            - relationship: User accessed File
              id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
              event_id: 5145
    logic: |-
      SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, d.SubjectLogonId, IpAd
      FROM sdTable d
      INNER JOIN (
          SELECT b.SubjectLogonId
          FROM sdTable b
          INNER JOIN (
              SELECT SubjectLogonId
              FROM sdTable
              WHERE LOWER(Channel) = "security"
                  AND EventID = 5140
                  AND ShareName LIKE '%IPC$'
                  AND NOT SubjectUserName LIKE '%$'
          ) a
          ON b.SubjectLogonId = a.SubjectLogonId
          WHERE LOWER(b.Channel) = 'security'
              AND b.EventID = 5140
              AND b.ShareName LIKE '%C$'
      ) c
      ON d.SubjectLogonId = c.SubjectLogonId
      WHERE LOWER(d.Channel) = 'security'
          AND d.EventID = 5145
          AND d.ShareName LIKE '%C$'
          AND d.AccessMask = '0x2'
  - name: Analytic V
    description: Look for files that were accessed over the network with write (0x2) ac
    data_sources:
      - name: File
        event_providers:
        - name: Microsoft-Windows-Security-Auditing
          data_model:
            - relationship: User accessed File
              id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
```

```
       event_id: 5145
    - name: Microsoft-Windows-Sysmon/Operational
     data_model:
      - relationship: Process created File
       id: 109A870F-84A2-4CE4-948A-4773CD283F76
       event_id: 11
  logic: |-
   SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId, IpAddr
   FROM sdTable b
   INNER JOIN (
     SELECT LOWER(REVERSE(SPLIT(TargetFilename, '\'))[0]) as TargetFilename
     FROM sdTable
     WHERE Channel = 'Microsoft-Windows-Sysmon/Operational'
       AND Image = 'System'
       AND EventID = 11
   ) a
   ON LOWER(REVERSE(SPLIT(RelativeTargetName, '\'))[0]) = a.TargetFilename
   WHERE LOWER(b.Channel) = 'security'
     AND b.EventID = 5145
     AND b.AccessMask = '0x2'
known_bypasses:
false_positives:
additional_notes: |-
 * Baseline your environment to identify normal activity. Document all accounts creati
research_output:
references: |-
 * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/8341356c-ede3-4
 * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/e8fb45c1-a03d-
```