



159 lines (159 loc) · 7.04 KB


Code

Blame

Raw







```
1  title: SMB Create Remote File
2  id: WIN-201012004336
3  collaborators:
4    - '@Cyb3rWard0g'
5    - '@Cyb3rPandaH'
6  playbooks_related:
7  creation_date: 2020/10/12
8  modification_date: 2020/10/12
9  platform: Windows
10 attack_mappings:
11   - tactics:
12     - TA0008
13     technique: T1021
14     sub-technique: "002"
15 hypothesis: Adversaries might be creating a file remotely via the Server Message Block (SMB) Protocol
16 technical_context: |-
17     Client systems use the Common Internet File System (CIFS) Protocol to request file and print serv
18     The extended CIFS Protocol is known as the Server Message Block (SMB). The SMB2 CREATE Request pa
19 offensive_tradecraft: |-
20     Adversaries leverage SMB to copy files over the network to either execute code remotely or exfilt
21 test_data:
22   metadata: https://securitydatasets.com/notebooks/atomic/windows/lateral_movement/SDWIN-2008060157
23   link: https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lat
24 analytics:
25   - name: Analytic I
26     description: Look for non-system accounts SMB connecting (Tree Connect) to a file share that is
```

```
27     data_sources:
28       - name: File
29       event_providers:
30       - name: Microsoft-Windows-Security-Auditing
31       data_model:
32       - relationship: User accessed file share
33         id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
34         event_id: 5140
35     logic: |-
36       SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId, AccessMask
37       FROM sdTable
38       WHERE LOWER(Channel) = 'security'
39         AND (EventID = 5140)
40         AND NOT ShareName LIKE '%IPC$'
41         AND NOT SubjectUserName LIKE '%$'
42   - name: Analytic II
43     description: Look for non-system accounts SMB connecting (Tree Connect) to an IPC$ Share and ac
44     data_sources:
45       - name: File
46       event_providers:
47       - name: Microsoft-Windows-Security-Auditing
48       data_model:
49       - relationship: User accessed file share
50         id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
51         event_id: 5140
52     logic: |-
53       SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, b.SubjectLogonId, IpAddress, IpPor
54       FROM sdTable b
55       INNER JOIN (
56         SELECT SubjectLogonId
57         FROM sdTable
58         WHERE LOWER(Channel) = "security"
59           AND EventID = 5140
60           AND ShareName LIKE '%IPC$'
61           AND NOT SubjectUserName LIKE '%$'
62       ) a
63       ON b.SubjectLogonId = a.SubjectLogonId
64       WHERE LOWER(b.Channel) = 'security'
65         AND b.EventID = 5140
66         AND b.ShareName LIKE '%C$'
67         AND NOT SubjectUserName LIKE '%$'
68   - name: Analytic III
69     description: Look for non-system accounts SMB accessing a file with write (0x2) access mask via
70     data_sources:
71       - name: File
72       event_providers:
```

```
73     - name: Microsoft-Windows-Security-Auditing
74       data_model:
75         - relationship: User accessed File
76           id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
77           event_id: 5145
78     logic: |-
79       SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId, IpAddress, IpPort,
80       FROM sdTable
81       WHERE LOWER(Channel) = "security"
82             AND EventID = 5145
83             AND ShareName LIKE '%C$'
84             AND NOT SubjectUserName LIKE '%$'
85             AND AccessMask = '0x2'
86   - name: Analytic IV
87     description: Look for non-system accounts SMB connecting (Tree Connect) to an IPC$ Share and ac
88     data_sources:
89       - name: File
90         event_providers:
91         - name: Microsoft-Windows-Security-Auditing
92           data_model:
93             - relationship: User accessed file share
94               id: 53DE6467-D39D-434B-9EF7-69C7F4098DF9
95               event_id: 5140
96             - relationship: User accessed File
97               id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
98               event_id: 5145
99     logic: |-
100       SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, d.SubjectLogonId, IpAddress, IpPor
101       FROM sdTable d
102       INNER JOIN (
103         SELECT b.SubjectLogonId
104         FROM sdTable b
105         INNER JOIN (
106           SELECT SubjectLogonId
107           FROM sdTable
108           WHERE LOWER(Channel) = "security"
109                 AND EventID = 5140
110                 AND ShareName LIKE '%IPC$'
111                 AND NOT SubjectUserName LIKE '%$'
112         ) a
113         ON b.SubjectLogonId = a.SubjectLogonId
114         WHERE LOWER(b.Channel) = 'security'
115               AND b.EventID = 5140
116               AND b.ShareName LIKE '%C$'
117       ) c
118       ON d.SubjectLogonId = c.SubjectLogonId
```

```
118         ON d.SubjectLogonId = c.SubjectLogonId
119         WHERE LOWER(d.Channel) = 'security'
120             AND d.EventID = 5145
121             AND d.ShareName LIKE '%C$'
122             AND d.AccessMask = '0x2'
123     - name: Analytic V
124       description: Look for files that were accessed over the network with write (0x2) access mask via
125       data_sources:
126         - name: File
127           event_providers:
128             - name: Microsoft-Windows-Security-Auditing
129               data_model:
130                 - relationship: User accessed File
131                   id: 2A9FC474-29C0-4582-9DA8-1F4197874F8C
132                   event_id: 5145
133             - name: Microsoft-Windows-Sysmon/Operational
134               data_model:
135                 - relationship: Process created File
136                   id: 109A870F-84A2-4CE4-948A-4773CD283F76
137                   event_id: 11
138       logic: |-
139         SELECT `@timestamp`, Hostname, ShareName, SubjectUserName, SubjectLogonId, IpAddress, IpPort,
140         FROM sdTable b
141         INNER JOIN (
142             SELECT LOWER(REVERSE(SPLIT(TargetFilename, '\'))[0]) as TargetFilename
143             FROM sdTable
144             WHERE Channel = 'Microsoft-Windows-Sysmon/Operational'
145                 AND Image = 'System'
146                 AND EventID = 11
147         ) a
148         ON LOWER(REVERSE(SPLIT(RelativeTargetName, '\'))[0]) = a.TargetFilename
149         WHERE LOWER(b.Channel) = 'security'
150             AND b.EventID = 5145
151             AND b.AccessMask = '0x2'
152       known_bypasses:
153       false_positives:
154       additional_notes: |-
155         * Baseline your environment to identify normal activity. Document all accounts creating files over
156       research_output:
157       references: |-
158         * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/8341356c-ede3-4e1c-a056-3de
159         * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/e8fb45c1-a03d-44ca-b7ae-47
```