

📄

OTRF / ThreatHunter-Playbook

Public

🔔

Notifications

🍴

Fork807

★

Star4k

&lt;&gt; Code🕒 Issues6🔗 Pull requests2🎬 Actions📁 Projects🛡 Security📈 Insights

📁

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

&gt;

📁

&gt;

📁

📄

.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

📄

📥

🔗

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

16

technical\_context: |-

17

Client systems use the Common Internet File System (CIFS) Protocol to request file an

18

The extended CIFS Protocol is known as the Server Message Block (SMB). The SMB2 CREAT

19

offensive\_tradecraft: |-

20

Adversaries leverage SMB to copy files over the network to either execute code remote

21

test\_data:

22

metadata: https://securitydatasets.com/notebooks/atomic/windows/lateral\_movement/SDWI

23

link: https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic

24

analytics:

25

- name: Analytic I

26

description: Look for non-system accounts SMB connecting (Tree Connect) to a file s

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, Acces

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\$

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, IpAd

54

FROM sdTable b

55

INNER JOIN (

56

SELECT SubjectLogonId

57

FROM sdTable

Page 1 of 3

```
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
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
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
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
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$'
117     ) c
118     ON d.SubjectLogonId = c.SubjectLogonId
119     WHERE LOWER(d.Channel) = 'security'
120         AND d.EventID = 5145
121         AND d.ShareName LIKE '%C$'
122         AND d.AccessMask = '0x2'
123 - name: Analytic V
124 description: Look for files that were accessed over the network with write (0x2) access
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, IpAddr
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 creati
156     research_output:
157     references: |-
158       * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb/8341356c-ed3-4
159       * https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-smb2/e8fb45c1-a03d-
```