



splunk / security\_content Public

Notifications Fork 359 Star 1.3k

<> Code Issues 21 Pull requests 10 Discussions Actions Projects Wiki S

security\_content / detections / endpoint / office\_spawning\_control.yml

82 lines (82 loc) · 5 KB

Code Blame Raw Copy Download Edit

```
1  name: Office Spawning Control
2  id: 053e027c-10c7-11ec-8437-acde48001122
3  version: 7
4  date: '2024-09-30'
5  author: Michael Haag, Splunk
6  status: production
7  type: TTP
8  description: The following analytic identifies instances where `control.exe` is spawned by a Micros
9  data_source:
10 - Sysmon EventID 1
11 - Windows Event Log Security 4688
12 - CrowdStrike ProcessRollup2
13 search: '| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as last
14 how_to_implement: The detection is based on data that originates from Endpoint Detection and Respor
15 known_false_positives: Limited false positives should be present.
16 references:
17 - https://strontic.github.io/xcyclopedia/library/control.exe-1F13E714A0FEA8887707DFF49287996F.html
18 - https://app.any.run/tasks/36c14029-9df8-439c-bba0-45f2643b0c70/
19 - https://attack.mitre.org/techniques/T1218/011/
20 - https://www.echotrail.io/insights/search/control.exe/
21 - https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
22 - https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.002/T1218.002.yaml1
23 - https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trojanized-onenote-document-leads
24 drilldown_searches:
25 - name: View the detection results for - "$dest$"
26   search: '%original_detection_search% | search dest = "$dest$"'
```

```
27     earliest_offset: $info_min_time$
28     latest_offset: $info_max_time$
29   - name: View risk events for the last 7 days for - "$dest$"
30     search: '| from datamodel Risk.All_Risk | search normalized_risk_object IN ("$dest$") starthoursa
31     earliest_offset: $info_min_time$
32     latest_offset: $info_max_time$
33   tags:
34     analytic_story:
35     - Spearphishing Attachments
36     - Microsoft MSHTML Remote Code Execution CVE-2021-40444
37   asset_type: Endpoint
38   confidence: 100
39   cve:
40   - CVE-2021-40444
41   impact: 80
42   message: An instance of $parent_process_name$ spawning $process_name$ was identified on endpoint
43   mitre_attack_id:
44   - T1566
45   - T1566.001
46   observable:
47   - name: dest
48     type: Hostname
49     role:
50     - Victim
51   - name: parent_process_name
52     type: Process
53     role:
54     - Attacker
55   - name: process_name
56     type: Process
57     role:
58     - Attacker
59   product:
60   - Splunk Enterprise
61   - Splunk Enterprise Security
62   - Splunk Cloud
63   required_fields:
64   - Processes.dest
65   - Processes.user
66   - Processes.parent_process_name
67   - Processes.parent_process
68   - Processes.original_file_name
69   - Processes.process_name
70   - Processes.process
71   - Processes.process_id
72   - Processes.parent_process_path
```

```
73     - Processes.process_path
74     - Processes.parent_process_id
75     risk_score: 80
76     security_domain: endpoint
77     tests:
78     - name: True Positive Test
79       attack_data:
80       - data: https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack_techr
81         source: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
82         sourcetype: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
```