```yaml
name: Office Spawning Control
id: 053e027c-10c7-11ec-8437-acde48001122
version: 7
date: '2024-09-30'
author: Michael Haag, Splunk
status: production
type: TTP
description: The following analytic identifies instances where `control.exe` is spawned
data_source:
- Sysmon EventID 1
- Windows Event Log Security 4688
- CrowdStrike ProcessRollup2
search: '| tstats `security_content_summariesonly` count min(_time) as firstTime max(_t
how_to_implement: The detection is based on data that originates from Endpoint Detectio
known_false_positives: Limited false positives should be present.
references:
- https://strontic.github.io/xcyclopedia/library/control.exe-1F13E714A0FEA8887707DFF492
- https://app.any.run/tasks/36c14029-9df8-439c-bba0-45f2643b0c70/
- https://attack.mitre.org/techniques/T1218/011/
- https://www.echotrail.io/insights/search/control.exe/
- https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444
- https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1218.002/T1218.00
- https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/trojanized-onenote-do
drilldown_searches:
- name: View the detection results for - "$dest$"
  search: '%original_detection_search% | search  dest = "$dest$"'
  earliest_offset: $info_min_time$
  latest_offset: $info_max_time$
- name: View risk events for the last 7 days for - "$dest$"
  search: '| from datamodel Risk.All_Risk | search normalized_risk_object IN ("$dest$")
  earliest_offset: $info_min_time$
  latest_offset: $info_max_time$
tags:
  analytic_story:
  - Spearphishing Attachments
  - Microsoft MSHTML Remote Code Execution CVE-2021-40444
  asset_type: Endpoint
  confidence: 100
  cve:
  - CVE-2021-40444
  impact: 80
  message: An instance of $parent_process_name$ spawning $process_name$ was identified
  mitre_attack_id:
  - T1566
  - T1566.001
  observable:
  - name: dest
    type: Hostname
    role:
    - Victim
  - name: parent_process_name
    type: Process
    role:
    - Attacker
  - name: process_name
    type: Process
    role:
```

powershell_processing_stream...
powershell_remote_services_ad...
powershell_remote_thread_to_...
powershell_remove_windows_...
powershell_script_block_with_u...
powershell_start_bitstransfer.yml

```
      role:
      - Attacker
    product:
    - Splunk Enterprise
    - Splunk Enterprise Security
    - Splunk Cloud
    required_fields:
    - Processes.dest
    - Processes.user
    - Processes.parent_process_name
    - Processes.parent_process
    - Processes.original_file_name
    - Processes.process_name
    - Processes.process
    - Processes.process_id
    - Processes.parent_process_path
    - Processes.process_path
    - Processes.parent_process_id
    risk_score: 80
    security_domain: endpoint
  tests:
  - name: True Positive Test
    attack_data:
    - data: https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/
      source: XmlWinEventLog:Microsoft-Windows-Sysmon/Operational
      sourcetype: XmlWinEventLog
```