Files

0dd6de3

Go to file

.github
automated_detection_testing
bin
dashboards
deployments
detections
cloud
deprecated
endpoint
7zip_commandline_to_smb_sh...
access_lsass_memory_for_dum...
account_discovery_with_net_a...
all_backup_logs_for_host.yml
allow_file_and_printing_sharing...
allow_inbound_traffic_by_firew...
allow_inbound_traffic_in_firewa...
allow_network_discovery_in_fir...
allow_operation_with_consent_...
anomalous_usage_of_7zip.yml
any_powershell_downloadfile.y...
any_powershell_downloadstrin...
attacker_tools_on_endpoint.yml
attempt_to_add_certificate_to_...
attempt_to_stop_security_servi...
attempted_credential_dump_fr...
baseline_of_command_line_len...
batch_file_write_to_system32.y...
bcdedit_failure_recovery_modif...
bits_job_persistence.yml
bitsadmin_download_file.yml
certutil_download_with_urlcach...
certutil_download_with_verifyc...
certutil_exe_certificate_extracti...
certutil_with_decode_argumen...
chcp_command_execution.yml
clear_unallocated_sector_using...

security_content / detections / endpoint / petitpotam_network_share_access_request.yml

root Added detection testing service results inWindows Desired Access ... 052594e · 3 years ago History

Code Blame 70 lines (67 loc) · 2.64 KB · Raw

```yaml
name: PetitPotam Network Share Access Request
id: 95b8061a-0a67-11ec-85ec-acde48001122
version: 1
date: '2021-08-31'
author: Michael Haag, Mauricio Velazco, Splunk
type: TTP
datamodel: []
description: 'The following analytic utilizes Windows Event Code 5145, "A network
  share object was checked to see whether client can be granted desired access". During
  our research into PetitPotam, CVE-2021-36942, we identified the ocurrence of this
  event on the target host with specific values. \

  To enable 5145 events via Group Policy - Computer Configuration->Polices->Windows
  Settings->Security Settings->Advanced Audit Policy Configuration. Expand this node,
  go to Object Access (Audit Polices->Object Access), then select the Setting Audit
  Detailed File Share Audit \

  It is possible this is not enabled by default and may need to be reviewed and enabled
  \

  During triage, review parallel security events to identify further suspicious activit
search: '`wineventlog_security` Account_Name="ANONYMOUS LOGON" EventCode=5145 Relative_
  | stats count min(_time) as firstTime max(_time) as lastTime by dest, Security_ID,
  Share_Name, Source_Address, Accesses, Message | `security_content_ctime(firstTime)`
  | `security_content_ctime(lastTime)` | `petitpotam_network_share_access_request_filte
how_to_implement: Windows Event Code 5145 is required to utilize this analytic and
  it may not be enabled in most environments.
known_false_positives: False positives have been limited when the Anonymous Logon
  is used for Account Name.
references:
- https://attack.mitre.org/techniques/T1187/
- https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=5
- https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/event-51
tags:
  analytic_story:
  - PetitPotam NTLM Relay on Active Directory Certificate Services
  dataset:
  - https://media.githubusercontent.com/media/splunk/attack_data/master/datasets/attack
  kill_chain_phases:
  - Exploitation
  - Lateral Movement
  mitre_attack_id:
  - T1187
  product:
  - Splunk Enterprise
  - Splunk Enterprise Security
  - Splunk Cloud
  required_fields:
  - _time
  - dest
  - Security_ID
  - Share_Name
  - Source_Address
  - Accesses
  - Message
  security_domain: endpoint
```

clop_common_exec_parameter....
clop_ransomware_known_servi...
cmd_echo_pipe___escalation.yml
cmlua_or_cmstplua_uac_bypas...
cobalt_strike_named_pipes.yml
common_ransomware_extensi...

```
    security_domain: endpoint
    impact: 80
    confidence: 70
    risk_score: 56
    context:
    - Source:Endpoint
    - Stage:Credential Access
    message: A remote host is enumerating a $dest$ to identify permissions. This is
      a precursor event to CVE-2021-36942, PetitPotam.
    observable:
    - name: dest
      type: Hostname
      role:
      - Victim
    automated_detection_testing: passed
```