Alexander Ticket

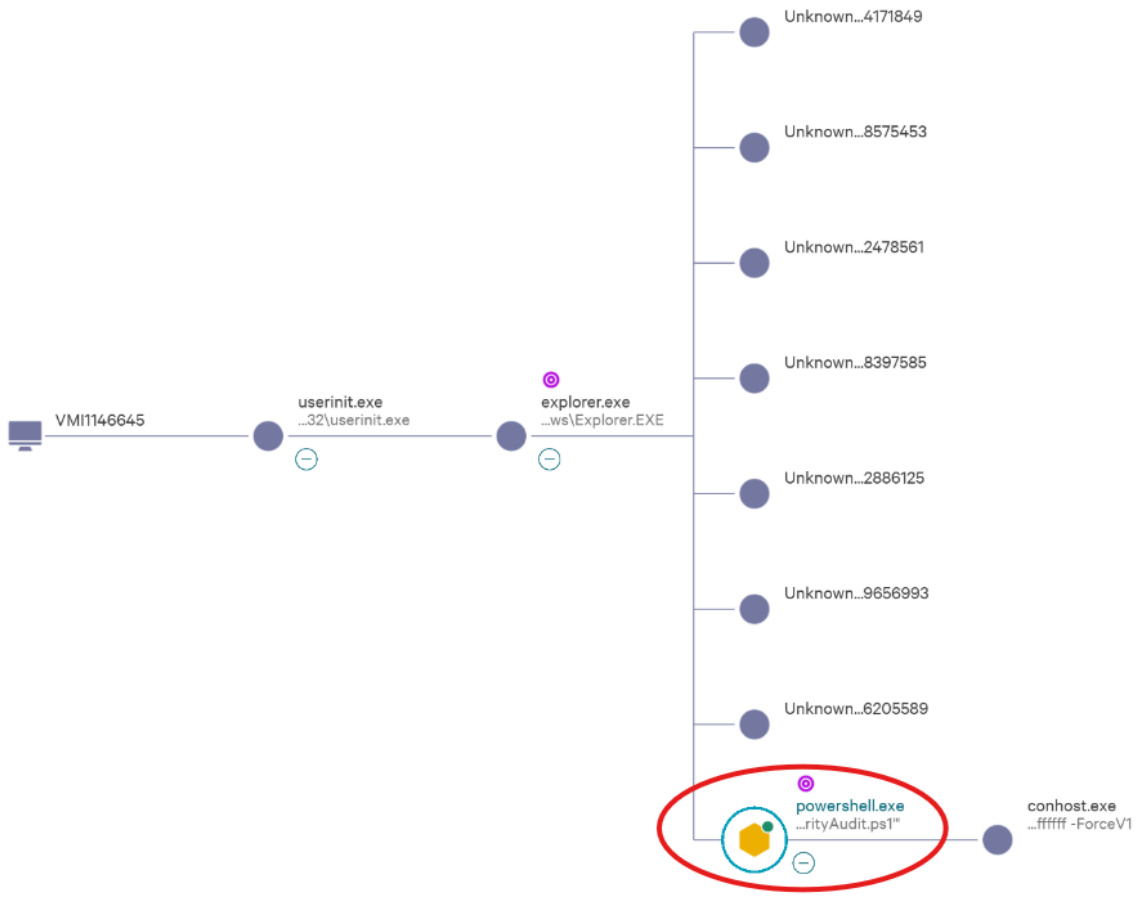
Note: This report has been sanitized for public sharing.

All internal IPs, hostnames, and Splunk URLs have been redacted or replaced with simulated values.

Report was originally prepared for Jira; internal console links are not publicly accessible. Query references shown for context

The Summary :

The related PowerShell script is considered potentially malicious as it shares patterns with known malicious scripts.



CrowdStrike Link:

- **Incident(CrowdScore):**

(internal link, redacted for confidentiality)

- **Endpoint Detection:**

(internal link, redacted for confidentiality)

Description

Suspicious PowerShell activity was detected on host [redacted-host] under the **Administrator** account. The script modified the execution policy to *Bypass* and executed *DocumentSecurityAudit.ps1* from the Downloads folder — a technique often used to evade security controls. Although the process was blocked and the file quarantined, this activity maps to **MITRE ATT&CK T1059.001 (PowerShell Execution)** and may indicate the start of a larger intrusion attempt.

- **Host Information:**

Hostname: [redacted-host]

Operating System: Windows Server 2022

IP Address: [redacted internal IP]

Local IP Address: [redacted]

Host Type: Server

- **User Information:**

Username: Administrator

Local Admin: Yes

Login Type: REMOTE_INTERACTIVE (remote terminal server session)

Login Time: Dec. 4, 2024, 13:01:49

Login Domain: [internal-domain-redacted]

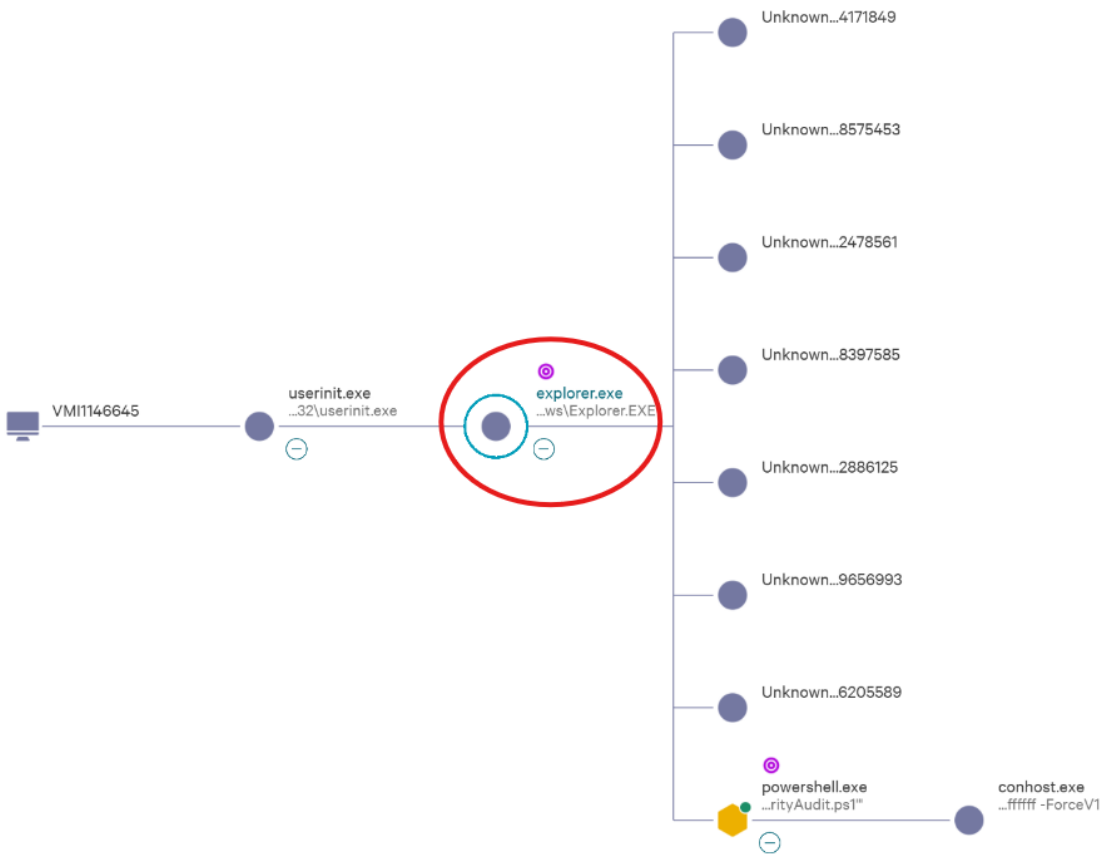
- **Tactic & Technique:**

Execution via PowerShell

MITRE ATT&CK ID: T1059.001

Investigation Findings and Analysis:

Observed Command 1:



The process explorer.exe did not exhibit malicious behavior itself but served as the parent process for suspicious script execution. The binary (SHA256: `53f36699c35c8f2360608a79f0809ba888c61f15886ae2b1f209a3e9b896cba7`, not detected as malicious) was launched from `C:\Windows\explorer.exe` on June 23, 2025, at 16:33:45 on host VMI1146645 (Windows Server 2022).

During execution, Explorer created shortcut files in the *Recent* folder, suggesting user interaction with a potentially malicious script:

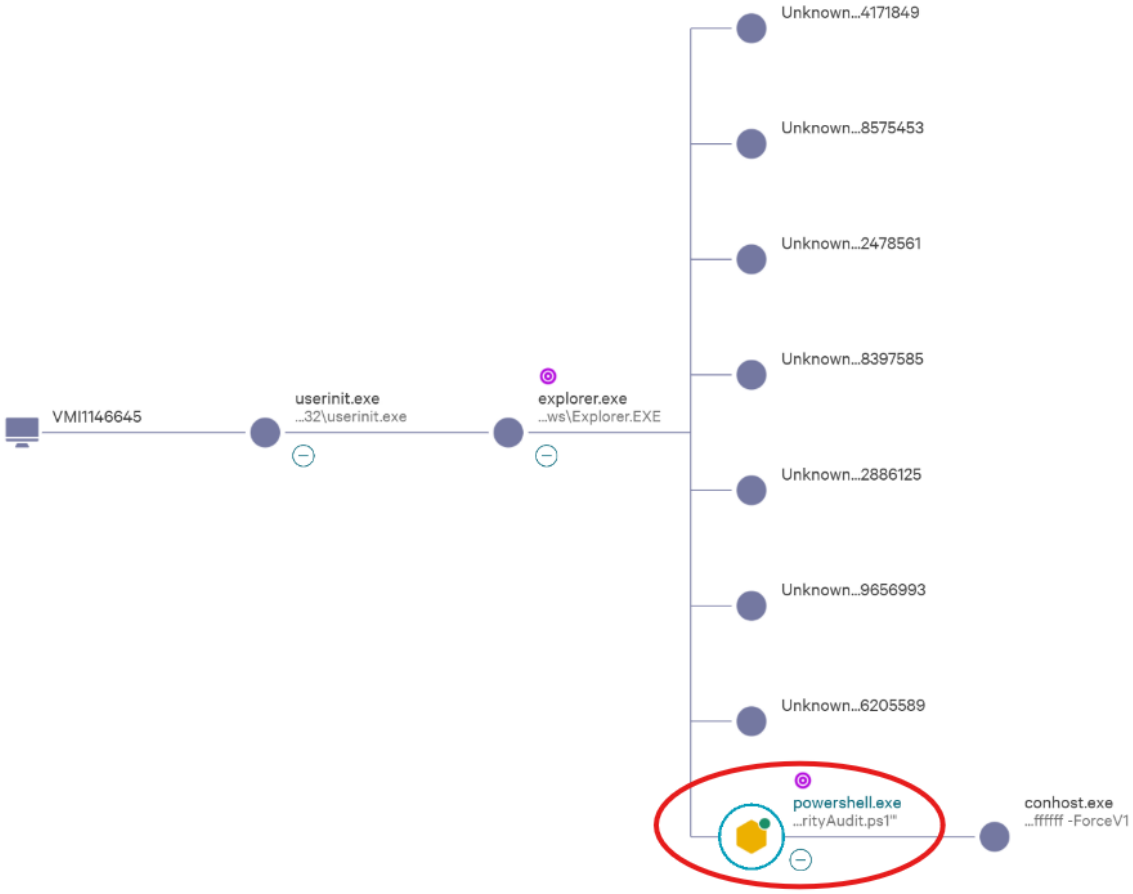
- **`DocumentSecurityAudit.ps1.lnk`**
- **`Downloads (2).lnk`**

Following this action, a PowerShell process was spawned with the command line:

```
powershell.exe -Command if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'C:\Users\Administrator\Downloads\DocumentSecurityAudit.ps1'
```

This behavior demonstrates an attempt to bypass the default PowerShell execution policy, which is a common technique used to execute potentially malicious scripts. The activity maps to MITRE ATT&CK T1059.001 (PowerShell Execution) and may be indicative of post-exploitation behavior or staging of a secondary payload under the Administrator account via remote interactive session.

Observed Command 2:



Command line

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command"
"if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope
Process Bypass }; &
'C:\Users\Administrator\Downloads\DocumentSecurityAudit.ps1'"
```

File path:

```
\Device\HarddiskVolume2\Windows\System32\WindowsPowerShell\v1.0\powershell.
exe
```

Executable SHA256:
38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033

Triggering indicator:
Associated IOC (SHA256):
64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485

Timestamp:
Jun. 23, 2025 16:34:50

Detection:
Execution via PowerShell

CrowdStrike Actions Taken

- Operation was blocked ☑
- File *DocumentSecurityAudit.ps1* was quarantined ☑
  (C:\Users\Administrator\Downloads\)

Partial raw command observed :

{"ProcessStartTime":1750710890,"ProcessEndTime":1750710891,"ProcessId":5562256338213,"ParentProcessId":5562194611777,"Hostname":" [redacted-host] ","UserName":"Administrator","Name":"Suspicious Activity","Description":"A PowerShell script related to this process is likely malicious or shares characteristics with known malicious scripts. Review the script.","Severity":50,"SeverityName":"Medium","FileName":"powershell.exe","FilePath":"\\Device\\HarddiskVolume2\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe","CommandLine":"\"C:\\Windows\\System32\\WindowsPowerShell\\v1.0\\powershell.exe\" \"-Command\" \"if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; \u0026 'C:\\Users\\Administrator\\Downloads\\DocumentSecurityAudit.ps1'\"","SHA256String":"64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485","MD5String":"dd6f4b7818a253887b8ea86515f6fb7d","SHA1String":"0000000000000000000000000000000000000000","LogonDomain":" [internal-domain-redacted] ","FalconHostLink":"https://falcon.us-2.crowdstrike.com/activity-v2/detections/55ff35c57f0441f19baad0a47c239f7d:ind:fd0ae32b624a4baa83845321c1cf0e52:5562256338213-10142-776464?_cid=g04000se3r2o4ldzhrvino6eqba52w6a","AgentId":"fd0ae32b624a4baa83845321c1cf0e52","IOCType":"hash_sha256","IOCValue":"64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485","CompositeId":"55ff35c57f0441f19baad0a47c239f7d:ind:fd0ae32b624a4baa83845321c1cf0e52:5562256338213-10142-776464","QuarantineFiles":[{"ImageFileName":"\\Device\\HarddiskVolume2\\Users\\Administrator\\Downloads\\DocumentSecurityAudit.ps1","SHA256HashData":"64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485"}],"LocalIP":" [redacted internal IP]","MACAddress":"00-50-56-49-71-48","Tactic":"Execution","Technique":"PowerShell","Objective":"Follow Through","PatternDispositionDescription":"Quarantine file + Operation Blocked","PatternDispositionValue":1152,"PatternDispositionFlags":{"Indicator":false,"Detect":false,"InddetMask":false,"SensorOnly":false,"Rooting":false,"KillProcess":false,"KillSubProcess":false,"QuarantineMachine":false,"QuarantineFile":true,"PolicyDisabled":false,"KillParent":false,"OperationBlocked":true,"ProcessBlocked":false,"RegistryOperationBlocked":false,"CriticalProcessDisabled":false,"BootupSafeguardEnabled":false,"FsOperationBlocked":false,"HandleOperationDowngraded":false,"KillActionFailed":false,"BlockingUnsupportedOrDisabled":false,"SuspendProcess":false,"SuspendParent":false,"ContainmentFileSystem":false},"ParentImageFileName":"explorer.exe","ParentCommandLine":"C:\\Windows\\Explorer.EXE","GrandParentImageFileName":"userinit.exe","GrandParentCommandLine":"C:\\Windows\\system32\\userinit.exe","HostGroups":"c6cffe1d95944fe48f105a75c4bf4ec6","AssociatedFile":"\\??\\C:\\Users\\Administrator\\Downloads\\DocumentSecurityAudit.ps1","PatternId":10142,"SourceVendors":"CrowdStrike","SourceProducts":"Falcon Insight","DataDomains":"Endpoint","AggregateId":"aggind:fd0ae32b624a4baa83845321c1cf0e52:330713051389","Type":"ldt","ParentImageFilePath":"\\Device\\HarddiskVolume2\\

Windows\\explorer.exe","GrandParentImageFilePath":"\\Device\\HarddiskVolume2\\Windows\\System32\\userinit.exe","LocalIPv6":"","PlatformId":"0","PlatformName":"Windows","CustomerIdString":"55ff35c57f0441f19baad0a47c239f7d","UTCTimestamp":1750710955,"Nonce":4420129881392241730,"AgentIdString":"fd0ae32b624a4baa83845321c1cf0e52","cid":"55ff35c57f0441f19baad0a47c239f7d","eid":118,"timestamp":"2025-06-23T20:35:55Z","EventType":"Event_ExternalApiEvent","ExternalApiType":"Event_EppDetectionSummaryEvent"}

Jun. 23, 2025 16:35:55.000

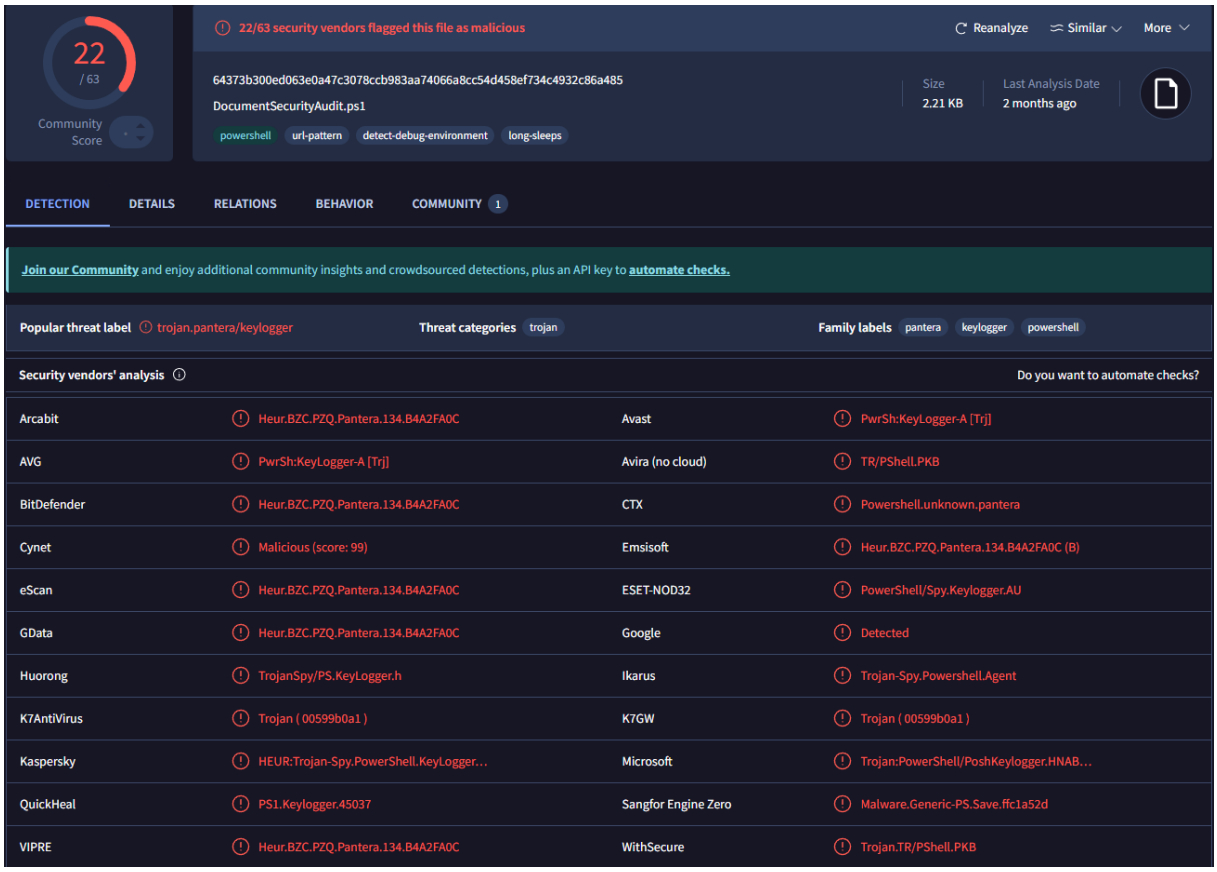
#repo: detections
#repo.cid: 55ff35c57f0441f19baad0a47c239f7d
#type: AssociateTreeIdWithRoot_duplicate
@id: z6P8c3k08cjstMQGzVYZ5CAM_12_0_1750710891
@ingesttimestamp: 1750710893528

Associated IOC Hash_sha256

This hash is detected as malicious by VirusTotal, with 22 out of 63 antivirus engines flagging it as harmful. Multiple security vendors classify the file as a PowerShell-based keylogger / Trojan-Spy, indicating its use for credential theft and surveillance activities.

64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485

[here|https://www.virustotal.com/gui/file/64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485]



IOC Summary

Filename: DocumentSecurityAudit.ps1

SHA256:
64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485

File path: C:\Users\Administrator\Downloads\DocumentSecurityAudit.ps1

Parent process: explorer.exe (SHA256:
53f36699c35c8f2360608a79f0809ba888c61f15886ae2b1f209a3e9b896cba7)

Execution process: powershell.exe (SHA256:
38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033)

Analysis

The process launched the legitimate Windows PowerShell interpreter but was abused to execute a suspicious script located in the user's Downloads folder.

Command line breakdown:

- 🔸 **powershell.exe** → **Launches the PowerShell interpreter.**
- 🔸 **-Command** → Instructs PowerShell to run the provided string as code.
- 🔸 **if((Get-ExecutionPolicy) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }** → Temporarily sets the execution policy to Bypass, allowing execution of unsigned scripts. This is a known evasion tactic to disable PowerShell script restrictions.
- 🔸 **& 'C:\Users\Administrator\Downloads\DocumentSecurityAudit.ps1'** → Executes the downloaded script directly from the user's folder.

Suspicious behavior:

- **The script was identified by multiple antivirus engines on VirusTotal (22/63) as malicious.**
- **Execution policy tampering indicates an attempt to weaken PowerShell's default security controls.**
- **Running unsigned scripts under the Administrator account via a remote interactive session increases the risk of system compromise.**

Potential Impact

1. **Bypassing PowerShell Restrictions**
   The command line showed an explicit change of the execution policy to Bypass:

   ```
   if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }
   ```

   This bypass allowed the script *DocumentSecurityAudit.ps1* to run despite not being signed, reducing built-in PowerShell protections.

2. **Execution of Malicious Script**
   The script *DocumentSecurityAudit.ps1* (SHA256: `64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485`) was launched from the Downloads folder under the Administrator account.
   VirusTotal reports show 22/63 detections, with multiple vendors classifying it as a PowerShell keylogger / Trojan-Spy, indicating functionality for credential theft and surveillance.

3. **Privilege Abuse**
   Execution occurred under the Administrator account via a Remote Interactive session. Running malicious scripts with elevated privileges increases risk of:
   - **Disabling security controls.**
   - **Modifying critical system settings.**
   - **Deploying additional payloads with unrestricted access.**
4. **Persistence Risk**
   Although persistence mechanisms were not directly observed in this detection, malicious PowerShell scripts typically establish persistence through:
   - **Scheduled tasks.**
   - **Registry Run/autorun keys.**
   - **Malicious Windows services.**
5. **Further Payload Delivery**
   With ExecutionPolicy set to Bypass, the script could have downloaded and executed secondary payloads (e.g., additional spyware, RATs, or ransomware). Even if not observed here, the capability is present due to the relaxed policy.
6. **Living-off-the-Land Techniques**
   The activity relied on the trusted system binary powershell.exe (SHA256: `38f4384643b3fa0de714d2367b712c2e0fa1c89e2cfd131ae6b831ad962b1033`). Using native tools enables attackers to blend in with legitimate admin activity and evade traditional detection.
7. **Business Impact**
   If leveraged further, the malicious script could lead to:
   - **Theft of administrator credentials.**
   - **Unauthorized access to sensitive systems and data.**
   - **Deployment of additional malware, including ransomware.**
   - **Operational disruption and reputational damage to the organization.**

Host Verification

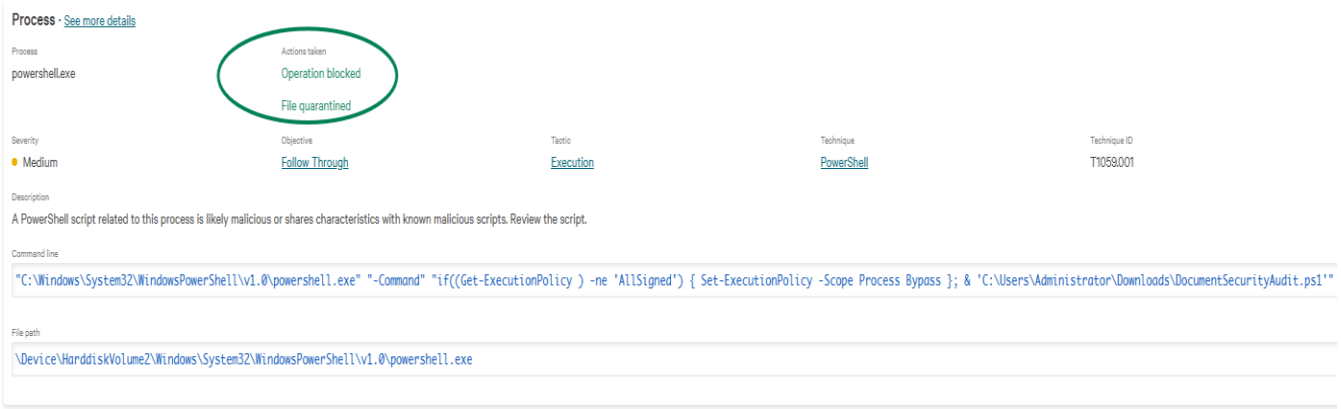
The host [redacted-host] was accessed for verification. A manual inspection of the Downloads directory was performed to check for the presence of the suspicious script ***DocumentSecurityAudit.ps1*****.**

```
C:\> cd C:\Users\Administrator\Downloads\

C:\Users\Administrator\Downloads

C:\Users\Administrator\Downloads> ls

Directory listing for C:\Users\Administrator\Downloads -

Name                                Type            Size (bytes)       Size (MB) Last Modified (UTC+2)     Created (UTC+2)
----                                ----            ------------       --------- ----------------------    ---------------
desktop.ini                         .ini                     282              0 1/2/2023 9:09:09 PM       1/2/2023 9:09:09 PM
managers.xlsm                       .xlsm                   9290          0.009 7/25/2025 5:15:27 PM      7/25/2025 5:15:27 PM

C:\Users\Administrator\Downloads> cat DocumentSecurityAudit.ps1

Check your filename. Couldn't find 'DocumentSecurityAudit.ps1'

C:\Users\Administrator\Downloads> cat __PSScriptPolicyTest_myeg4rrh.pfz.ps1

Check your filename. Couldn't find '__PSScriptPolicyTest_myeg4rrh.pfz.ps1'
```

As shown in the results, the file was not found in the directory. Only benign files (`desktop.ini`, `managers.xlsm`) were present. This confirms that the malicious script is no longer present on the host.

Response:

The malicious PowerShell script execution was blocked by CrowdStrike, and the suspicious file *DocumentSecurityAudit.ps1* (SHA256: `64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485`) was quarantined on the host [redacted-host] on Jun. 23, 2025 at 16:34:54 and later purged, preventing further execution or potential compromise.



Overall Analyst Assessment:

The PowerShell script *DocumentSecurityAudit.ps1* was executed from the **Downloads** directory via `powershell.exe` with the command line:

```
if((Get-ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass };

& 'C:\Users\Administrator\Downloads\DocumentSecurityAudit.ps1'
```

This shows a deliberate attempt to **bypass the default PowerShell execution policy** and run unsigned code.

The process ran under the **Administrator** account on host [redacted-host] (Windows Server 2022) in a **remote interactive session**, increasing the potential impact due to elevated privileges.

The file *DocumentSecurityAudit.ps1* (SHA256: `64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485`) was identified as malicious by **VirusTotal (22/63 detections)**, with several vendors classifying it as a **PowerShell keylogger / Trojan-Spy**. This strongly indicates functionality related to **credential theft and surveillance**.

CrowdStrike detected the activity as **MaliciousPowershell (T1059.001 – PowerShell Execution)**, blocked the operation, and quarantined the file at **16:34:54 on June 23, 2025**. The file was later purged from the system.

Although the malicious execution was prevented, the event demonstrates use of **defense evasion** (ExecutionPolicy Bypass) and **living-off-the-land techniques** (using `powershell.exe`). If successful, this script could have enabled **keylogging, credential compromise, and additional malware delivery** under Administrator-level access.

Mini Attack Visualization

[User (**Administrator**) initiates action via **explorer.exe**]

↓

[**explorer.exe** creates Recent shortcuts: *DocumentSecurityAudit.ps1.lnk*, *Downloads (2).lnk*]

↓

[**powershell.exe** launched from `C:\Windows\System32\WindowsPowerShell\v1.0\`]

↓

[**Execution policy bypass**: `Set-ExecutionPolicy -Scope Process Bypass`]

↓

[*DocumentSecurityAudit.ps1* executed from **Downloads** folder]

↓

[Script hash: `64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485`]

↓

[Classified by multiple vendors on VirusTotal as **PowerShell Keylogger / Trojan-Spy**]

↓

[Process flagged as **MaliciousPowershell (T1059.001)**]

↓

[CrowdStrike blocks execution and quarantines *DocumentSecurityAudit.ps1*]

RECOMMENDED ACTIONS:

1. Host Verification

- Confirm *DocumentSecurityAudit.ps1* (SHA256: `64373b3…6a485`) is removed (CrowdStrike shows quarantined & purged).
- Scan host [redacted-host] for other `.ps1` files, shortcuts, or suspicious artifacts.

2. Persistence & Malware Cleanup

- Check and remove any malicious scheduled tasks, registry autoruns, or services.
- Verify no additional copies of the script exist elsewhere.

3. Credential Hygiene

- Reset **Administrator** password (used in remote interactive session).
- Review login history for unusual activity.

4. PowerShell Hardening

- Enforce stricter execution policies (e.g., `AllSigned`).
- Restrict script execution from untrusted folders (Downloads).
- Enable Script Block & Module Logging.

5. IOC Hunting

- Sweep environment for IOC hash: `64373b300ed063e0a47c3078ccb983aa74066a8cc54d458ef734c4932c86a485`.
- Hunt for suspicious `explorer.exe → powershell.exe` chains.

6. Coordination

- Escalate results to Incident Response team.