Sign in

Azure / **Azure-Sentinel** Public

Notifications | Fork 3k | Star 4.6k

Code | Issues 26 | Pull requests 84 | Actions | Projects | Wiki | Security | Insig

Azure-Sentinel / Hunting Queries / Microsoft 365 Defender / Ransomware / DEV-0270 / **Email data exfiltration via PowerShell.yaml**

14 lines (14 loc) · 500 Bytes

Code | Blame | Raw

```
id: 1115e499-45a0-470c-b0ec-e2f204831341
name: Email data exfiltration via PowerShell
description: |
  Identify email exfiltration conducted by PowerShell.
requiredDataConnectors:
- connectorId: MicrosoftThreatProtection
  dataTypes:
  - DeviceProcessEvents
tactics:
- Exfiltration
query: |
  DeviceProcessEvents
  | where FileName =~ 'powershell.exe'
  | where ProcessCommandLine has_all('Add-PSSnapin', 'Get-Recipient', '-ExpandProperty', 'EmailAddr
```