Files

7e6aa43

Go to file

.azure-pipelines
.github
.script
.vscode
ASIM
BYOML
Dashboards
DataConnectors
Detections
Exploration Queries
Functions
Hunting Queries
ASimProcess
ASimRegistry
AWSCloudTrail
AWSS3
AuditLogs
AzureActivity
AzureDevOpsAuditing
AzureDiagnostics
AzureStorage
BehaviorAnalytics
CommonSecurityLog
DnsEvents
GitHub
LAQueryLogs
Microsoft 365 Defender
Campaigns
Collection
Command and Control
Credential Access
Defense evasion
Delivery
Device Inventory
Discovery
Email Queries

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

jonahbaron Update Email data exfiltration via PowerShell.yaml 67909f7 · 2 years ago History

Code Blame 14 lines (14 loc) · 500 Bytes · Raw

```yaml
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'
```

- Execution
- Exfiltration
- Exploits
- Fun
- General queries
- Impact