

Files

fa0411f

Go to file







- .azure-pipelines
- .github
- .script
- .vscode
- ASIM
- BYOML
- Dashboards
- DataConnectors
- Detections
 - ASimAuthentication
 - ASimDNS
 - imDNS_Miners.yaml
 - imDNS_TorProxies.yaml
 - imDns_DomainEntity_DnsEven...
 - imDns_ExcessiveNXDOMAIND...
 - imDns_HighNXDomainCount_...
 - imDns_IPEntity_DnsEvents.yaml
- ASimFileEvent
- ASimNetworkSession
- ASimProcess
- ASimWebSession
- AWSCloudTrail
- AWSGuardDuty
- AuditLogs
- AzureActivity
- AzureAppServices
- AzureDevOpsAuditing
- AzureDiagnostics
- AzureFirewall
- CiscoUmbrella
- CommonSecurityLog
- DeviceEvents
- DeviceFileEvents
- DeviceNetworkEvents
- DeviceProcessEvents
- DnsEvents

Azure-Sentinel / Detections / ASimDNS / imDNS_Miners.yaml

oshezaf remove-tabs-from-detections 8ad8ab9 · 2 years ago History

Code Blame 71 lines (70 loc) · 2.95 KB Raw Copy Download Compare

```
1 id: c094384d-7ea7-4091-83be-18706ecca981
2 name: DNS events related to mining pools (ASIM DNS Schema)
3 description: |
4   'Identifies IP addresses that may be performing DNS lookups associated with common cu
5   This analytic rule uses [ASIM](https://aka.ms/AboutASIM) and supports any built-in or
6 severity: Low
7 requiredDataConnectors:
8   - connectorId: WindowsForwardedEvents
9     dataTypes:
10       - WindowsEvent
11   - connectorId: DNS
12     dataTypes:
13       - DnsEvents
14   - connectorId: AzureFirewall
15     dataTypes:
16       - AzureDiagnostics
17   - connectorId: Zscaler
18     dataTypes:
19       - CommonSecurityLog
20   - connectorId: InfobloxNIOs
21     dataTypes:
22       - Syslog
23   - connectorId: GCPDNSDataConnector
24     dataTypes:
25       - GCP_DNS_CL
26   - connectorId: NXLogDnsLogs
27     dataTypes:
28       - NXLog_DNS_Server_CL
29   - connectorId: CiscoUmbrellaDataConnector
30     dataTypes:
31       - Cisco_Umbrella_dns_CL
32   - connectorId: Corelight
33     dataTypes:
34       - Corelight_CL
35
36 queryFrequency: 1d
37 queryPeriod: 1d
38 triggerOperator: gt
39 triggerThreshold: 0
40 tactics:
41   - Impact
42 relevantTechniques:
43   - T1496
44 tags:
45   - ParentAlert: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/DnsEven
46     version: 1.0.0
47   - Schema: ASIMDns
48     SchemaVersion: 0.1.1
49 query: |
50   let minersDomains=dynamic(["monerohash.com", "do-dear.com", "xmrminerpro.com", "secum
51   "xmrget.com", "mininglottery.eu", "minergate.com", "moriaxmr.com", "multipooler.com",
52   "supportxmr.com", "minexmr.com", "hashvault.pro", "xmrpool.net", "crypto-pool.fr", "x
53   "gntl.co.uk", "semipool.com", "coinfoundry.org", "cryptoknight.cc", "fairhash.org", "
54   "coinpoolit.webhop.me", "nanopool.org", "moneropool.com", "miner.center", "prohash.ne
55   "extrmepool.org", "webcoin.me", "kippo.eu", "hashinvest.ws", "monero.farm", "supportx
56   "dwarfpool.com", "hash-to-coins.com", "hashvault.pro", "pool-proxy.com", "hashfor.cas
57   "moneropool.eu", "cryptonotopool.org.uk", "extranepool.org", "extranepool.com", "hash
```

- >  Duo Security
- >  GitHub
- >  Heartbeat
- >  LAQueryLogs
- >  MultipleDataSources
- >  OfficeActivity

```
57         moneropool.ru , cryptonodepool.org.uk , extremepool.org , extremenash.com , nash
58         "backup-pool.com", "mooo.com", "freeyy.me", "cryptonight.net", "shscrypto.net"]]);
59     _Im_Dns(domain_has_any=minersDomains)
60     | extend timestamp = TimeGenerated, IPCustomEntity = SrcIpAddr, HostCustomEntity = Dv
61 entityMappings:
62   - entityType: Host
63     fieldMappings:
64       - identifier: FullName
65         columnName: HostCustomEntity
66   - entityType: IP
67     fieldMappings:
68       - identifier: Address
69         columnName: IPCustomEntity
70 version: 1.3.1
71 kind: Scheduled
```