



Azure / Azure-Sentinel Public

Notifications

Fork 3k

Star 4.6k

Code

Issues 26

Pull requests 82

Actions

Projects

Wiki

Security

Insights

Azure-Sentinel / Detections / ASimDNS / imDNS_TorProxies.yaml

oshezaf remove-tabs-from-detections

8ad8ab9 · 2 years ago

62 lines (62 loc) · 2.11 KB ·

Code

Blame

Raw

```
1 id: 3fe3c520-04f1-44b8-8398-782ed21435f8
2 name: DNS events related to Tor proxies (ASIM DNS Schema)
3 description: |
4     'Identifies IP addresses performing DNS lookups associated with common Tor proxies.
5     This analytic rule uses [ASIM](https://aka.ms/AboutASIM) and supports any built-in or custom sour
6 severity: Low
7 requiredDataConnectors:
8     - connectorId: DNS
9       dataTypes:
10         - DnsEvents
11     - connectorId: AzureFirewall
12       dataTypes:
13         - AzureDiagnostics
14     - connectorId: Zscaler
15       dataTypes:
16         - CommonSecurityLog
17     - connectorId: InfobloxNIOs
18       dataTypes:
19         - Syslog
20     - connectorId: GCPDNSDataConnector
21       dataTypes:
22         - GCP_DNS_CL
23     - connectorId: NXLogDnsLogs
24       dataTypes:
25         - NXLog_DNS_Server_CL
26     - connectorId: CiscoUmbrellaDataConnector
```

```
27     dataTypes:
28       - Cisco_Umbrella_dns_CL
29   - connectorId: Corelight
30     dataTypes:
31       - Corelight_CL
32   queryFrequency: 1d
33   queryPeriod: 1d
34   triggerOperator: gt
35   triggerThreshold: 0
36   tactics:
37     - Exfiltration
38   relevantTechniques:
39     - T1048
40   tags:
41     - ParentAlert: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/DnsEvents/DNS_TorProxies.yaml
42       version: 1.0.0
43     - Schema: ASIMDNS
44       SchemaVersion: 0.1.1
45   query: |
46     let torProxies=dynamic(["tor2web.org", "tor2web.com", "torlink.co", "onion.to", "onion.ink", "onion.city", "onion.it", "onion.direct", "onion.top", "onion.casa", "onion.plus", "onion.rip", "onion.sh", "onion.lu", "onion.pet", "t2w.pw", "tor2web.ae.org", "tor2web.blutmagie.de", "s1.tor-gateways.de", "s2.tor-gateways.de", "s3.tor-gateways.de", "s4.tor-gateways.de", "s5.tor-gateways.de"])
47     _Im_Dns(domain_has_any=torProxies)
48     | extend timestamp = TimeGenerated, IPCustomEntity = SrcIpAddr, HostCustomEntity = Dvc
49   entityMappings:
50     - entityType: Host
51       fieldMappings:
52         - identifier: FullName
53           columnName: HostCustomEntity
54     - entityType: IP
55       fieldMappings:
56         - identifier: Address
57           columnName: IPCustomEntity
58   version: 1.3.1
59   kind: Scheduled
```