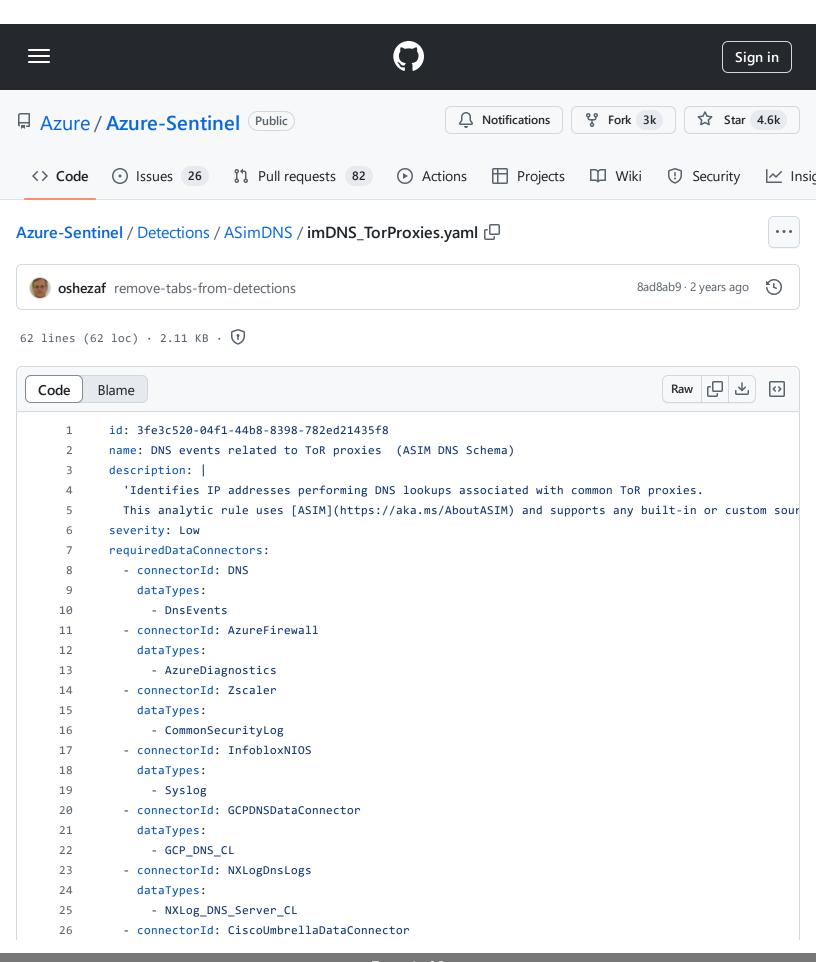
Azure-Sentinel/Detections/ASimDNS/imDNS_TorProxies.yaml at f99542b94afe0ad2f19a82cc08262e7ac8e1428e · Azure/Azure-Sentinel · GitHub - 31/10/2024 15:22 https://github.com/Azure/Azure-Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/ASimDNS/imDNS TorProxies.yaml



```
Sentinel/blob/f99542b94afe0ad2f19a82cc08262e7ac8e1428e/Detections/ASimDNS/imDNS_TorProxies.yamI
```

```
27
           dataTypes:
28
             - Cisco_Umbrella_dns_CL
29
         - connectorId: Corelight
           dataTypes:
30
             - Corelight_CL
31
32
       queryFrequency: 1d
       queryPeriod: 1d
33
34
       triggerOperator: gt
       triggerThreshold: 0
35
36
       tactics:
         - Exfiltration
37
38
       relevantTechniques:
39
         - T1048
40
       tags:
         - ParentAlert: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/DnsEvents/DNS_TorPr
41
           version: 1.0.0
42
         - Schema: ASIMDns
43
           SchemaVersion: 0.1.1
44
       query: |
45
         let torProxies=dynamic(["tor2web.org", "tor2web.com", "torlink.co", "onion.to", "onion.ink", "oni
46
         "onion.it", "onion.city", "onion.direct", "onion.top", "onion.casa", "onion.plus", "onion.rip", '
47
         "tor2web.blutmagie.de", "onion.sh", "onion.lu", "onion.pet", "t2w.pw", "tor2web.ae.org", "tor2web
48
         "s1.tor-gateways.de", "s2.tor-gateways.de", "s3.tor-gateways.de", "s4.tor-gateways.de", "s5.tor-gateways.de",
49
50
         _Im_Dns(domain_has_any=torProxies)
51
         | extend timestamp = TimeGenerated, IPCustomEntity = SrcIpAddr, HostCustomEntity = Dvc
       entityMappings:
52
         - entityType: Host
53
54
           fieldMappings:
             - identifier: FullName
55
                columnName: HostCustomEntity
56
         - entityType: IP
57
           fieldMappings:
58
             - identifier: Address
59
               columnName: IPCustomEntity
60
       version: 1.3.1
61
       kind: Scheduled
62
```