



Azure / Azure-Sentinel Public

Notifications

Fork 3k

Star 4.6k

<> Code

Issues 27

Pull requests 84

Actions

Projects

Wiki

Security

Insights

Azure-Sentinel / Solutions / Legacy IOC based Threat Protection / Analytic Rules / GalliumIOCs.yaml

...

145 lines (144 loc) · 7.02 KB

CodeBlame

Raw

```
1 id: 26a3b261-b997-4374-94ea-6c37f67f4f39
2 name: Known GALLIUM domains and hashes
3 description: |
4     'GALLIUM command and control domains and hash values for tools and malware used by GALLIUM.
5     Matches domain name IOCs related to the GALLIUM activity group with CommonSecurityLog, DnsEvents
6     References: https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/
7 severity: High
8 status: Available
9 tags:
10     - Schema: ASIMDns
11       SchemaVersion: 0.1.1
12 requiredDataConnectors:
13     - connectorId: DNS
14       dataTypes:
15         - DnsEvents
16     - connectorId: AzureMonitor(VMInsights)
17       dataTypes:
18         - VMConnection
19     - connectorId: CiscoASA
20       dataTypes:
21         - CommonSecurityLog
22     - connectorId: PaloAltoNetworks
23       dataTypes:
24         - CommonSecurityLog
25     - connectorId: SecurityEvents
26       dataTypes:
```

```
27         - SecurityEvent
28     - connectorId: AzureFirewall
29       dataTypes:
30         - AzureDiagnostics
31         - AZFWApplicationRule
32         - AZFWDnsQuery
33     - connectorId: Zscaler
34       dataTypes:
35         - CommonSecurityLog
36     - connectorId: InfobloxNIOs
37       dataTypes:
38         - Syslog
39     - connectorId: GCPDNSDataConnector
40       dataTypes:
41         - GCP_DNS_CL
42     - connectorId: NXLogDnsLogs
43       dataTypes:
44         - NXLog_DNS_Server_CL
45     - connectorId: CiscoUmbrellaDataConnector
46       dataTypes:
47         - Cisco_Umbrella_dns_CL
48     - connectorId: Corelight
49       dataTypes:
50         - Corelight_CL
51
52   queryFrequency: 1d
53   queryPeriod: 1d
54   triggerOperator: gt
55   triggerThreshold: 0
56   tactics:
57     - CommandAndControl
58     - CredentialAccess
59   query: |
60     let DomainNames = dynamic(["asyspy256.ddns.net","hotkillmail9sddcc.ddns.net","rosaf112.ddns.net",
61     let SHA1Hash = dynamic (["53a44c2396d15c3a03723fa5e5db54cafd527635", "9c5e496921e3bc882dc40694f1c
62     let SHA256Hash = dynamic (["9ae7c4a4e1cfe9b505c3a47e66551eb1357affee65bfefb0109d02f4e97c06dd", "7
63     let SigNames = dynamic(["TrojanDropper:Win32/BlackMould.A!dha", "Trojan:Win32/BlackMould.B!dha",
64     (union isfuzzy=true
65     (CommonSecurityLog
66     | parse Message with * '(' DNSName ')' *
67     | where isnotempty(FileHash)
68     | where FileHash in (SHA256Hash) or DNSName in~ (DomainNames)
69     | extend Account = SourceUserID, Computer = DeviceName, IPAddress = SourceIP
70     ),
71     ( _Im_Dns(domain_has_any=DomainNames)
72     | extend DNSName = DnsQuery
```

```
73 | extend IPAddress = SrcIpAddr
74 ),
75 (VMConnection
76 | parse RemoteDnsCanonicalNames with * '[' DNSName ']' *
77 | where isnotempty(DNSName)
78 | where DNSName in~ (DomainNames)
79 | extend IPAddress = RemoteIp
80 ),
81 (Event
82 //This query uses sysmon data depending on table name used this may need updating
83 | where Source == "Microsoft-Windows-Sysmon"
84 | extend EvData = parse_xml(EventData)
85 | extend EventDetail = EvData.DataItem.EventData.Data
86 | extend Hashes = EventDetail.[16].["#text"]
87 | parse Hashes with * 'SHA1=' SHA1 ',' *
88 | where isnotempty(Hashes)
89 | where Hashes in (SHA1Hash)
90 | extend Account = UserName
91 ),
92 (SecurityAlert
93 | where ProductName == "Microsoft Defender Advanced Threat Protection"
94 | extend ThreatName = tostring(parse_json(ExtendedProperties).ThreatName)
95 | where isnotempty(ThreatName)
96 | where ThreatName has_any (SigNames)
97 | extend Computer = tostring(parse_json(Entities)[0].HostName)
98 ),
99 (AzureDiagnostics
100 | where ResourceType == "AZUREFIREWALLS"
101 | where Category == "AzureFirewallApplicationRule"
102 | parse msg_s with Protocol 'request from ' SourceHost ':' SourcePort 'to ' DestinationHost ':' D
103 | where isnotempty(DestinationHost)
104 | where DestinationHost has_any (DomainNames)
105 | extend DNSName = DestinationHost
106 | extend IPAddress = SourceHost
107 ),
108 (AzureDiagnostics
109 | where ResourceType == "AZUREFIREWALLS"
110 | where Category == "AzureFirewallDnsProxy"
111 | project TimeGenerated,Resource, msg_s, Type
112 | parse msg_s with "DNS Request: " ClientIP ":" ClientPort " - " QueryID " " Request_Type " " Rec
113 | where Request_Name has_any (DomainNames)
114 | extend DNSName = Request_Name
115 | extend IPAddress = ClientIP
116 ),
117 (AZFWApplicationRule
118 | where isnotempty(Fadn)
```

```
118     | where isnotempty(QueryName)
119     | where Fqdn has_any (DomainNames)
120     | extend DNSName = Fqdn
121     | extend IPAddress = SourceIp
122     ),
123     (AZFWDnsQuery
124     | where isnotempty(QueryName)
125     | where QueryName has_any (DomainNames)
126     | extend DNSName = QueryName
127     | extend IPAddress = SourceIp
128     )
129     )
130     | extend timestamp = TimeGenerated, AccountCustomEntity = Account, HostCustomEntity = Computer, IPCustomEntity = IPAddress
131 entityMappings:
132   - entityType: Account
133     fieldMappings:
134       - identifier: FullName
135         columnName: AccountCustomEntity
136   - entityType: Host
137     fieldMappings:
138       - identifier: FullName
139         columnName: HostCustomEntity
140   - entityType: IP
141     fieldMappings:
142       - identifier: Address
143         columnName: IPCustomEntity
144 version: 1.6.1
145 kind: Scheduled
```