



Azure / Azure-Sentinel Public

Notifications

Fork 3k

Star 4.6k

Code

Issues 27

Pull requests 84

Actions

Projects

Wiki

Security

Insights

Azure-Sentinel / Detections / MultipleDataSources / SOURGUM\_IOC.yaml

189 lines (189 loc) · 12 KB

CodeBlame

RawCopyDownloadCode

```
1 id: 94749332-1ad9-49dd-a5ab-5ff2170788fc
2 name: SOURGUM Actor IOC - July 2021
3 description: |
4     'Identifies a match across IOC's related to an actor tracked by Microsoft as SOURGUM'
5 severity: High
6 requiredDataConnectors:
7     - connectorId: DNS
8       dataTypes:
9         - DnsEvents
10    - connectorId: AzureMonitor(VMInsights)
11      dataTypes:
12        - VMConnection
13    - connectorId: F5
14      dataTypes:
15        - CommonSecurityLog
16    - connectorId: CiscoASA
17      dataTypes:
18        - CommonSecurityLog
19    - connectorId: PaloAltoNetworks
20      dataTypes:
21        - CommonSecurityLog
22    - connectorId: Fortinet
23      dataTypes:
24        - CommonSecurityLog
25    - connectorId: CheckPoint
26      dataTypes:
```

```
27         - CommonSecurityLog
28     - connectorId: CEF
29       dataTypes:
30         - CommonSecurityLog
31     - connectorId: MicrosoftThreatProtection
32       dataTypes:
33         - DeviceNetworkEvents
34         - DeviceRegistryEvents
35         - DeviceFileEvents
36         - DeviceEvents
37         - DeviceProcessEvents
38     - connectorId: SecurityEvents
39       dataTypes:
40         - SecurityEvent
41     - connectorId: Office365
42       dataTypes:
43         - OfficeActivity
44     - connectorId: AzureFirewall
45       dataTypes:
46         - AzureDiagnostics
47     - connectorId: WindowsFirewall
48       dataTypes:
49         - WindowsFirewall
50     - connectorId: WindowsSecurityEvents
51       dataTypes:
52         - SecurityEvents
53     - connectorId: WindowsForwardedEvents
54       dataTypes:
55         - WindowsEvent
56   queryFrequency: 6h
57   queryPeriod: 6h
58   triggerOperator: gt
59   triggerThreshold: 0
60   tactics:
61     - Persistence
62   relevantTechniques:
63     - T1546
64   tags:
65     - SOURGUM
66   query: |
67     let iocs = externaldata(DateAdded:string,IoC:string,Type:string,TLP:string) [@"https://raw.githubusercontent.com/Azure/Azure-Sentinel/blob/master/Sentinel/Detections/MultipleDataSources/SOURGUM_IOC.yaml"]
68     let domains = (iocs | where Type =~ "domainname" | project IoC);
69     let sha256Hashes = (iocs | where Type =~ "sha256" | project IoC);
70     let file_path1 = (iocs | where Type =~ "filepath1" | project IoC);
71     let file_path2 = (iocs | where Type =~ "filepath2" | project IoC);
72     let file_path3 = (iocs | where Type =~ "filepath3" | project IoC);
```

```
73     let reg_key = (iocs | where Type =~ "regkey" | project IoC);
74     (union isfuzzy=true
75     (CommonSecurityLog
76     | where DestinationHostName has_any (domains) or RequestURL has_any (domains) or Message has_any
77     | parse Message with * '(' DNSName ')' *
78     | project TimeGenerated, Message, SourceUserID, RequestURL, DestinationHostName, Type, SourceIP,
79     | extend Alert = 'SOURGUM IOC detected'
80     | extend timestamp = TimeGenerated, AccountCustomEntity = SourceUserID, UrlCustomEntity = Request
81     ),
82     (DnsEvents
83     | where Name in~ (domains)
84     | project TimeGenerated, Computer, IPAddresses, Name, ClientIP, Type
85     | extend DNSName = Name, Host = Computer , Alert = 'SOURGUM IOC detected'
86     | extend timestamp = TimeGenerated, HostCustomEntity = Host, DNSCustomEntity = DNSName, IPCustomE
87     ),
88     (VMConnection
89     | where RemoteDnsCanonicalNames has_any (domains)
90     | parse RemoteDnsCanonicalNames with * '[' DNSName '"' *
91     | project TimeGenerated, Computer, Direction, RemoteDnsCanonicalNames, ProcessName, SourceIp, Des
92     | extend timestamp = TimeGenerated, IPCustomEntity = DestinationIp, HostCustomEntity = Computer,
93     ),
94     (Event
95     | where Source == "Microsoft-Windows-Sysmon"
96     | where EventID == 3
97     | extend EvData = parse_xml(EventData)
98     | extend EventDetail = EvData.DataItem.EventData.Data
99     | extend SourceIP = tostring(EventDetail.[9].["#text"]), DestinationIP = tostring(EventDetail.[14
100    | where Image has_any (file_path1) or Image has_any (file_path3)
101    | project TimeGenerated, SourceIP, DestinationIP, Image, Username, Computer, EventDetail, Type
102    | extend timestamp = TimeGenerated, AccountCustomEntity = Username, ProcessCustomEntity = tostrin
103    ),
104    (DeviceNetworkEvents
105    | where (RemoteUrl has_any (domains)) or (InitiatingProcessSHA256 in (sha256Hashes) and Initiati
106    | project TimeGenerated, ActionType, DeviceId, DeviceName, InitiatingProcessAccountDomain, Initia
107    | extend timestamp = TimeGenerated, IPCustomEntity = RemoteIP, HostCustomEntity = DeviceName, AI
108    ),
109    (AzureDiagnostics
110    | where ResourceType == "AZUREFIREWALLS"
111    | where Category == "AzureFirewallDnsProxy"
112    | project TimeGenerated,Resource, msg_s, Type
113    | parse msg_s with "DNS Request: " ClientIP ":" ClientPort " - " QueryID " " Request_Type " " Rec
114    | where Request_Name has_any (domains)
115    | extend timestamp = TimeGenerated, DNSName = Request_Name, IPCustomEntity = ClientIP, Alert = 'S
116    ),
117    (AzureDiagnostics
118    | where ResourceType == "AZUREFIREWALLS"
```

```
118 | where ResourceType == "AZURE_FIREWALLS"
119 | where Category == "AzureFirewallApplicationRule"
120 | project TimeGenerated, Resource, msg_s
121 | parse msg_s with Protocol 'request from ' SourceHost ':' SourcePort 'to ' DestinationHost ':'
122 | where DestinationHost has_any (domains)
123 | extend timestamp = TimeGenerated, DNSName = DestinationHost, IPCustomEntity = SourceHost, Alert
124 ),
125 (Event
126 | where Source == "Microsoft-Windows-Sysmon"
127 | where EventID == 1
128 | extend EvData = parse_xml(EventData)
129 | extend EventDetail = EvData.DataItem.EventData.Data
130 | parse EventDetail with * 'SHA256=' SHA256 '",' *
131 | extend Image = EventDetail.[4].["#text"], CommandLine = EventDetail.[10].["#text"]
132 | where (SHA256 has_any (sha256Hashes) and Image has_any (file_path1)) or (Image has_any (file_pa
133 | project TimeGenerated, EventDetail, UserName, Computer, Type, Source, SHA256, CommandLine, Image
134 | extend Type = strcat(Type, ": ", Source), Alert = 'SOURGUM IOC detected'
135 | extend timestamp = TimeGenerated, HostCustomEntity = Computer , AccountCustomEntity = UserName,
136 ),
137 (DeviceRegistryEvents
138 | where RegistryKey has_any (reg_key) and RegistryValueData has_any (file_path2)
139 | project TimeGenerated, ActionType, DeviceId, DeviceName, InitiatingProcessAccountDomain, Initia
140 | extend timestamp = TimeGenerated, HostCustomEntity = DeviceName , AccountCustomEntity = Initia
141 ),
142 (DeviceProcessEvents
143 | where ( InitiatingProcessCommandLine has_any (file_path1)) or ( InitiatingProcessCommandLine h
144 | project TimeGenerated, ActionType, DeviceId, DeviceName, InitiatingProcessAccountDomain, Initia
145 | extend timestamp = TimeGenerated, HostCustomEntity = DeviceName , AccountCustomEntity = Initia
146 ),
147 (DeviceFileEvents
148 | where (InitiatingProcessSHA256 has_any (sha256Hashes) and InitiatingProcessFolderPath has_any
149 | project TimeGenerated, ActionType, DeviceId, DeviceName, InitiatingProcessAccountDomain, Initia
150 | extend timestamp = TimeGenerated, HostCustomEntity = DeviceName , AccountCustomEntity = Request
151 ),
152 (DeviceEvents
153 | where ( InitiatingProcessCommandLine has_any (file_path1)) or ( InitiatingProcessCommandLine h
154 | project TimeGenerated, ActionType, DeviceId, DeviceName, InitiatingProcessAccountDomain, Initia
155 | extend CommandLine = InitiatingProcessCommandLine, Alert = 'SOURGUM IOC detected'
156 | extend timestamp = TimeGenerated, HostCustomEntity = DeviceName , AccountCustomEntity = Initia
157 ),
158 ( SecurityEvent
159 | where EventID == 4688
160 | where ( CommandLine has_any (file_path1)) or ( CommandLine has_any (file_path3)) or ( CommandLi
161 | project TimeGenerated, Computer, NewProcessName, ParentProcessName, Account, NewProcessId, Type
162 | extend timestamp = TimeGenerated, HostCustomEntity = Computer , AccountCustomEntity = Account,
163 )
164 ,
```

```
164     )
165     entityMappings:
166     - entityType: Account
167       fieldMappings:
168       - identifier: FullName
169         columnName: AccountCustomEntity
170     - entityType: Host
171       fieldMappings:
172       - identifier: FullName
173         columnName: HostCustomEntity
174     - entityType: IP
175       fieldMappings:
176       - identifier: Address
177         columnName: IPCustomEntity
178     - entityType: Process
179       fieldMappings:
180       - identifier: ProcessId
181         columnName: ProcessCustomEntity
182     - entityType: FileHash
183       fieldMappings:
184       - identifier: Algorithm
185         columnName: AlgorithmCustomEntity
186       - identifier: Value
187         columnName: FileHashCustomEntity
188     version: 1.1.1
189     kind: Scheduled
```