v-atulyadav Update version f926e11 · last year History

Code Blame 145 lines (144 loc) · 7.02 KB · Raw

```yaml
id: 26a3b261-b997-4374-94ea-6c37f67f4f39
name: Known GALLIUM domains and hashes
description: |
  'GALLIUM command and control domains and hash values for tools and malware used by GA
   Matches domain name IOCs related to the GALLIUM activity group with CommonSecurityLo
   References: https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-glo
severity: High
status: Available
tags:
  - Schema: ASIMDns
    SchemaVersion: 0.1.1
requiredDataConnectors:
  - connectorId: DNS
    dataTypes:
      - DnsEvents
  - connectorId: AzureMonitor(VMInsights)
    dataTypes:
      - VMConnection
  - connectorId: CiscoASA
    dataTypes:
      - CommonSecurityLog
  - connectorId: PaloAltoNetworks
    dataTypes:
      - CommonSecurityLog
  - connectorId: SecurityEvents
    dataTypes:
      - SecurityEvent
  - connectorId: AzureFirewall
    dataTypes:
      - AzureDiagnostics
      - AZFWApplicationRule
      - AZFWDnsQuery
  - connectorId: Zscaler
    dataTypes:
      - CommonSecurityLog
  - connectorId: InfobloxNIOS
    dataTypes:
      - Syslog
  - connectorId: GCPDNSDataConnector
    dataTypes:
      - GCP_DNS_CL
  - connectorId: NXLogDnsLogs
    dataTypes:
      - NXLog_DNS_Server_CL
  - connectorId: CiscoUmbrellaDataConnector
    dataTypes:
      - Cisco_Umbrella_dns_CL
  - connectorId: Corelight
    dataTypes:
      - Corelight_CL

queryFrequency: 1d
queryPeriod: 1d
triggerOperator: gt
triggerThreshold: 0
tactics:
```

ApacheHTTPServer
AristaAwakeSecurity
Armis
Armorblox
Aruba ClearPass
AtlassianConfluenceAudit

```
    tactics:
      - CommandAndControl
      - CredentialAccess
    query: |
      let DomainNames = dynamic(["asyspy256.ddns.net","hotkillmail9sddcc.ddns.net","rosaf11
      let SHA1Hash = dynamic (["53a44c2396d15c3a03723fa5e5db54cafd527635", "9c5e496921e3bc8
      let SHA256Hash = dynamic (["9ae7c4a4e1cfe9b505c3a47e66551eb1357affee65bfefb0109d02f4e
      let SigNames = dynamic(["TrojanDropper:Win32/BlackMould.A!dha", "Trojan:Win32/BlackMo
      (union isfuzzy=true
      (CommonSecurityLog
      | parse Message with * '(' DNSName ')' *
      | where isnotempty(FileHash)
      | where FileHash in (SHA256Hash) or DNSName in~ (DomainNames)
      | extend Account = SourceUserID, Computer = DeviceName, IPAddress = SourceIP
      ),
      ( _Im_Dns(domain_has_any=DomainNames)
      | extend DNSName = DnsQuery
      | extend IPAddress = SrcIpAddr
      ),
      (VMConnection
      | parse RemoteDnsCanonicalNames with * '["' DNSName '"]' *
      | where isnotempty(DNSName)
      | where DNSName  in~ (DomainNames)
      | extend IPAddress = RemoteIp
      ),
      (Event
      //This query uses sysmon data depending on table name used this may need updataing
      | where Source == "Microsoft-Windows-Sysmon"
      | extend EvData = parse_xml(EventData)
      | extend EventDetail = EvData.DataItem.EventData.Data
      | extend Hashes = EventDetail.[16].["#text"]
      | parse Hashes with * 'SHA1=' SHA1 ',' *
      | where isnotempty(Hashes)
      | where Hashes in (SHA1Hash)
      | extend Account = UserName
      ),
      (SecurityAlert
      | where ProductName == "Microsoft Defender Advanced Threat Protection"
      | extend ThreatName = tostring(parse_json(ExtendedProperties).ThreatName)
      | where isnotempty(ThreatName)
      | where ThreatName has_any (SigNames)
      | extend Computer = tostring(parse_json(Entities)[0].HostName)
      ),
      (AzureDiagnostics
      | where ResourceType == "AZUREFIREWALLS"
      | where Category == "AzureFirewallApplicationRule"
      | parse msg_s with Protocol 'request from ' SourceHost ':' SourcePort 'to ' Destinati
      | where isnotempty(DestinationHost)
      | where DestinationHost has_any (DomainNames)
      | extend DNSName = DestinationHost
      | extend IPAddress = SourceHost
      ),
      (AzureDiagnostics
      | where ResourceType == "AZUREFIREWALLS"
      | where Category == "AzureFirewallDnsProxy"
      | project TimeGenerated,Resource, msg_s, Type
      | parse msg_s with "DNS Request: " ClientIP ":" ClientPort " - " QueryID " " Request_
      | where  Request_Name  has_any (DomainNames)
      | extend DNSName = Request_Name
      | extend IPAddress = ClientIP
      ),
      (AZFWApplicationRule
      | where isnotempty(Fqdn)
      | where Fqdn has_any (DomainNames)
      | extend DNSName = Fqdn
      | extend IPAddress = SourceIp
      ),
      (AZFWDnsQuery
      | where isnotempty(QueryName)
      | where QueryName has_any (DomainNames)
      | extend DNSName = QueryName
      | extend IPAddress = SourceIp
      )
      )
      | extend timestamp = TimeGenerated, AccountCustomEntity = Account, HostCustomEntity =
```

```
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
```