Template - Digital currency mining activity

Link to alert

**Description**

Analysis of DNS transactions detected digital currency mining activity. Such activity, while possibly legitimate user behavior, is frequently performed by attackers following compromise of resources. Typical related attacker activity is likely to include the download and execution of common mining tools.

**Classification**: Incident

**How to investigate**

<https://docs.microsoft.com/en-us/azure/security-center/alerts-reference>

**Alert details**

Analytic Description:

Date:

Severity: Medium

Compromised Host:

* Server:
* Public IP:

Compromised Entity:

* IP Address:

Suspicious random domain:

* Server:
* IP Address(es):
* Blacklisted IP address(es):

**Remediation**

Check the below on the source computer.

* Find the tool that performed the supposed attack and remove it.
* Look for users who were logged on around the same time as the activity occurred, as these users may also be compromised.

Update antimalware Security intelligence (Microsoft Defender Antivirus)

If after your investigation, the registered query domain remains not trusted, we recommend blocking the destination domain to avoid all future communication.

If possible, trace the source IP address and block it to prevent future communication.

***NB: PROVIDE A SCREESNHOT OF THE WORK DONE***