Template - Attempted communication with suspicious sinkholed domain

Link to alert

**Description**

Analysis of DNS transactions detected request for sinkholed domain. Such activity, while possibly legitimate user behaviour, is frequently an indication of the download or execution of malicious software. Typical related attacker activity is likely to include the download and execution of further malicious software or remote administration 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:

Compromised Entity:

* IP Address:

Suspicious random domain:

* Server:
* 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.

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

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