Template - Network-mapping reconnaissance (DNS)

Link to alert

**Description**

The DNS protocol in most organizations is typically not monitored and rarely blocked for malicious activity. Enabling an attacker on a compromised machine, to abuse the DNS protocol. Malicious communication over DNS can be used for data exfiltration, command, and control, and/or evading corporate network restrictions.

**Classification**: Incident

**How to investigate**

[Microsoft Defender for Identity reconnaissance phase security alerts | Microsoft Docs](https://docs.microsoft.com/en-us/defender-for-identity/reconnaissance-alerts#network-mapping-reconnaissance-dns-external-id-2007)

**Alert details**

Run command:

Date:

Severity:

Compromised Host:

* Server:
* IP address

Compromised Entity:

* Server:
* 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.

Identify and block the source of the DNS communication but ensure that it does not affect the operations.

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