System information gathering using the Dxdiag application

You might need to identify system information gathering conducted with the Dxdiag application when doing the following:

- Detecting indicators of Remcos RAT malware

Prerequisites

In order to execute this procedure in your environment, the following data, services, or apps are required:

- People: Security analyst or Threat hunter
- Technologies: Splunk Enterprise or Splunk Cloud Platform
- Data: Endpoint data

Example

This search detects a suspicious dxdiag.exe process command-line execution. Dxdiag is used to collect the system information of the target host. This technique has been seen used by Remcos RATS, various actors, and other malware to collect information as part of the recon or collection phase of an attack.

- To optimize the search shown below, you should specify an index and a time range.
- Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). This search requires the Endpoint data model. For information on installing and using the CIM, see the Common Information Model documentation.

Run the following search:

```
| rename "Processes.**" AS *** |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) |
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

Search explanation

The table provides an explanation of what each part of this search achieves. You can adjust this query based on the...
specifics of your environment.

**Splunk Search**


| rename "Processes.*" AS "*"

| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime) | convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)

**Explanation**

Query the Endpoint.Processes data model object to search for dxdiag.exe process command-line executions. Sort first by destination, then by the rest of the fields shown.

Rename data model fields for better readability.

Convert these times into readable strings.

**Result**

This behavior should be rarely seen in a corporate network, but this command line could be used by a network administrator to audit host machine specifications. Because of this, this search may contain false positives in its results. To triage further, analyze what commands were passed after it pipes out the result to a file for further processing.

During triage, isolate the endpoint and review for source of exploitation.

If your results indicate an attack has occurred, the host or computer where the vulnerability is detected needs to be further investigated and remediated according to your response plan. This involves a final step of re-imaging the system with a known good system build after investigation.