Detecting Netsh attacks

Applicability

- Product: Splunk Cloud Platform or Splunk Enterprise
- Function: Search
- Data: Microsoft: Windows process launch
- Data: Sysmon

To run these searches, you'll need to populate the Endpoint data model. Content developed by the Splunk Security Research team requires the use of consistent, normalized data provided by the Common Information Model (CIM). For information on installing and using the CIM, see the Common Information Model documentation.

Scenario

You are an analyst responsible for your organization's overall security posture. You need to be able to detect activities and various techniques associated with the abuse of Netsh, through which netsh.exe can disable local firewall settings or set up a remote connection to a host from an infected system.

It is a common practice for attackers of all types to leverage native Windows tools and functionality to execute commands for malicious reasons, and Netsh.exe is one of these tools with abuse potential. It can be used locally or remotely as a command-line scripting utility to display or modify the network configuration of a computer that is currently running.

Detection search

Processes created by netsh.exe

To run this search, you need to ingest data that records process activity from your hosts.

This search looks for processes launching netsh.exe. Netsh is a command-line scripting utility that allows you to, either locally or remotely, display or modify the network configuration of a computer that is currently running. Netsh can be used as a persistence proxy technique to execute a helper DLL when netsh.exe is executed.

In this search, you are looking for processes spawned by netsh.exe and executing commands via the command line.

False positives from this search may occur since some VPN applications are known to launch netsh.exe. Outside of these instances, it is unusual for an executable to launch netsh.exe and run commands.
Investigative searches

Parent processes running on a host

To run this search, you'll need to populate the Endpoint data model.

This search queries the Endpoint data model to give you details about the parent process of a process running on a host which is under investigation. Enter the values of the process name in question and the destination IP address.

```
| tstats summariesonly=true allow_old_summaries=true count, values("Processes.process") AS process, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes BY "Processes.user", "Processes.parent_process_name", "Processes.process_name", "Processes.dest"
| rename "Processes.**" AS ***
| search (dest=<field on the host where the process is running> parent_process_name=<parent_process_name>)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

For more help with this search, see this article.

Processes running on a host

To run this search, you'll need to populate the Endpoint data model.

This search queries the Endpoint data model to give you details about the process running on a host which is under investigation. To gather the process information, enter the values for the process name in question and the destination IP address.

```
| tstats summariesonly=true allow_old_summaries=true count, values("Processes.process") AS process, min(_time) AS firstTime, max(_time) AS lastTime FROM datamodel=Endpoint.Processes BY "Processes.user", "Processes.parent_process_name", "Processes.process_name", "Processes.dest"
| rename "Processes.**" AS ***
| search (dest=<field on the host where the process is running> process_name=<process_name>)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(firstTime)
| convert timeformat="%Y-%m-%dT%H:%M:%S" ctime(lastTime)
```

For more help with this search, see this article.
Additional resources

This use case is included within Splunk Enterprise Security, a Splunk app that provides prebuilt content and searches to help answer root-cause questions in real-time about malicious and anomalous events in your IT infrastructure. In addition, Splunk Enterprise Security provides a number of other searches to help you detect abuse attempts within your environment, including:

- Detecting host redirection attacks
- Detecting web fraud
- Detecting SNICat SNI data exfiltration