Detecting Lateral Movement Using Sysmon and Splunk

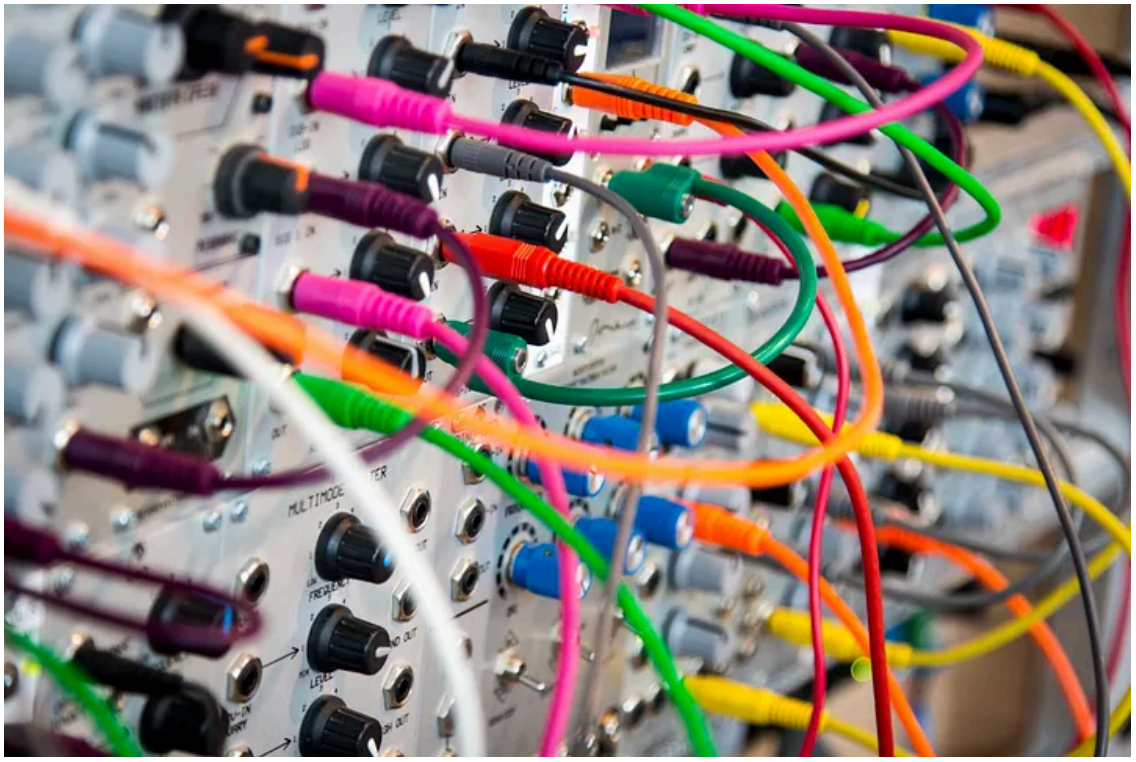
By David French

Published: 2020-09-28 · Archived: 2026-04-06 01:57:34 UTC

4 min read

Sep 30, 2018

Press enter or click to view image in full size



Detecting an attacker moving laterally in your environment can be a challenge. It can be difficult to obtain the logs required to identify this activity and differentiate between what is normal versus what is malicious.

This post highlights a few things that you can look for to detect an attacker moving between hosts. With Sysmon installed on Windows hosts and the events being sent to SIEM, you can detect attempts to move laterally and questions during incident response can be answered in minutes versus hours.

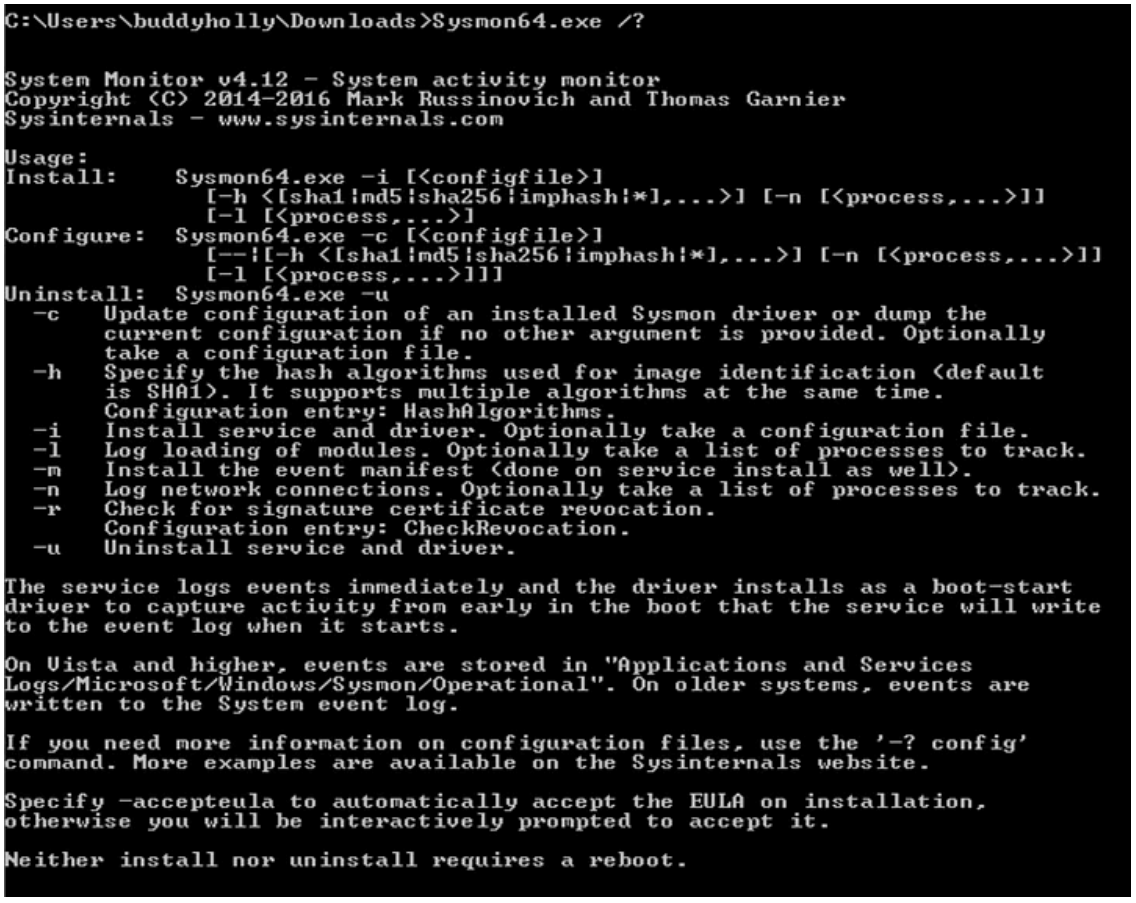
Note, if you decide to implement any of the monitoring and detection detailed in this post in a production environment, it’s likely that some tuning will be required to filter benign or expected behavior.

Install and Configure Sysmon on a Windows Host

Download Sysmon and install it on the Windows host as follows.

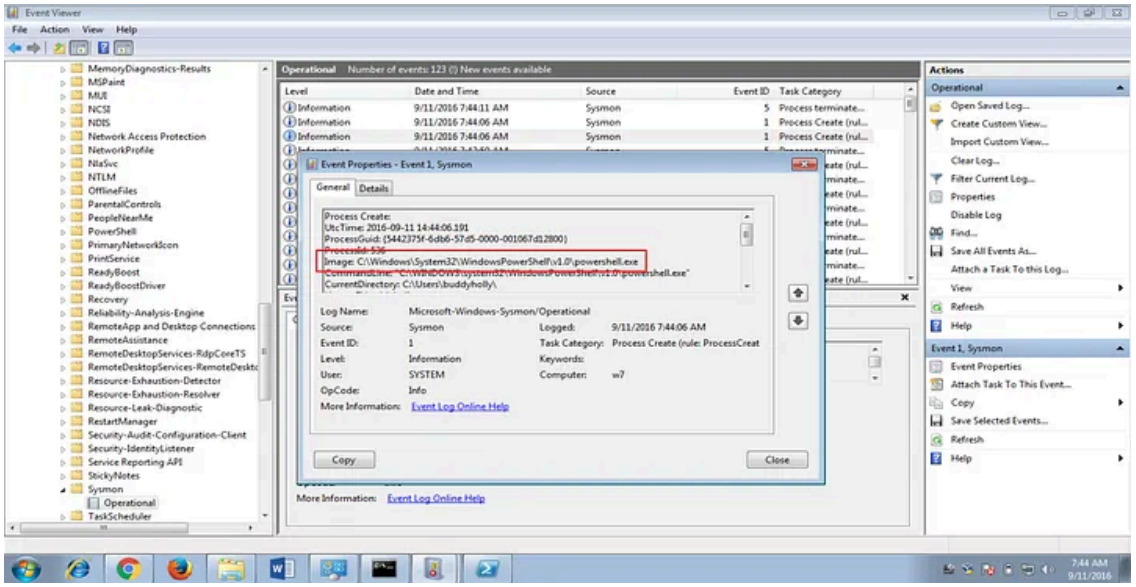
```
sysmon -i -n
```

Press enter or click to view image in full size



You can view Sysmon events locally by opening Event Viewer and navigating to Microsoft — Windows — Sysmon — Operational. You can see that Sysmon logged the creation of a new process, `powershell.exe`, in the image below.

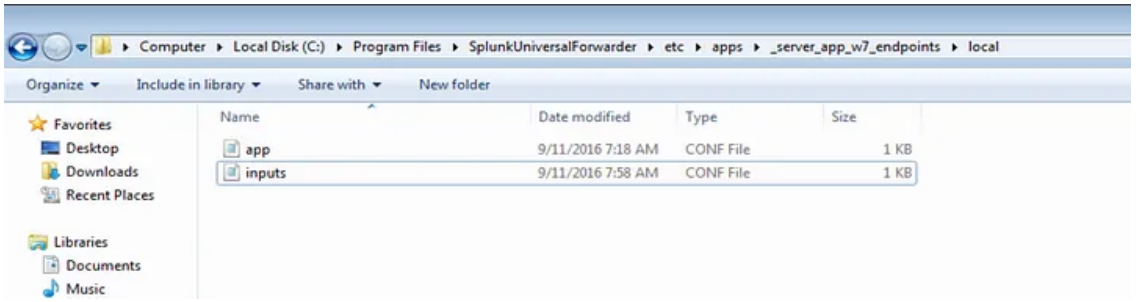
Press enter or click to view image in full size



Add the following text to the inputs.conf file.

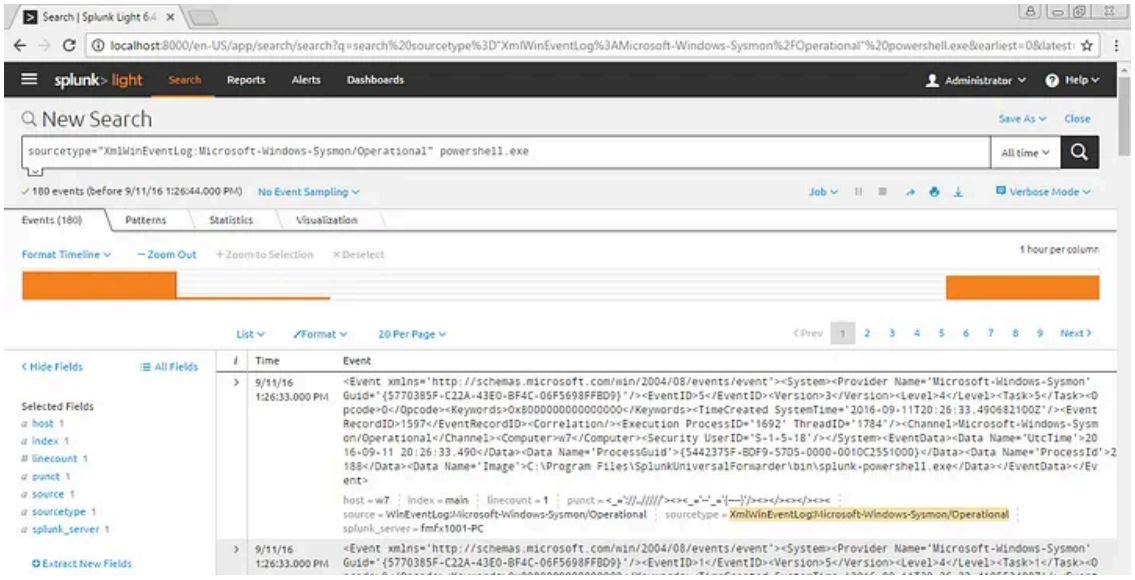
```
[WinEventLog://Microsoft-Windows-Sysmon/Operational]
disabled = false
renderXml = true
```

Press enter or click to view image in full size



Sysmon events from the host can be found in Splunk under `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"`

Press enter or click to view image in full size

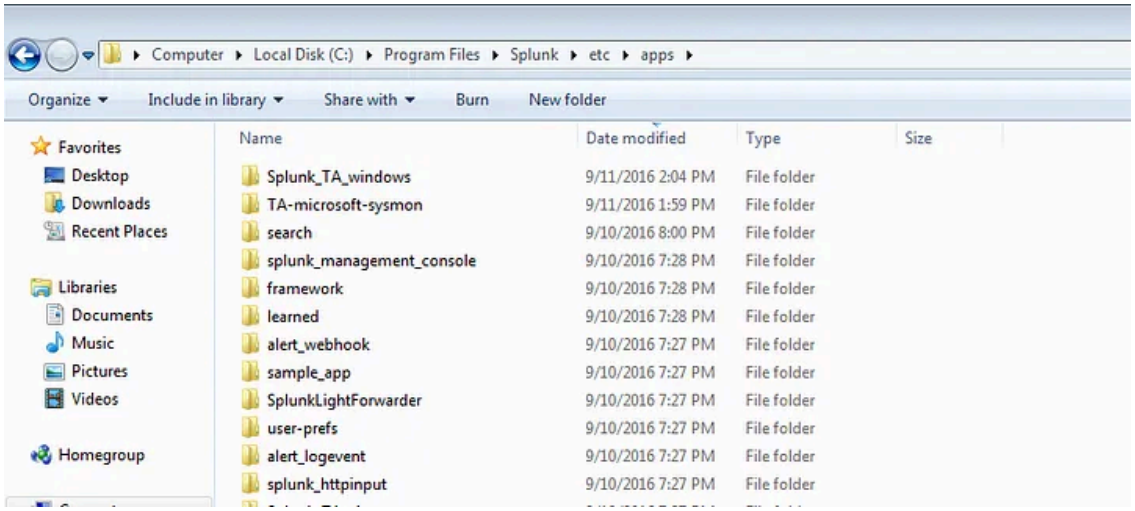


Install the Splunk “Add-on for Microsoft Sysmon”

Download the add-on from https://splunkbase.splunk.com/app/1914/#/overview

Unzip the contents of the compressed file to `C:\Program Files\Splunk\etc\apps` on the Splunk server.

Press enter or click to view image in full size



Restart Splunk Light.

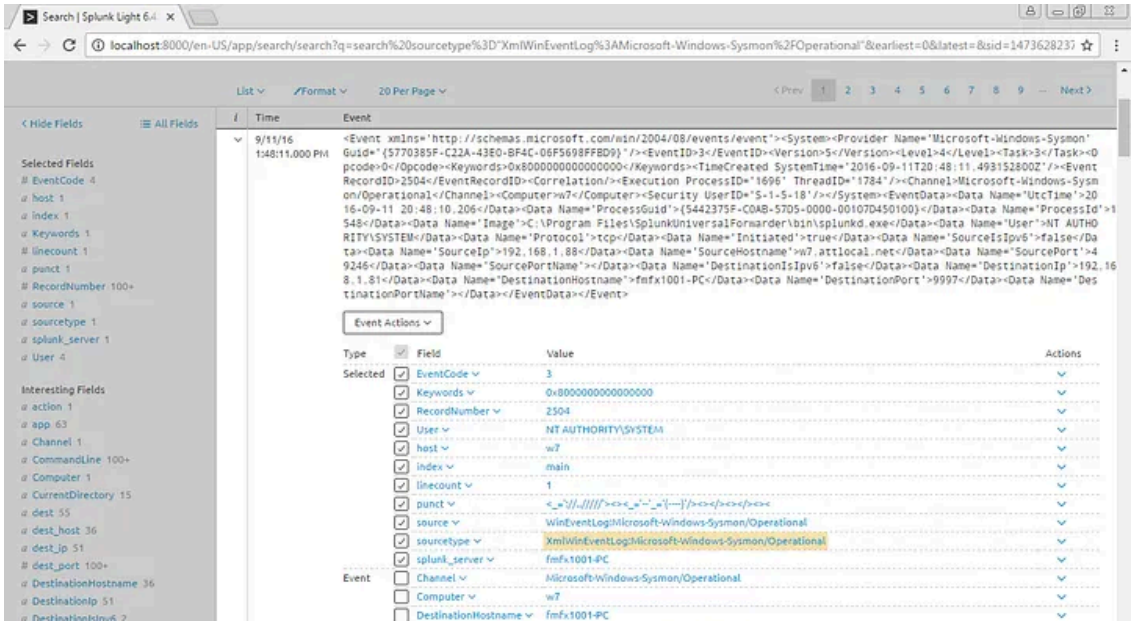
Get David French’s stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

Events in `sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational"` should be parsed into the appropriate fields.

Press enter or click to view image in full size



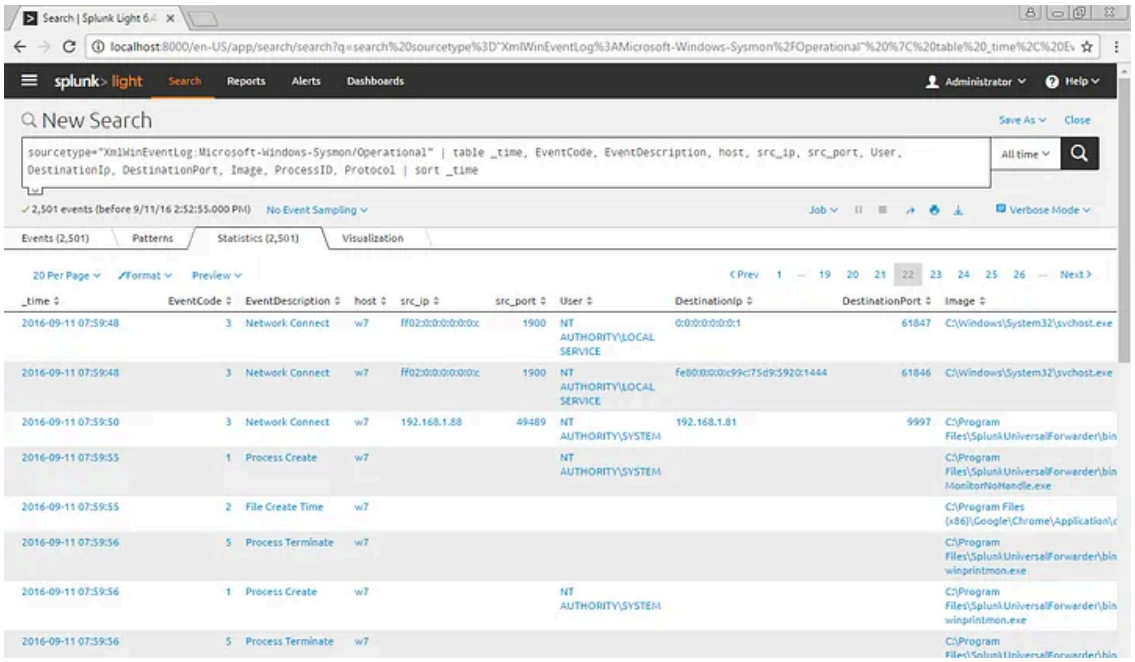
Sysmon Event Codes

In the examples below, we are interested in the following Sysmon event IDs:

```
Event ID 1: Process creation
Event ID 3: Network connection
```

Refer to the official Sysmon page for further details on the various Event Codes: https://technet.microsoft.com/en-us/sysinternals/sysmon

Press enter or click to view image in full size



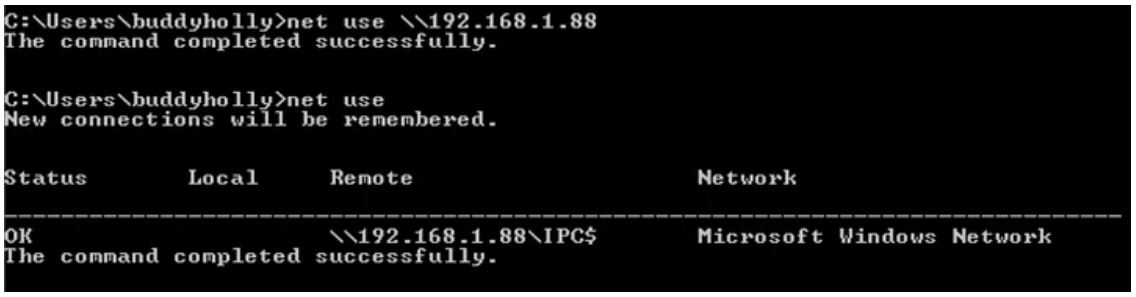
Detecting an Attacker Establishing SMB Sessions to Move Laterally

The attacker uses the following command or similar to establish a session to the victim.

```
net use \\192.168.1.88
```

Windows Admin Shares is MITRE ATT&CK Technique T1077.

Press enter or click to view image in full size



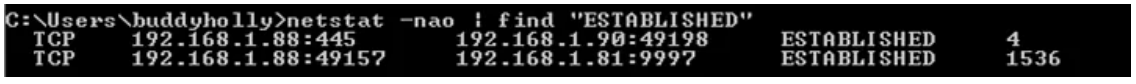
Search sysmon events in Splunk to identify the suspicious SMB (Port 445) session established between the two Windows hosts. See the search string below.

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 192.168.1.90 445
| table _time, EventCode, EventDescription, host, SourceIp, src_port, User, DestinationIp, Destinati
```

Press enter or click to view image in full size

Execute `netstat nao | find "ESTABLISHED"` on the victim computer to view the established SMB session to the attacker.

Press enter or click to view image in full size



Is it normal for a SMB session to be established between these two hosts? Analyze events in your environment, understand what is normal in terms of process creation/termination and network connections established between hosts, and have your analysts investigate and identify abnormal activity.

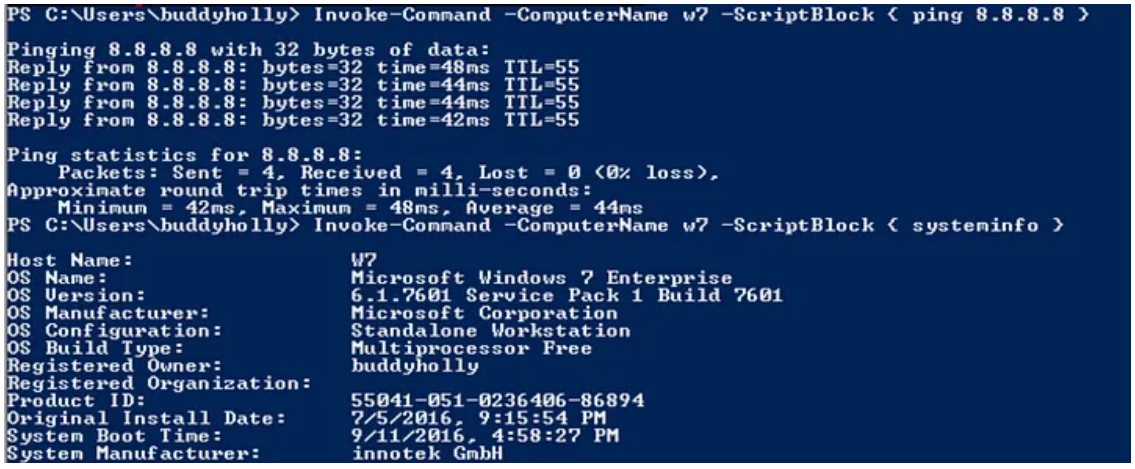
Detecting an Attacker Using PowerShell to Move Laterally

Windows RemoteManagement (WinRM) traffic initiated via PowerShell will be transmitted over ports 5985 and 5986.

Windows Remote Management is MITRE ATT&CK Technique T1028.

In this example, the attacker executes the commands below to remotely execute scripts on the victim or establish a connection to the victim.

Press enter or click to view image in full size

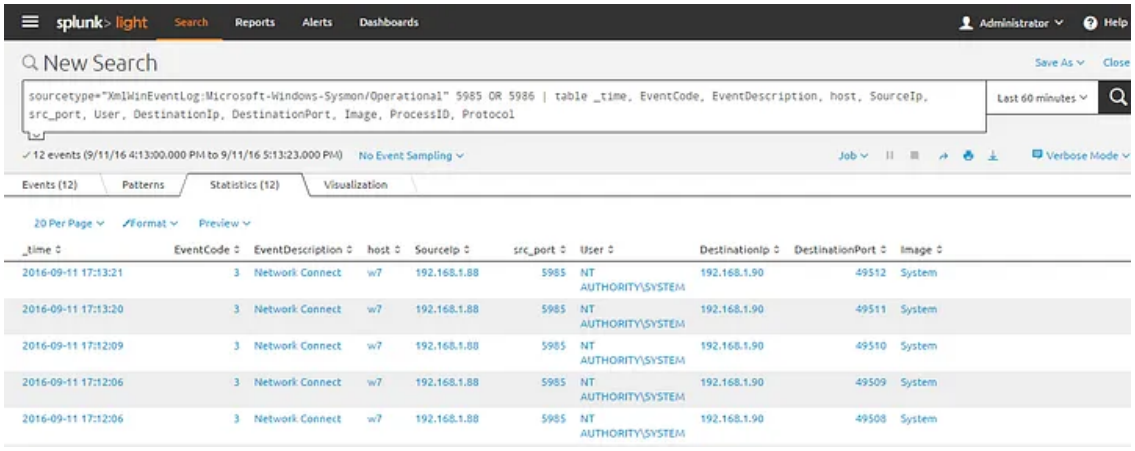


In Splunk, we can see the following Sysmon events to identify the suspicious activity.

We can see WinRM traffic from the attacker to the victim over port 5985.

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" 5985 OR 5986
| table _time, EventCode, EventDescription, host, SourceIp, src_port, User, DestinationIp, Destinati
```

Press enter or click to view image in full size

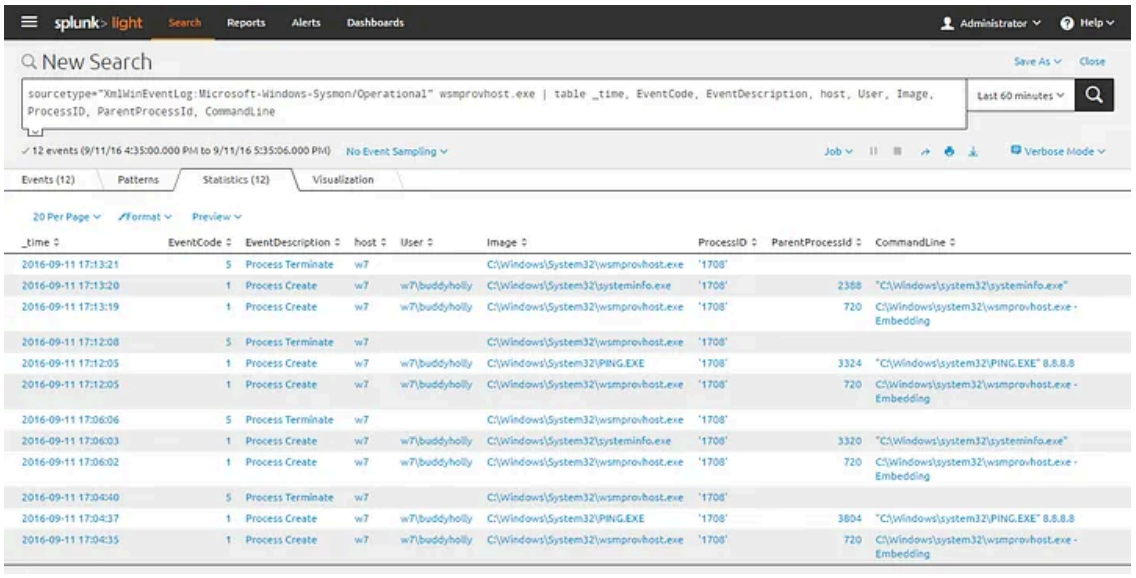


We can see the WinRM Remote PowerShell process (wsmprovhost.exe) on the victim start the ping.exe and systeminfo.exe processes. We can also see the strings entered on the command line. Would this behavior be

normal in your environment?

```
sourcetype="XmlWinEventLog:Microsoft-Windows-Sysmon/Operational" wsmprovhost.exe
| table _time, EventCode, EventDescription, host, Image, ProcessID, ParentProcessId, CommandLine
```

Press enter or click to view image in full size



It is possible that the above activity happens often in your environment, which can make it challenging to differentiate between expected and malicious activity. Attackers will use tools that are native to the OS in the hope that their activities go unnoticed. It is important to be familiar with what's normal in your environment and monitor for behavior that is out of the ordinary.
