Lab 09 – Sysmon, Windows Logs

Compromise Investigation

In this lab, you’ll use Windows logs and Sysmon logs to investigate a possible breach.

1. If you haven’t already, start the Graylog Virtual Machine.
	1. When Graylog boots up, you should see a message in the VM with its IP address.
2. Open Graylog in a web browser, and log in.
	1. Default username and password is admin
3. The dataset for this lab can be obtained by limiting the source and searching for messages over all time.
	1. In the search query, enter source:Host-Compromise and click enter.
		1. You should see 3416 messages
4. Network indicators noticed something suspicious occurring on the Windows machine in the logs. Nothing else is known at this point. See if you can figure out what happened. Ideally, spend some time looking through the logs on your own. If you get stuck, go through the walkthrough, continuing with step 5.

Answer the following:

* What is the “malicious” executable in this case?
* Where did it come from, how did it get on the system?
* Can you identify it? Is it a custom-written tool?
* Who was logged on at the time?
1. Let’s start by looking at processes and network connections. Most of the time, attackers and malware will traverse the network at some point.
	1. Generate a Quick Values chart for EventID 3
	2. source:Host-Compromise AND EventID:3
	3. Are there any processes that shouldn’t normally be making network connections?
2. PowerShell.exe certainly could make network connectinos, but not normally. This might be something to check on.
	1. Click on the plus/magnifying glass to add PowerShell to the search, and click enter.
	2. Generate a quick values chart for DestinationIP to see where PowerShell is connecting
		1. This is a private IP address that we don’t necessairily know about – maybe something to keep investigating.
	3. Generate a QuickValues chart for ProcessID
		1. It looks like just one PowerShell process is running, making all the network connections
	4. Take a look at the histogram. It looks like there are about 12 messages every minute – that is, 12 network connections every minute. It’s fairly consistent – this could be indicative of some beaconing activity.
3. Let’s see if we can find when that PowerShell process was created using Sysmon EventID 1.
	1. source:Host-Compromise AND \*powershell\* AND ProcessID:2220 AND NOT EventID:1
	2. Take a look the event.
		1. CommandLIne: This is how this PowerShell process was created. Notice the encoded payload.
		2. The parent image is cmd.exe -this means it was cmd.exe that started Powershell.exe
		3. Notice the ParentCommandLine, and the clickme.bat file
4. Let’s see if we can find anything else in the logs on clickme.bat
	1. source:Host-Compromise AND \*clickme.bat\*
	2. There are 10 events returned: one process create, one process terminate, one 4688 process create, and 6 file stream creations.
	3. The process creates are from the starting of the powershell.exe process
	4. Look at the Image field in the 6 file stream events, or generate a QuickValues.
		1. All are created using chrome.exe
5. It seems the file was downloaded using Chrome – can we find where it was downloaded from?
	1. Looking at network connection events for chrome.exe, there are 222 events, and no good way to correlate with the clickme file download other than time. If the user visited multiple sites around the same time, that. Can become difficult. This is where correlating network events can be useful!

Summary:

A malicious .bat file was downloaded using chrome, and was subsequently executed. It creates a powershell.exe process that beacons to 192.168.1.104. Through looking at the encoded payload, you might have been able to find this is PowerShell Empire.