Hunting Evil with Sigma (Splunk Edition)

As discussed when introducing Sigma, Sigma rules revolutionize our approach to log analysis and threat detection. What we're dealing with here is a sort of Rosetta Stone for SIEM systems. Sigma is like a universal translator that brings in a level of abstraction to event logs, taking away the painful element of SIEM-specific query languages.

Let's validate this assertion by converting two Sigma rules into their corresponding SPL formats and examining the outcomes.

Example 1: Hunting for MiniDump Function Abuse to Dump LSASS's Memory (comsvcs.dll via rundll32)

A Sigma rule named `proc_access_win_lsass_dump_comsvcs_dll.yml` can be found inside the `C:\Tools\chainsaw\sigma\rules\windows\process_access` directory of the `previous` section's target.

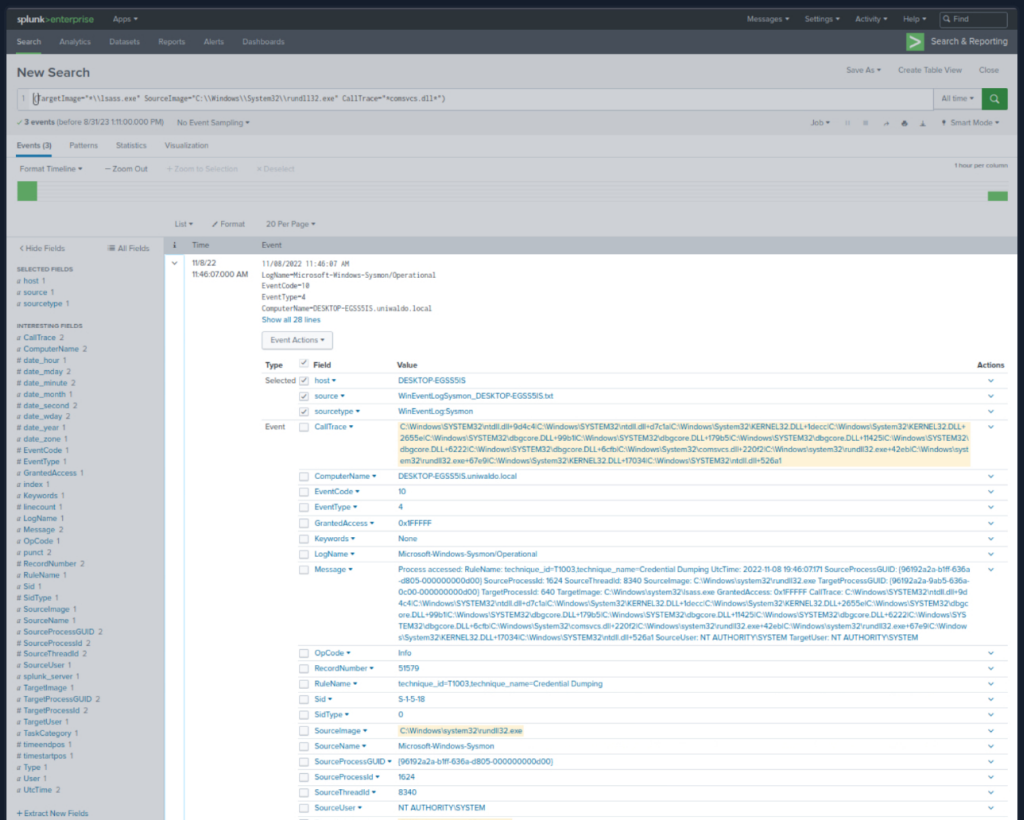
This Sigma rule detects adversaries leveraging the `MiniDump` export function of `comsvcs.dll` via `rundll32` to perform a memory dump from LSASS.

We can translate this rule into a Splunk search with `sigmac` (available at `C:\Tools\sigma-0.21\tools`) as follows.

Hunting Evil with Sigma (Splunk Edition)

```
PS C:\Tools\sigma-0.21\tools> python sigmac -t splunk C:\Tools\chainsaw\sigma\rules\windows\process
(TargetImage="*\\lsass.exe" SourceImage="C:\\Windows\\System32\\rundll32.exe" CallTrace="*comsvcs.d
```

Let's now navigate to the bottom of this section and click on `Click here to spawn the target system!`. Then, let's navigate to `http://[Target IP]:8000`, open the "Search & Reporting" application, and submit the Splunk search `sigmac` provided us with.



My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

The Splunk search provided by `sigmac` was indeed able to detect MiniDump function abuse to dump LSASS's memory.

Example 2: Hunting for Notepad Spawning Suspicious Child Process

A Sigma rule named `proc_creation_win_notepad_susp_child.yml` can be found inside the `C:\Rules\sigma` directory of the `previous` section's target.

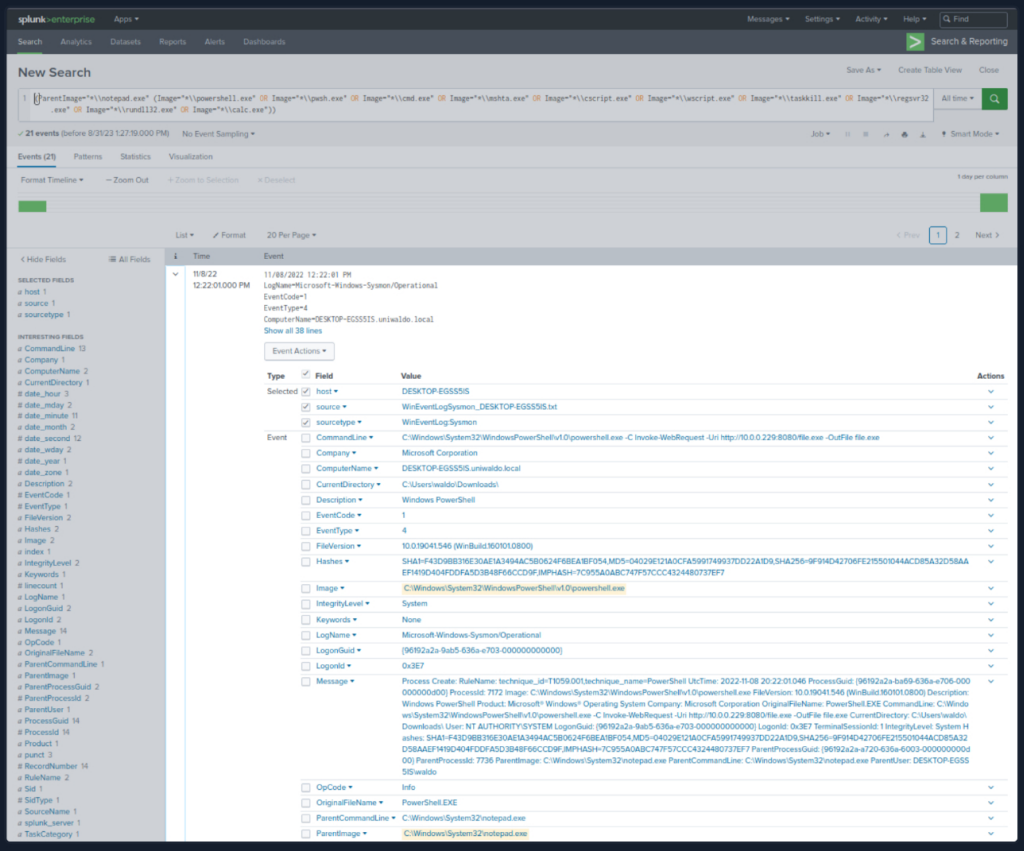
This Sigma rule detects `notepad.exe` spawning a suspicious child process.

We can translate this rule into a Splunk search with `sigmac` (available at `C:\Tools\sigma-0.21\tools`) as follows.

Hunting Evil with Sigma (Splunk Edition)

```
PS C:\Tools\sigma-0.21\tools> python sigmac -t splunk C:\Rules\sigma\proc_creation_win_notepad_susp
(ParentImage="*\\notepad.exe" (Image="*\\powershell.exe" OR Image="*\\pwsh.exe" OR Image="*\\cmd.ex
```

Let's now navigate to the bottom of this section and click on `Click here to spawn the target system!`, if we haven't done that already. Then, let's navigate to `http://[Target IP]:8000`, open the "Search & Reporting" application, and submit the Splunk search `sigmac` provided us with.



The Splunk search provided by `sigmac` was indeed able to detect `notepad.exe` spawning suspicious processes (such as PowerShell).

Please note that more frequently than not you will have to tamper with Sigma's config files (available inside the `C:\Tools\sigma-0.21\tools\config` directory of the previous section's target) in order for the SIEM queries to be readily usable.

VPN Servers

⚠ **Warning:** Each time you "Switch", your connection keys are regenerated and you must re-download your VPN connection file.

All VM instances associated with the old VPN Server will be terminated when switching to a new VPN server.

Existing PwnBox instances will automatically switch to the new VPN server.

US Academy 3 Medium Load

PROTOCOL

UDP 1337 TCP 443

DOWNLOAD VPN CONNECTION FILE

Connect to Pwnbox

Your own web-based Parrot Linux instance to play our labs.

Pwnbox Location

UK 161ms

Terminate Pwnbox to switch location

Start Instance

∞ / 1 spawns left

Waiting to start...

Enable step-by-step solutions for all questions

Questions

Answer the question(s) below to complete this Section and earn cubes!

Download VPN Connection File

Target(s): Click here to spawn the target system!

+ 2 Using sigmac translate the "C:\Rules\sigma\file_event_win_app_dropping_archive.yml" Sigma rule into the equivalent Splunk search. Then, navigate to http://[Target IP]:8000, open the "Search & Reporting" application, and submit the Splunk search sigmac provided. Enter the TargetFilename value of the returned event as your answer.

C:\Users\waldo\Downloads\20221108112718_BloodHound.zip

Submit Hint