proofpoint

ET Splunk Technical Add-On

Tech Brief

Overview:

The ET Splunk Technical Add-On (ET-TA) allows ET customers with Splunk implementations to greatly enhance their ability to enrich and search any log with ET Intelligence data. The ET-TA provides two primary functions:

1. Automatically Downloads, Installs, and Updates the ET Intelligence reputation list into Splunk.
2. Provides several Splunk Macros which allow organizations to build their own complex queries using not just ET, but virtually any data, including with other Splunk features and TA's.

This document will examine how to leverage the ET-TA to find suspicious activity in your network by enriching your enterprise security logs with ET Intelligence and then searching that data with ET Splunk Macros.

Identifying Suspicious Network Activity in Splunk with ET

This first workflow will examine finding suspicious activity in your Splunk log database in a single query. To effectively demonstrate this, we will create a query which defines the following information.

1. Filter Input Data (Recommended)
2. Select ET macro, and define field to match/enrich (Required)
3. Filter output Data (Recommended)

In this example we will look to enrich our FW logs with ET Intelligence. Normally FW logs only contain information that pertains only to that connection, and not any reputation or auxiliary information. A firewall will not normally raise any alerts if the traffic is permitted by policy. In this example we will search for logs whose destination are known to be involved in CNC activity.

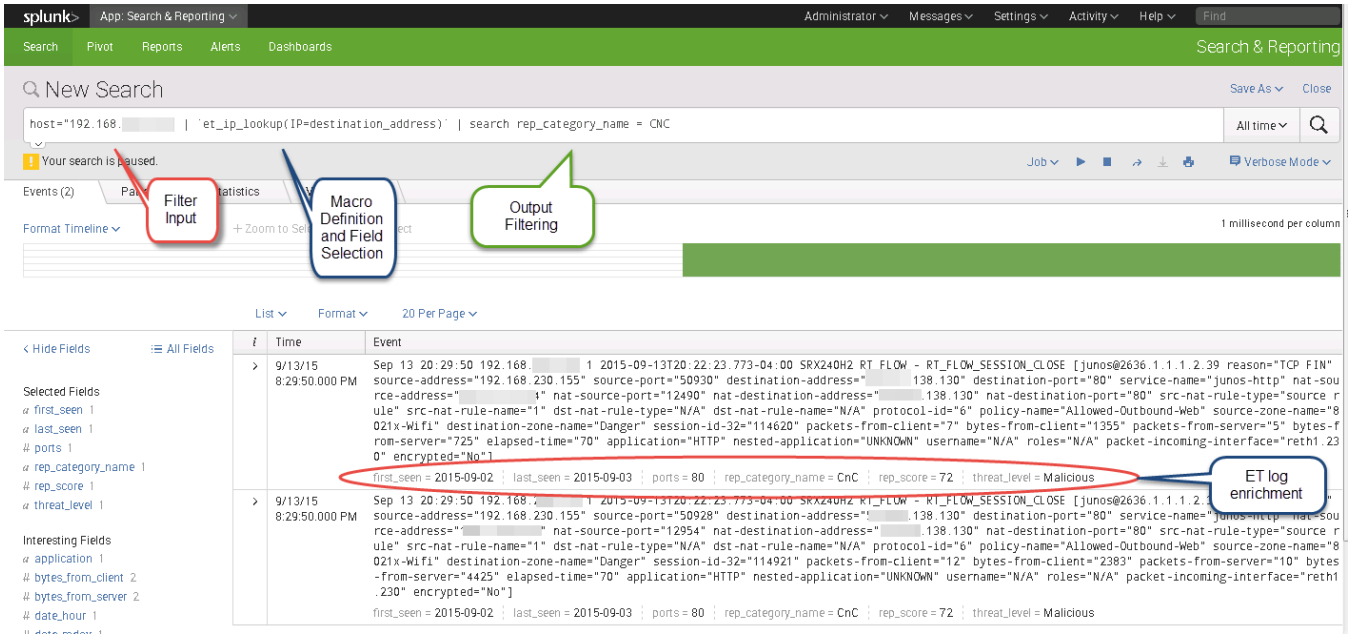

Figure 1: Finding Suspicious Activity in Network Logs

As you can see from Figure 1, we have searched through our Splunk log database to enrich our logs with ET Intelligence data, and then further searched to find any firewall logs who matched the Category CNC (or command and control.) We could then take this query and turn it into a dashboard, report, alert, or any other built in Splunk feature. We can also use it to form more complex log queries or feed logs into other macros and apps. Because the macro allows you to define what the IP field of your logs that you want to search, the ET-TA can input logs from any log source, so long as Splunk can parse it, the ET-TA can extract and enrich the data.

Recognizing Compromised Machines through DNS Profiling

Malicious attackers often use DNS to help ensure that their attack infrastructure is available and that no one command and control or exploit source can be taken offline if the offending machine is seized. ET Intelligence can help to identify both pre and post network compromise by examining DNS logs which are generated by internal machines. ET-TA can examine the DNS logs to identify hosts which are trying to resolve IP addresses for malicious domains. This is a high confidence mechanism to identify that a host is compromised or an attack has been leveraged against it.

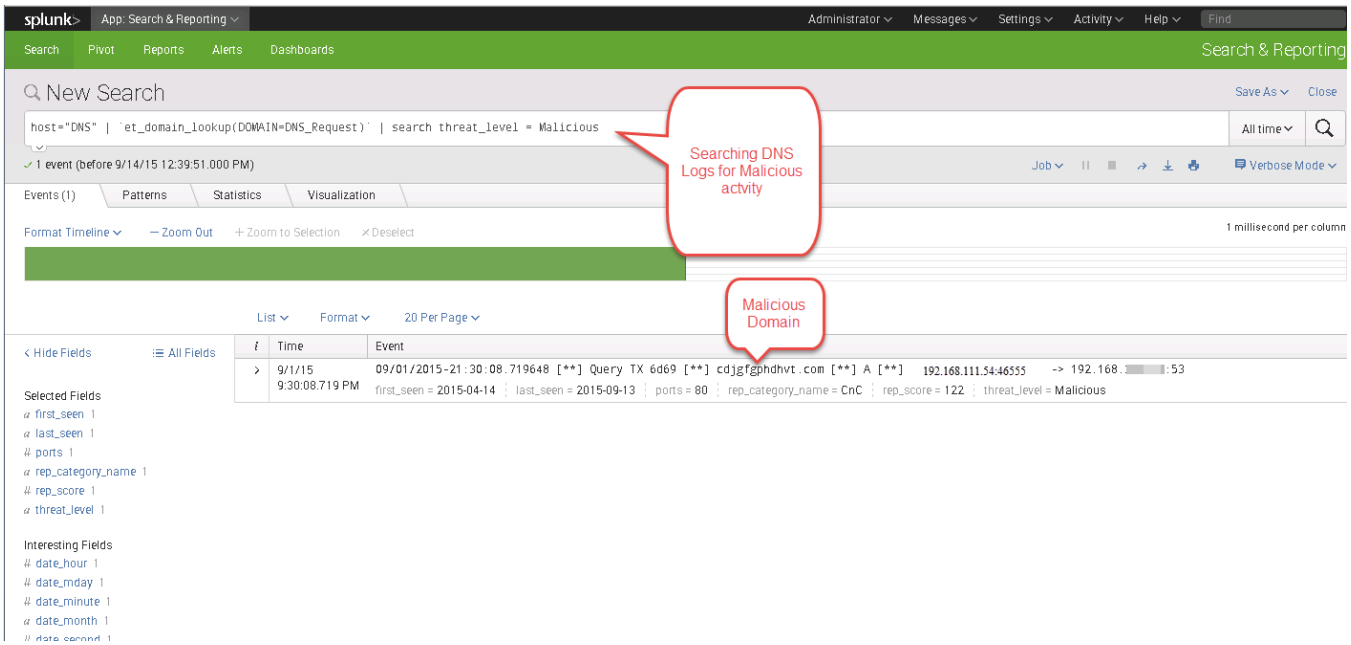

Figure 2: Identifying Network Compromise with DNS Profiling

In our second example, we have used the ET-TA to search through our DNS logs and enrich them with ET Intelligence data to find activity consistent with network compromise. In this case, we leveraged Suricata's built in DNS logging capabilities, but you can use any log source that can collect the Fully Qualified Domain Name in an event source which Splunk can process. Here we are searching all logs from our host called DNS, to enrich the data, specifically with logs who have the field DNS_Request, and display those who match the threat level of malicious.

The query provides us with output matching these conditions, and identifies that host 192.168.111.54 made queries for the malicious domain "cdjgfgphdhvt.com" With this information, we can evaluate the machine to investigate it further to determine why it is asking after a condemned domain.

Summary

Logs from network security devices like firewalls, IDS, proxies, as well as network infrastructure like DNS can provide a wealth of forensic information which is waiting to be unleashed. While the traditional logs provide little in the way of context, the ET-TA for Splunk can enrich the logs in your Splunk database with the acclaimed ET Intelligence reputation store and provide a time saving mechanism to efficiently identify malicious activity.