Integrate Grizzly steppe attacks detection script

EventTracker Enterprise
Abstract

This guide provides instructions to generate report of network traffic from internal network systems to grizzly steppe IP's.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 8.x and later.

Audience

EventTracker users, who wish to analyze network traffic from internal network systems to grizzly steppe IP's.
# Table of Contents

Abstract .................................................................................................................................................. 1  
Scope .................................................................................................................................................. 1  
Audience............................................................................................................................................. 1  
Introduction ........................................................................................................................................... 3  
Pre-requisites ........................................................................................................................................ 3  
Configuring GRIZZLY STEPPE detection script ................................................................................. 3  
EventTracker Knowledge Pack (KP)...................................................................................................... 6  
Report................................................................................................................................................... 6
Introduction

Russia’s civilian and military intelligence services engaged in aggressive and sophisticated cyber-enabled operations targeting the U.S. government and its citizens. The U.S. Government refers to this activity as GRIZZLY STEPPE. These cyber operations included spear-phishing campaigns targeting government organizations, critical infrastructure entities, think tanks, universities, political organizations, and corporations, and theft of information from these organizations. This stolen information was later publicly released by third parties.

EventTracker helps you to detect GRIZZLY STEPPE attack using PowerShell script. We need to run this script once an EventTracker NCM event or traffic report is generated and persisted in database. This report gives us information about the traffic which is related with grizzly steppe IP’s.

Pre-requisites

- EventTracker 8.x and later should be installed.
- NCM events or network traffic report should be scheduled with “Persist data in EventVault Explorer” option enabled.
- PowerShell execution policy should be unrestricted.
- PowerShell SQLPS module should be imported.

Configuring GRIZZLY STEPPE detection script

1. Scheduled flex reports (Cisco ASA: Traffic details, NCM-All new network Connection report or any other traffic report) after importing them.

2. During scheduling, please check Persist Data and select all the columns to persist.
**NOTE:** Please note down the field which contains Public IP address like ‘Source Address” in case of ‘Cisco ASA-Traffic details” report and ‘Remote address” in case of ‘NCM-All new network Connection report”

3. Now, wait for the report to run as per schedule time or run it manually.

4. Once the report is generated, please import PowerShell module for Grizzly Steppe detection.

   ```
   Import-Module .\GSdetectionmodule.psm1
   ```

5. After importing Grizzly steppe module, please run the following command to generate Grizzly steppe traffic report:

   ```
   Get-GrizzlysteppeReport -Remoteaddressfield "Source Address" -Reverselookup enable -Geolocationlookup enable -Addedby "ETAdmin" -Queueid "719" -Outfile "C:\Users\etadmin\desktop\Grizzly steppe traffic report.csv" -Startdate "2017\01\05" -Enddate "2017\01\10"
   ```

**SYNTAX**
- Remoteaddressfield ‘persisted report field which contains public IP address”
- Reverselookup ‘enables it for reverse lookup of public IP address”
- Geolocationlookup ‘enables it for geolocation lookup of public IP address”
- Addedby ‘gives username like ‘ETAdmin” by whom persisted report is added”
- Queueid ‘gives queue id of persisted report like ‘919”
- Outfile ‘directory location where CSV report is located.”

**NOTE:** For getting added by and queue id of persist report, run the following SQL command against ‘EventTracker” database. Following are the command:

```
SELECT [ID], [ReportTitle], [AddedBy]
FROM [eventtrackerdata].[dbo].[tbl_RptQueue]
where ReportTitle = 'Report Name' and QueueType = '133'
```

E.g. For report ‘Cisco ASA-Traffic details”:

```
SELECT [ID], [ReportTitle], [AddedBy]
FROM [eventtrackerdata].[dbo].[tbl_RptQueue]
where ReportTitle = 'Cisco ASA-Traffic details' and QueueType = '133'
```
EventTracker Knowledge Pack (KP)

After running GRIZZLY STEPPE script, it will generate CSV report. Following are the reports it will generate:

Report

- **Grizzly Steppe–Traffic details:** This report gives us the information about the network traffic details from internal IP address to Grizzly Steppe IP address.

Following are the grizzly steppe traffic report extracted from Cisco ASA–Traffic details persisted report.

<table>
<thead>
<tr>
<th>Grizzly steppe-Traffic details</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Source Port</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Bytes</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>host:192.168.253-38.nec5.to</td>
<td>10.0.0.1</td>
<td>192.168.5.9</td>
<td>80</td>
<td>0</td>
<td>TCP</td>
<td>8176</td>
<td>0:02:48</td>
</tr>
<tr>
<td>pr.net.sinp.egypt.yahoo.com</td>
<td>10.0.0.1</td>
<td>192.168.5.9</td>
<td>80</td>
<td>0</td>
<td>TCP</td>
<td>3724</td>
<td>0:02:48</td>
</tr>
<tr>
<td>bflip0009.pip.pf.com</td>
<td>10.0.0.1</td>
<td>192.168.5.9</td>
<td>80</td>
<td>0</td>
<td>TCP</td>
<td>0</td>
<td>0:00:00</td>
</tr>
</tbody>
</table>

Following are the grizzly steppe traffic report extracted from NCM–All new network connection report

<table>
<thead>
<tr>
<th>Grizzly step - Traffic details</th>
<th>Source Hostname</th>
<th>Source IP</th>
<th>Source Port</th>
<th>Destination Hostname</th>
<th>Destination IP</th>
<th>Destination Port</th>
<th>Protocol</th>
<th>Bytes</th>
<th>Duration</th>
</tr>
</thead>
<tbody>
<tr>
<td>customer.client</td>
<td>192.168.1.140</td>
<td>123.45</td>
<td>80</td>
<td>fast100.nl.rapid</td>
<td>192.168.1.140</td>
<td>80</td>
<td>TCP</td>
<td>5129</td>
<td>0:02:00</td>
</tr>
<tr>
<td>customer.client</td>
<td>192.168.1.140</td>
<td>123.45</td>
<td>80</td>
<td>fast100.nl.rapid</td>
<td>192.168.1.140</td>
<td>80</td>
<td>TCP</td>
<td>5129</td>
<td>0:02:00</td>
</tr>
<tr>
<td>fast100.nl.rapid</td>
<td>192.168.1.140</td>
<td>123.45</td>
<td>80</td>
<td>customer.client</td>
<td>192.168.1.140</td>
<td>80</td>
<td>TCP</td>
<td>5129</td>
<td>0:02:00</td>
</tr>
<tr>
<td>fast100.nl.rapid</td>
<td>192.168.1.140</td>
<td>123.45</td>
<td>80</td>
<td>customer.client</td>
<td>192.168.1.140</td>
<td>80</td>
<td>TCP</td>
<td>5129</td>
<td>0:02:00</td>
</tr>
<tr>
<td>fast100.nl.rapid</td>
<td>192.168.1.140</td>
<td>123.45</td>
<td>80</td>
<td>customer.client</td>
<td>192.168.1.140</td>
<td>80</td>
<td>TCP</td>
<td>5129</td>
<td>0:02:00</td>
</tr>
</tbody>
</table>