EventTracker
Secure. Comply. Succeed.

Integrate Grizzly steppe attacks detection script

EventTracker Enterprise

Publication Date: Jan. 24, 2017

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

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

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.

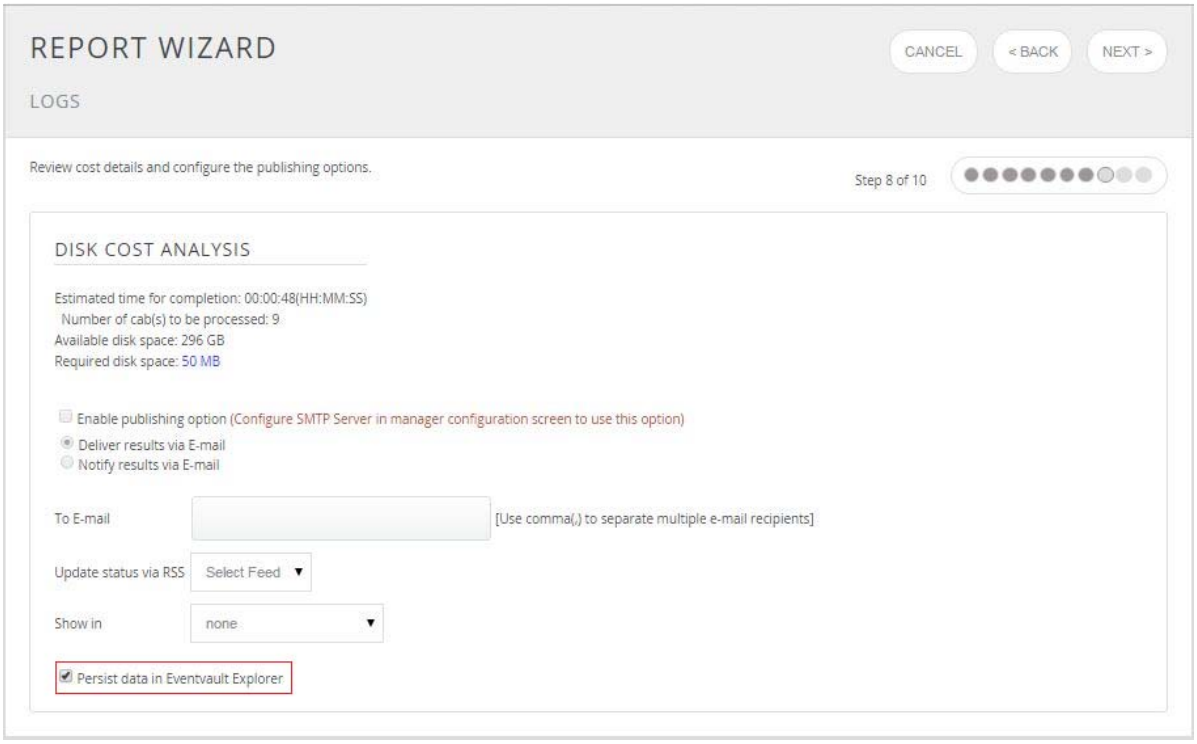

Figure 1

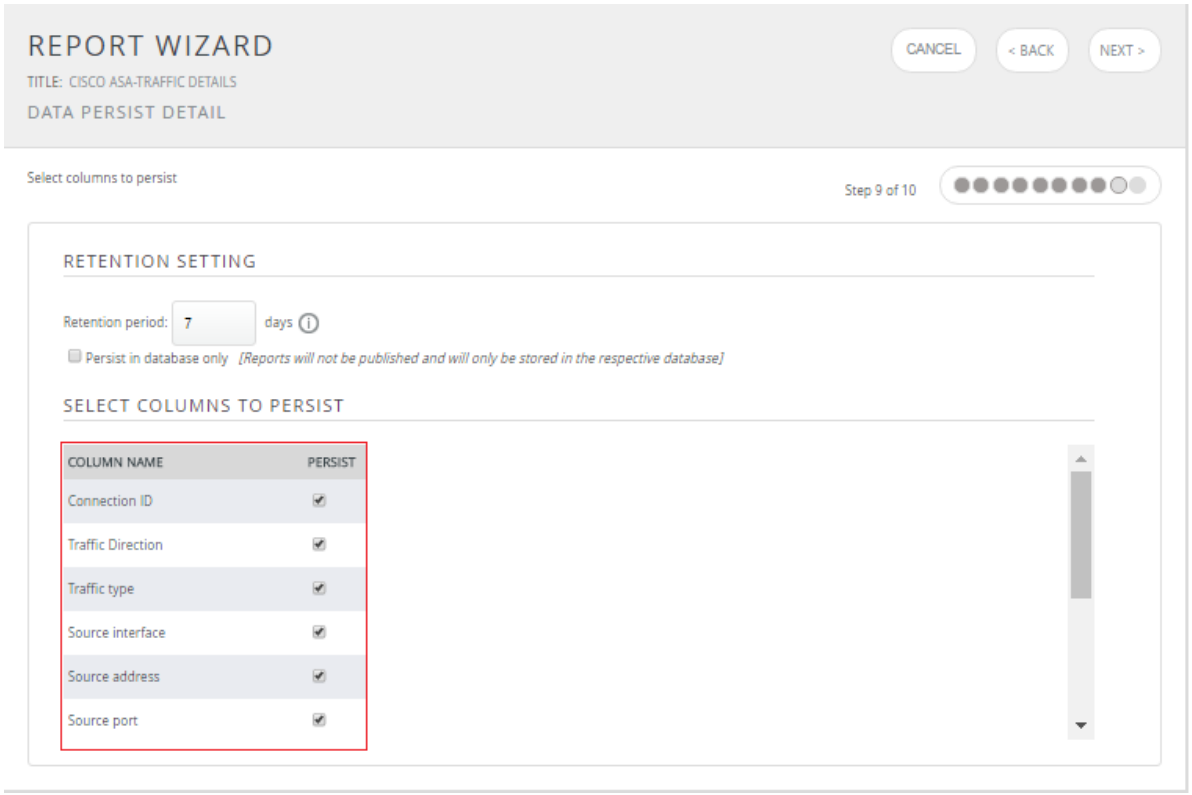

Figure 2

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.

Grizzly steppe-Traffic details

FQDNName	Country	City	LogTime	Traffic type	Source address	Source interface	Source port	Destination address	Destination interface	Destination port	Bytes	Duration
host-198-167-223-38.resolv.to	United States	San Jose	1/8/2017 21:52	TCP	199.68.196.125	OUTSIDE	33510	192.168.3.20	DMZ	443	0	0:00:00
pr.comet.vip.ne1.yahoo.com	United States	Sunnyvale	1/7/2017 15:06	TCP	98.138.79.73	OUTSIDE	443	192.168.5.9	INSIDE	52714	8179	0:02:49
bf1onepush.vip.bf1.yahoo.com	United States	Sunnyvale	1/7/2017 15:03	TCP	72.30.196.161	OUTSIDE	443	192.168.5.9	INSIDE	51230	178099	0:18:32
host-198-167-223-38.resolv.to	United States	San Jose	1/7/2017 10:22	TCP	199.68.196.125	OUTSIDE	41297	192.168.5.230	INSIDE	80	0	0:00:00
ne1onepush.vip.ne1.yahoo.com	United States	Sunnyvale	1/4/2017 7:51	TCP	98.138.199.240	OUTSIDE	443	192.168.5.9	INSIDE	58633	281207	0:06:12
msnbot-65-55-252-43.search.msn.com	United States	Redmond	1/3/2017 19:27	TCP	65.55.252.43	OUTSIDE	443	192.168.5.32	INSIDE	58072	10700	0:00:00
normalcitizen.spirosandreou.com	Sweden		1/3/2017 15:43	UDP	46.29.248.238	OUTSIDE	53	192.168.5.216	INSIDE	58820	55	0:02:02
pr.comet.vip.ne1.yahoo.com	United States	Sunnyvale	1/3/2017 15:48	TCP	98.138.79.73	OUTSIDE	443	192.168.5.9	INSIDE	56029	6224	0:00:00
bf1onepush.vip.bf1.yahoo.com	United States	Sunnyvale	1/3/2017 15:48	TCP	72.30.196.161	OUTSIDE	443	192.168.5.9	INSIDE	55297	69080	0:49:22
pr.comet.vip.ne1.yahoo.com	United States	Sunnyvale	1/3/2017 15:48	TCP	98.138.79.73	OUTSIDE	443	192.168.5.9	INSIDE	55304	58757	0:49:21
win2.scisiraq.net	Iraq		1/3/2017 15:50	UDP	185.76.35.11	OUTSIDE	53	192.168.5.216	INSIDE	59880	351	0:00:00
win2.scisiraq.net	Iraq		1/3/2017 15:37	UDP	185.76.35.10	OUTSIDE	53	192.168.5.216	INSIDE	59159	308	0:00:00

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

Grizzly steppe - Traffic details

ReverseDNS	Country	City	LogTime	Process Name	Image File Name	Local Address	Local Hostname	Remote Address	Local Port	Remote Port
customer.clients	Netherlands	Meppel	1/4/2017 18:17	chrome.exe	C:\Program Files (x8	192.168.1.140	PNPL-6-KP.Toons.	185.104.9.39	51291	80
customer.clients	Netherlands	Meppel	1/4/2017 18:17	chrome.exe	C:\Program Files (x8	192.168.1.140	PNPL-6-KP.Toons.	185.104.11.154	51290	443
adsl-065-015-088	United States	Atlanta	1/4/2017 18:17	chrome.exe	C:\Program Files (x8	192.168.1.140	PNPL-6-KP.Toons.	65.15.88.243	51289	80
adsl-065-015-088	Russia		1/4/2017 18:17	chrome.exe	C:\Program Files (x8	192.168.1.140	PNPL-6-KP.Toons.	95.213.157.140	51288	443
fast130.nl.rapids	Netherlands		1/4/2017 18:17	chrome.exe	C:\Program Files (x8	192.168.1.140	PNPL-6-KP.Toons.	95.211.214.81	51287	80