EventTracker
Secure. Comply. Succeed.

# Emerging Threat Blocked IP List Import

Publication Date: March 2, 2015

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

# About this Guide:

In the recent times we have seen increase in SPAM and different kind of attacks which occurs frequently. Many security research organizations such as Spamhaus keep track of the Internet's spam operations and sources, to provide dependable real-time anti-spam protection for Internet networks. There are other organizations who maintain the compromised or top attacker source ip addresses such as Dshield, abuse.ch and spyeye tracker.

Emerging Threats blocked ip list contains the SPAM source or top attackers source ip addresses from different sources which is downloaded by EventTracker.

EventTracker's IP activity monitoring feature extracts the IP addresses from all the logs received into EventTracker in real-time and allows user to lookup the IP address against the downloaded IP address list from Emerging Threat. This helps EventTracker users to detect any network communication happening from such known vulnerable IP addresses.

# Scope:

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.4 and later.

# Audience:

IT/Security or network administrators, who are responsible for monitoring and maintaining the security of the network.

# Table of Contents:

# Introduction

In the recent times we have seen increase in SPAM and different kind of attacks which is occurring frequently. Many security research organizations such as Spamhaus keep track of the Internet's spam operations and sources, to provide dependable real-time anti-spam protection for Internet networks. There are other organizations who maintain the compromised or top attacker source ip addresses such as Dshield, abuse.ch and spyeye tracker.

Emerging Threats blocked IP list contains the SPAM source or top attackers' source IP addresses from different sources which is downloaded by EventTracker.

EventTracker's IP activity monitoring feature extracts the IP addresses from all the logs received into EventTracker in real-time and allows users to lookup the IP address against the downloaded IP address list from Emerging Threat. This helps EventTracker users to detect any network communication happening from such known vulnerable IP addresses.

Example uses:

- Track any network communication happening from the IP address known to be source of attacker. Attackers may succeed after multiple failed attempts.

- Take precautionary measures such as hardening the server, or blocking the connection from those ip addresses to your network.

# Pre-requisite

- EventTracker v7.5 and later should be installed and List Management feature should be present.
- Windows PowerShell 4.0 and later must be installed.
  To check the PowerShell version:
  - Launch Windows PowerShell as Administrator.
  - Run command $PSVersionTable.PSVersion
- Script Execution policy must be set to Unrestricted.
  To change PowerShell execution policy,
  - Launch Windows PowerShell as Administrator.
  - Run command 'Set-Execution Policy Unrestricted".
  - Make sure you do this for both x86 and x64 versions.
- Critical servers or devices logs should be collected to EventTracker.

# How it works?

The List Management option in EventTracker, allows users to maintain the list of IP address. EmergingThreatBlockedIPListimport script downloads the known attackers IP addresses from https://rules.emergingthreats.net/fwrules/emerging-Block-IPs.txt daily at scheduled interval.

# Setting up Emerging Threat Blocked IP List Import

## Preparing Scripts for use as per your environment

- Contact support@eventtracker.com to obtain the EmergingThreatBlockedIPListimport Script pack.
- Save EmergingThreatBlockedIPListimportScript.zip (saved to D:\EmergingThreatBlockedIPListimportScript\folder in the example below).
- Extract all files to D:\EmergingThreatBlockedIPListimportScript\.
- Make sure all the checklists mentioned in the prerequisite section has been installed and configured.
- Files in the package are shown below.


Figure 1

- Copy the files in the install path under ScheduledActionScripts folder.

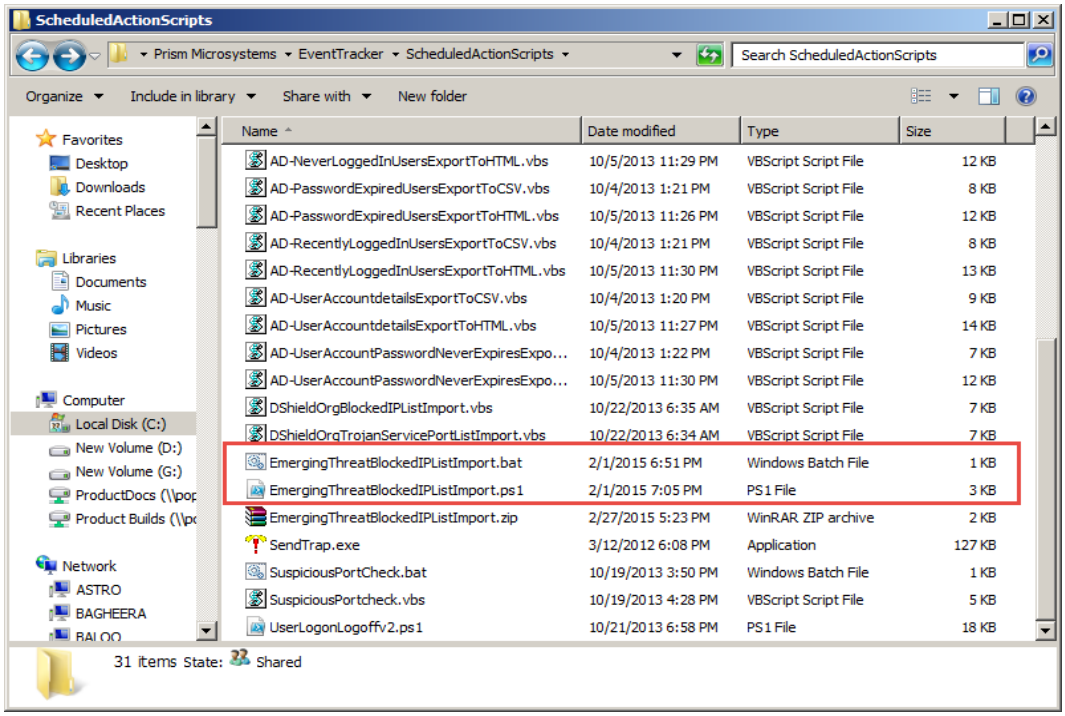



Figure: 2

## Create a Group under IP Address

- Log in to **EventTracker Web** and select **List Management** from **Admin** drop-down list.

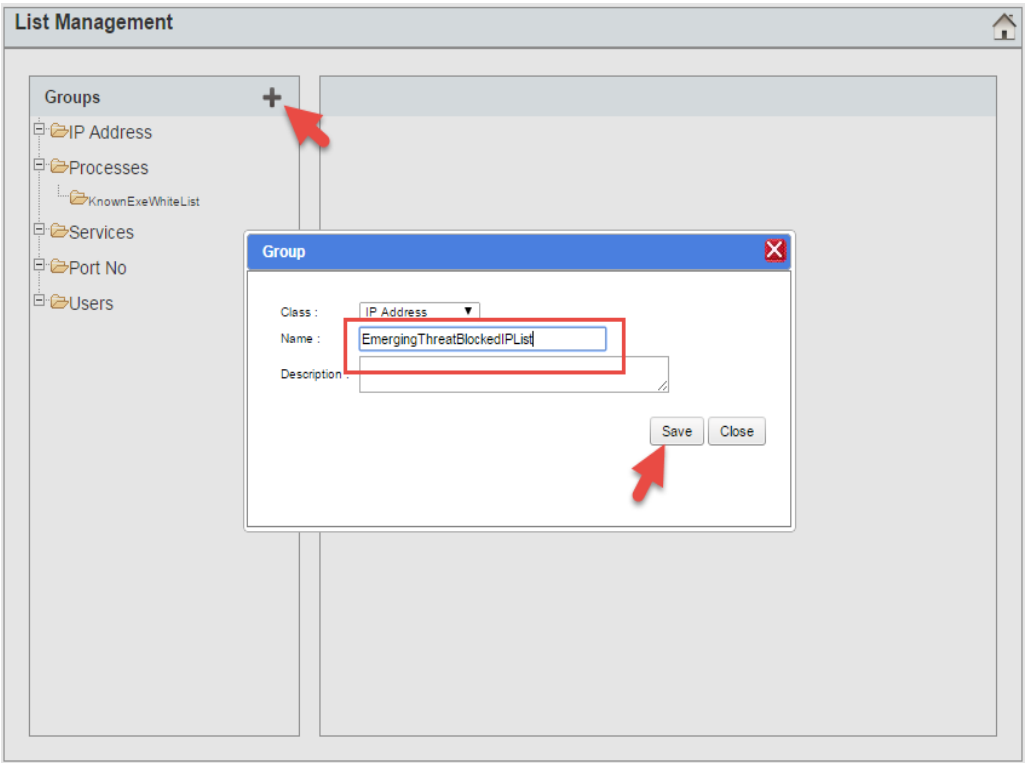



Figure: 3

- Add a group named as **EmergingThreatBlockedIPList** and click on **Save.**

The **EmergingThreatBlockedIPList** group gets created, as shown in the figure below:

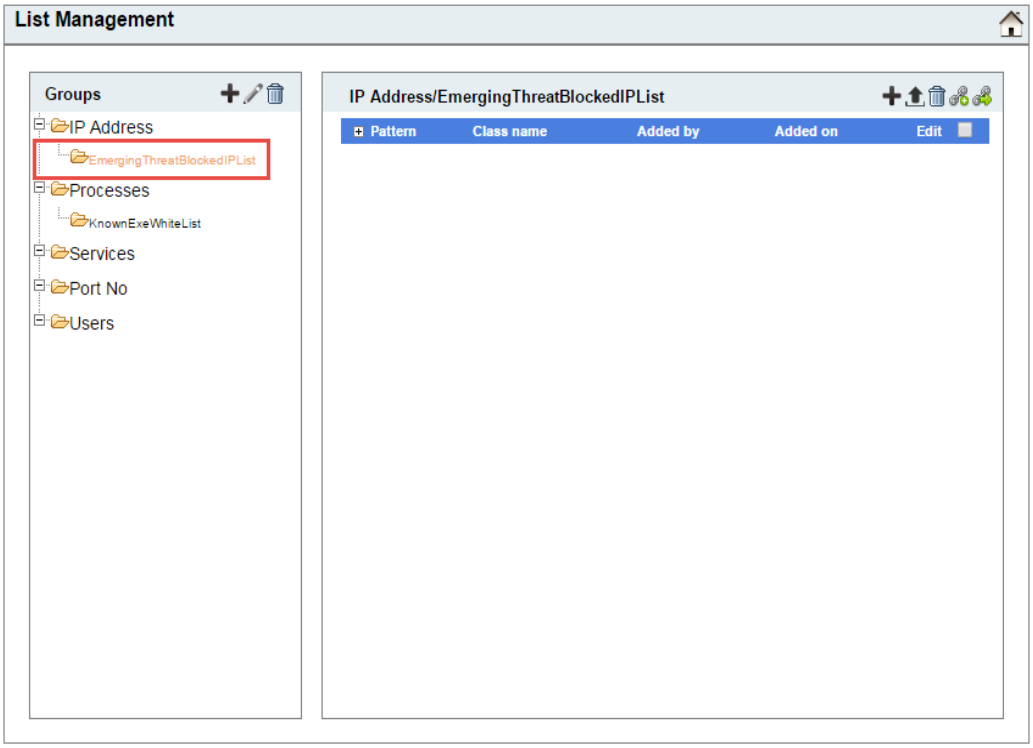



Figure: 4

## Schedule the Task

- Go to **Tools** and select **Scheduled Scripts** for the drop down list.
- Click on **Add New**.

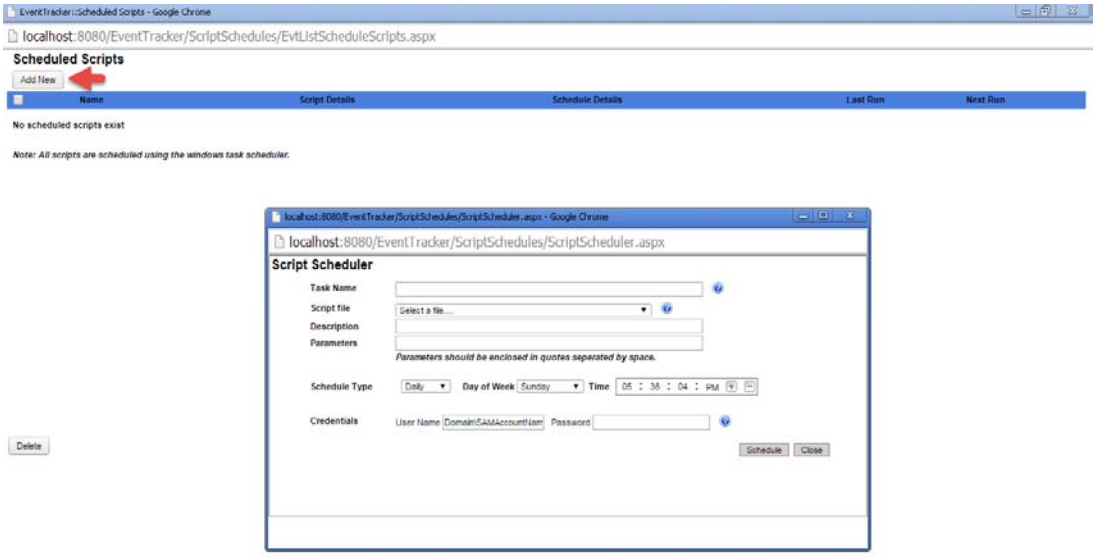



Figure: 5

- Add the Task Name and select the **EmergingThreatBlockedIPListImport.bat file** from the drop down list.

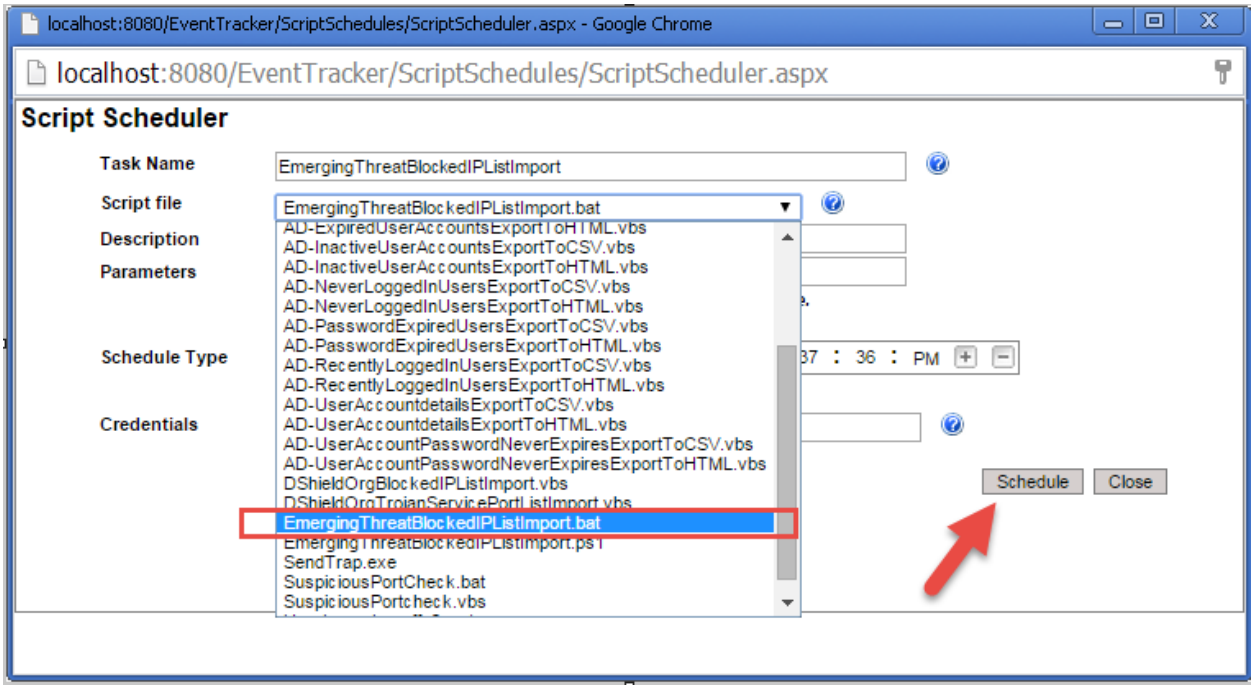



Figure: 6

- Provide your user credentials and click the **Scheduled** button.
- The Scheduled Script gets listed as highlighted in the figure below:

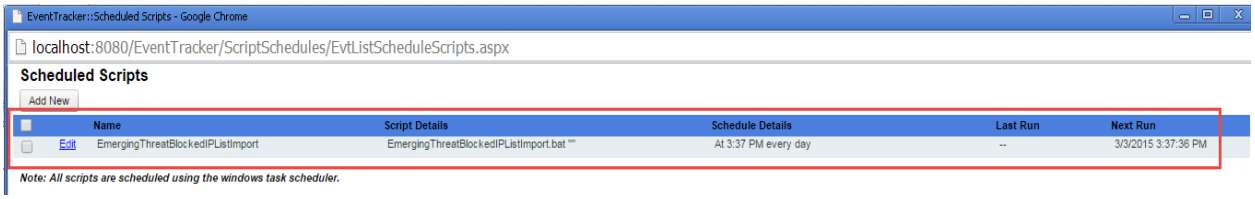



Figure: 7

**NOTE**: All the IP addresses will be listed under the **EmergingThreatBlockedIPList** group only after it runs on the scheduled time. After the list gets displayed, you can follow the below mentioned process.

- Now, go to **Admin** and select **List Management**.
- Click on the **EmergingThreatBlockedIPList** group.

All the IP Addresses are listed as shown in the below mentioned figure:

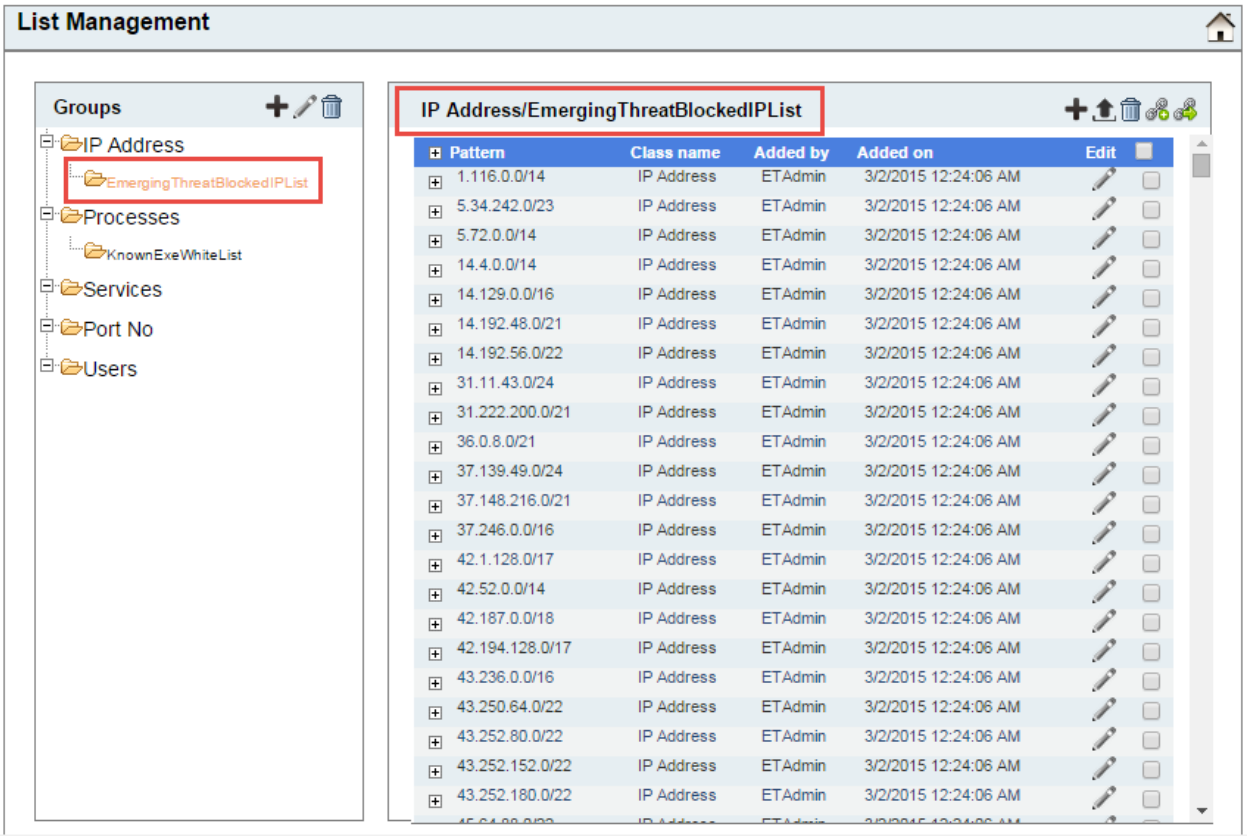



Figure: 8

## Lookup the Emerging Threat Blocked IP in Behavior

- Now, go to **Behavior** and select **Operations**.
- In **Behavior**, select the **IP Address Activity** from the drop down list.
- Click the List Lookup  icon.

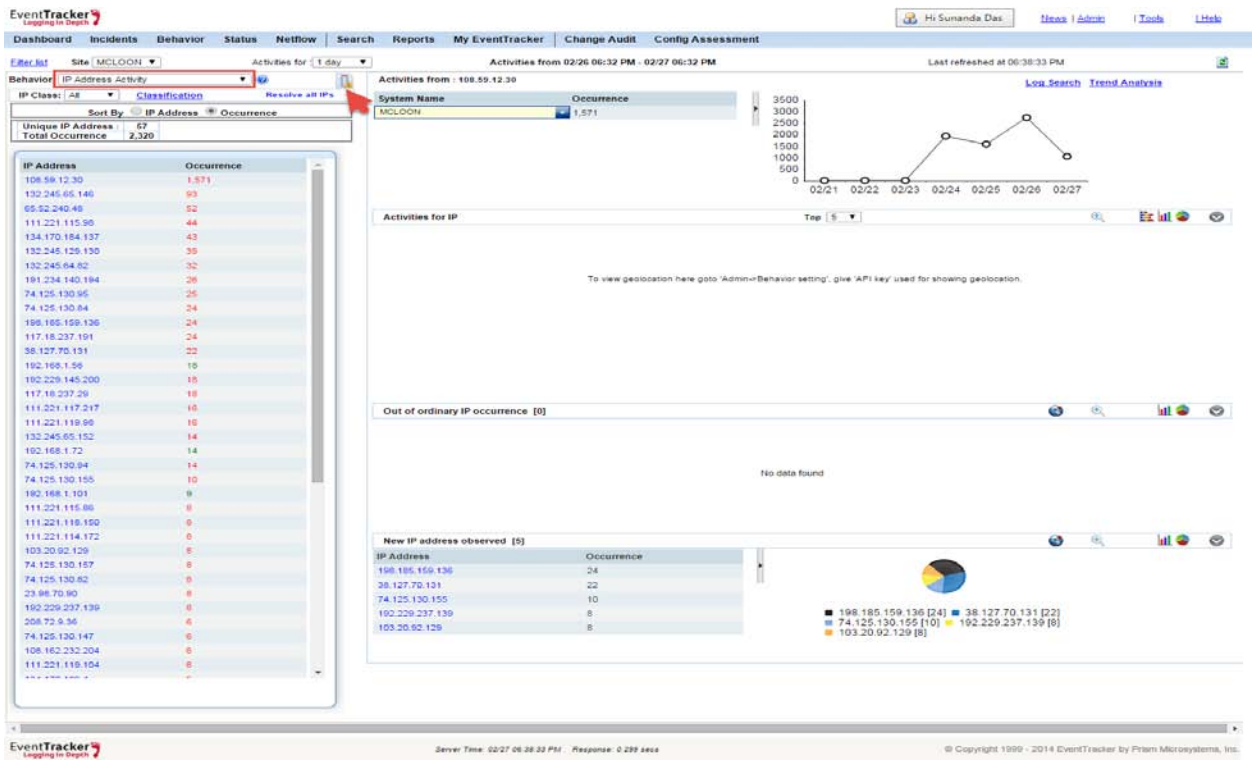
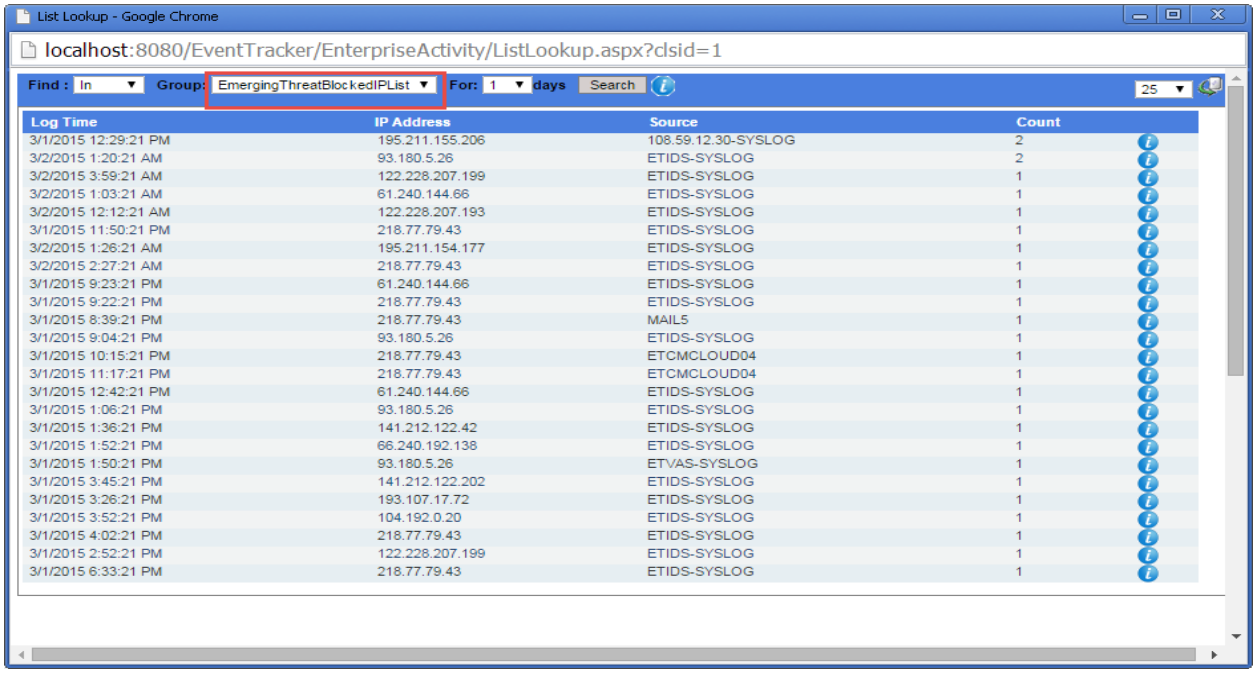


Figure: 9

- All the IP Address in the mentioned time range gets listed in the List Lookup window.




| Log Time | IP Address | Source | Count |
|---|---|---|---|
| 3/1/2015 12:29:21 PM | 195.211.155.206 | 108.59.12.30-SYSLOG | 2 |
| 3/2/2015 1:20:21 AM | 93.180.5.26 | ETIDS-SYSLOG | 2 |
| 3/2/2015 3:59:21 AM | 122.228.207.199 | ETIDS-SYSLOG | 1 |
| 3/2/2015 1:03:21 AM | 61.240.144.66 | ETIDS-SYSLOG | 1 |
| 3/2/2015 12:12:21 AM | 122.228.207.193 | ETIDS-SYSLOG | 1 |
| 3/1/2015 11:50:21 PM | 218.77.79.43 | ETIDS-SYSLOG | 1 |
| 3/2/2015 1:26:21 AM | 195.211.154.177 | ETIDS-SYSLOG | 1 |
| 3/2/2015 2:27:21 AM | 218.77.79.43 | ETIDS-SYSLOG | 1 |
| 3/1/2015 9:23:21 PM | 61.240.144.66 | ETIDS-SYSLOG | 1 |
| 3/1/2015 9:22:21 PM | 218.77.79.43 | ETIDS-SYSLOG | 1 |
| 3/1/2015 8:39:21 PM | 218.77.79.43 | MAIL5 | 1 |
| 3/1/2015 9:04:21 PM | 93.180.5.26 | ETIDS-SYSLOG | 1 |
| 3/1/2015 10:15:21 PM | 218.77.79.43 | ETCMCLOUD04 | 1 |
| 3/1/2015 11:17:21 PM | 218.77.79.43 | ETCMCLOUD04 | 1 |
| 3/1/2015 12:42:21 PM | 61.240.144.66 | ETIDS-SYSLOG | 1 |
| 3/1/2015 1:06:21 PM | 93.180.5.26 | ETIDS-SYSLOG | 1 |
| 3/1/2015 1:36:21 PM | 141.212.122.42 | ETIDS-SYSLOG | 1 |
| 3/1/2015 1:52:21 PM | 66.240.192.138 | ETIDS-SYSLOG | 1 |
| 3/1/2015 1:50:21 PM | 93.180.5.26 | ETVAS-SYSLOG | 1 |
| 3/1/2015 3:45:21 PM | 141.212.122.202 | ETIDS-SYSLOG | 1 |
| 3/1/2015 3:26:21 PM | 193.107.17.72 | ETIDS-SYSLOG | 1 |
| 3/1/2015 3:52:21 PM | 104.192.0.20 | ETIDS-SYSLOG | 1 |
| 3/1/2015 4:02:21 PM | 218.77.79.43 | ETIDS-SYSLOG | 1 |
| 3/1/2015 2:52:21 PM | 122.228.207.199 | ETIDS-SYSLOG | 1 |
| 3/1/2015 6:33:21 PM | 218.77.79.43 | ETIDS-SYSLOG | 1 |

Figure: 10

- The user can further perform a Log search on a selected IP Address. For this, put the cursor on the particular IP Address and select the **Log Search** option from the drop down box, as shown in the figure:

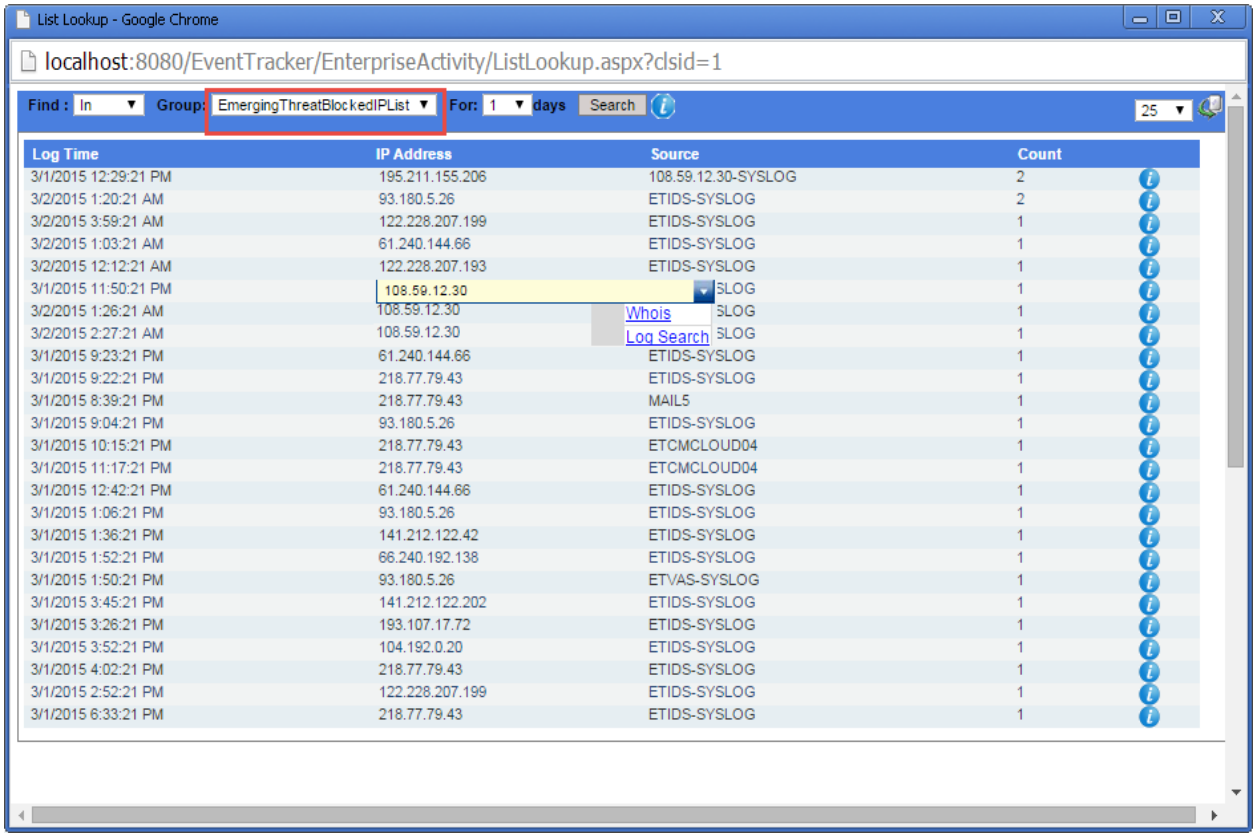



Figure: 10