EventTracker
Secure. Comply. Succeed.

I-Blocklist BlueTack Proxy IP List Import

Publication Date: April 29, 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. BlueTack frequently updates the Tor and known proxies' IP list.

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 Iblocklist. This helps EventTracker users to detect any network communication happening from or to such Unallocated address space which is known to be spoofed.

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.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred. © 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents:

Introduction

Blutack Tor and proxy IP list contains the known Tor and proxies IP address list 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. This helps EventTracker users to detect any network communication happening from such known 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 v7x and later should be installed and List Management feature should be present.
- Windows PowerShell 3.0 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. Iblocklistbluetackproxyiplistimport script downloads the known Tor and IP addresses from http://list.iblocklist.com/?list=xoebmbyexwuiogmbyprb&fileformat=p2p&archiveformat=zip daily at scheduled interval.

Setting up I-Blocklist BlueTack Proxy IP List Import

Preparing Scripts for use as per your environment

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

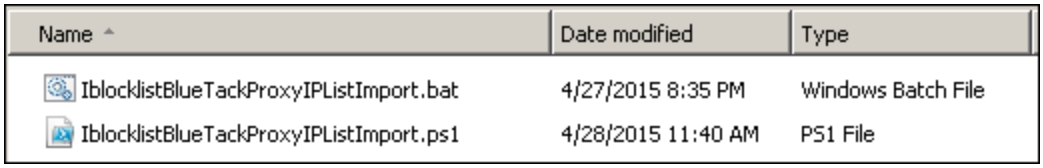

Figure 1

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

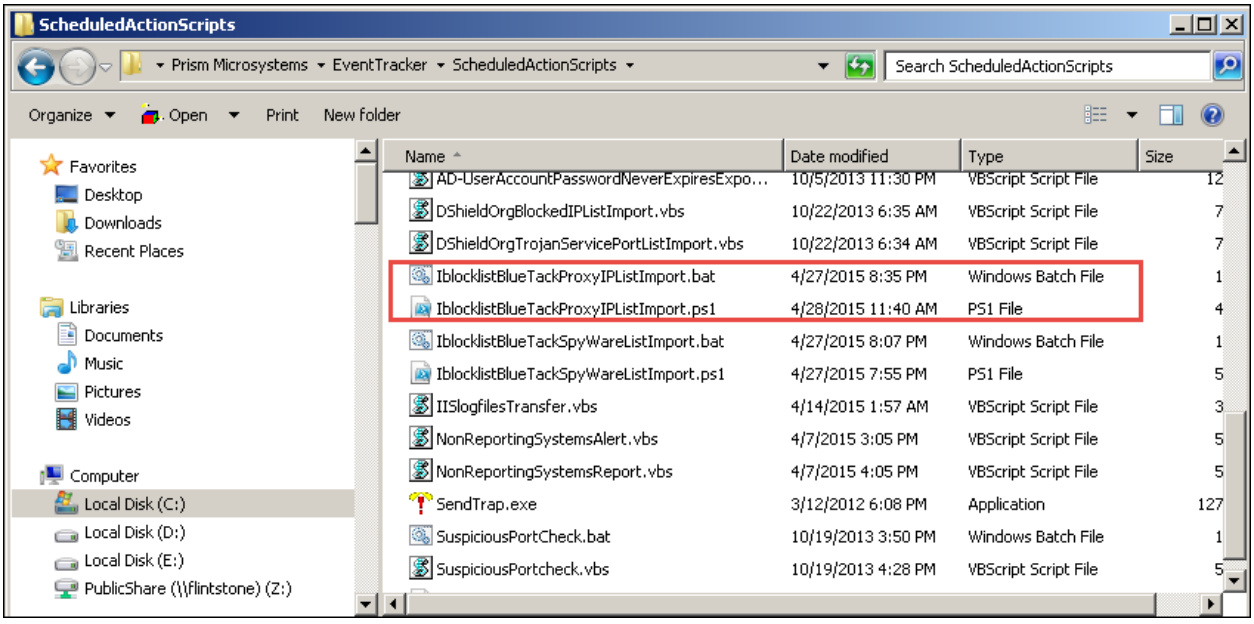

Figure: 2

Schedule the Task

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

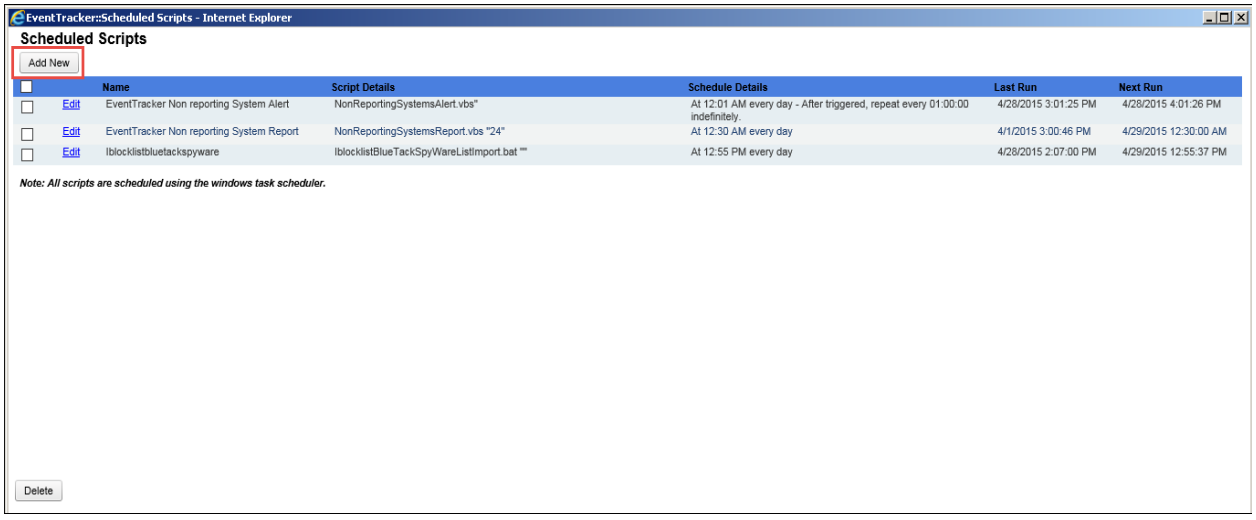

Figure: 3

The Script Scheduler window displays:

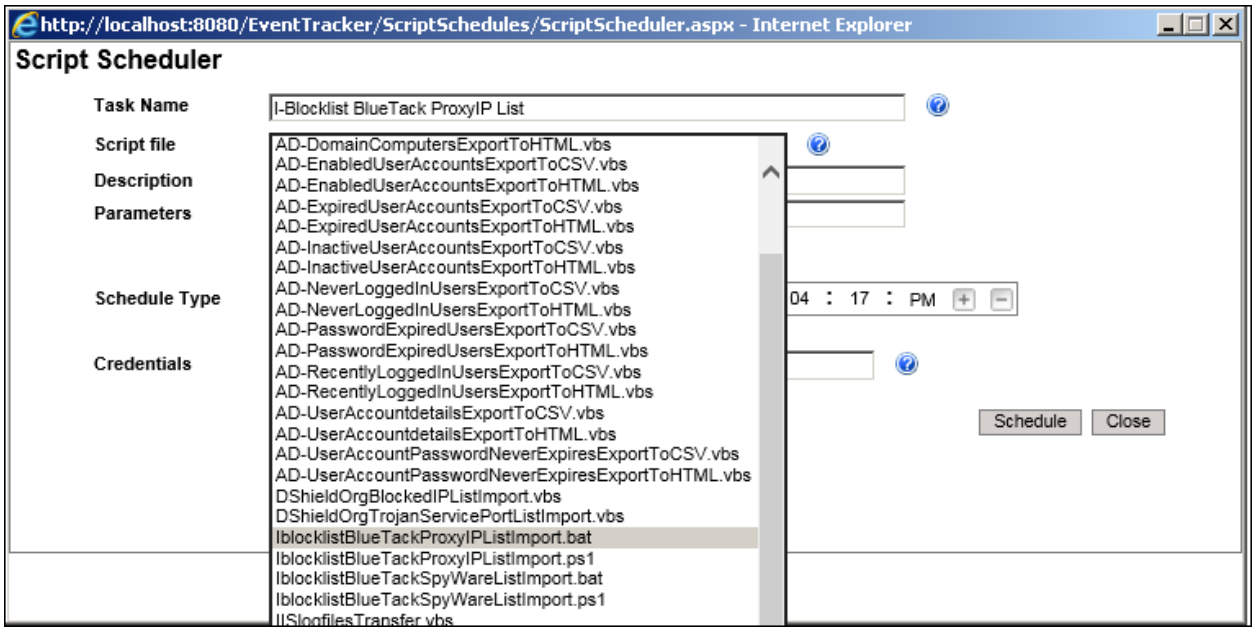

Figure: 4

- Add the Task Name and select the **IblocklistBlueTackProxyIPListImport.bat file** from the drop down list.
- Provide your user credentials and click the **Scheduled** button.
- The Scheduled Script gets listed as highlighted in the figure below:

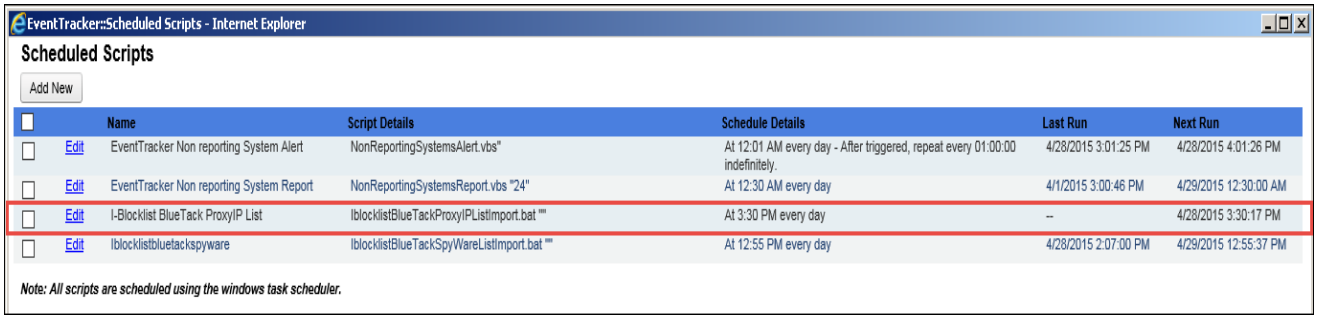

Figure: 5

NOTE: All the IP addresses will be listed under the **IblocklistBlueTackProxyIPListImport** group only after it runs on the scheduled time. Once it runs on scheduled time, you can follow the below mentioned process.

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

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

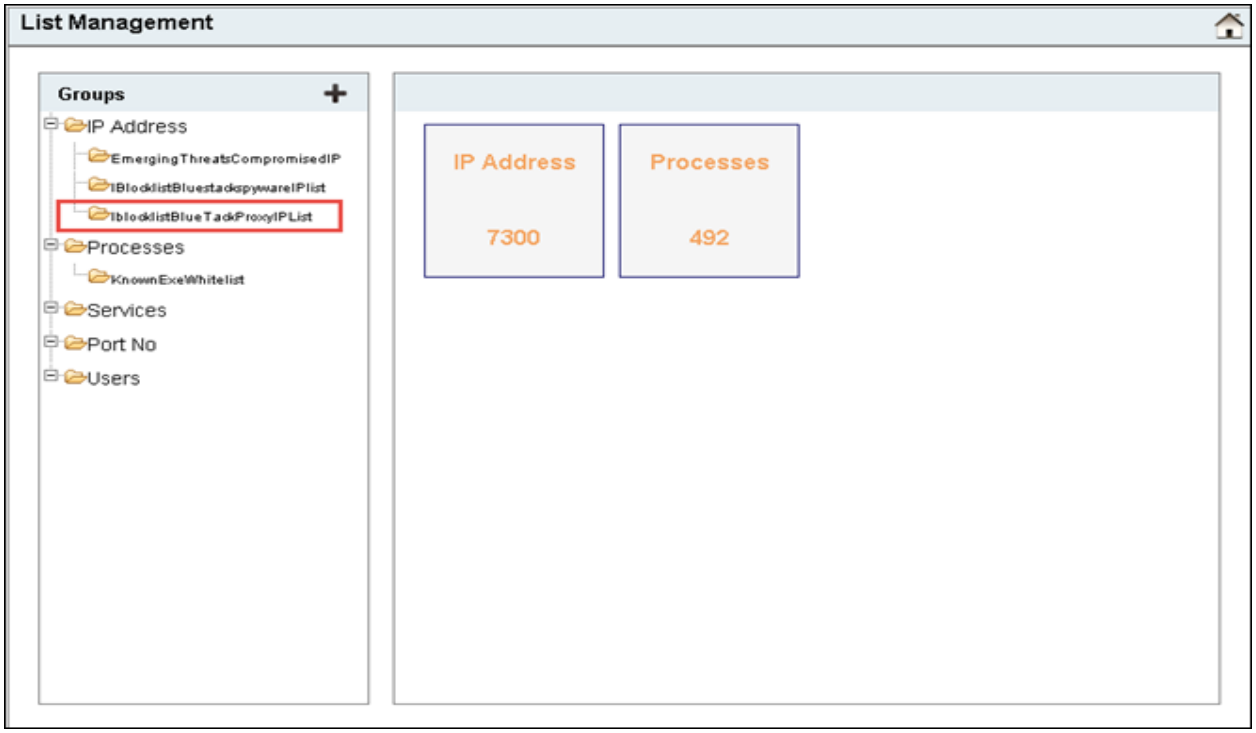

Figure: 6

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

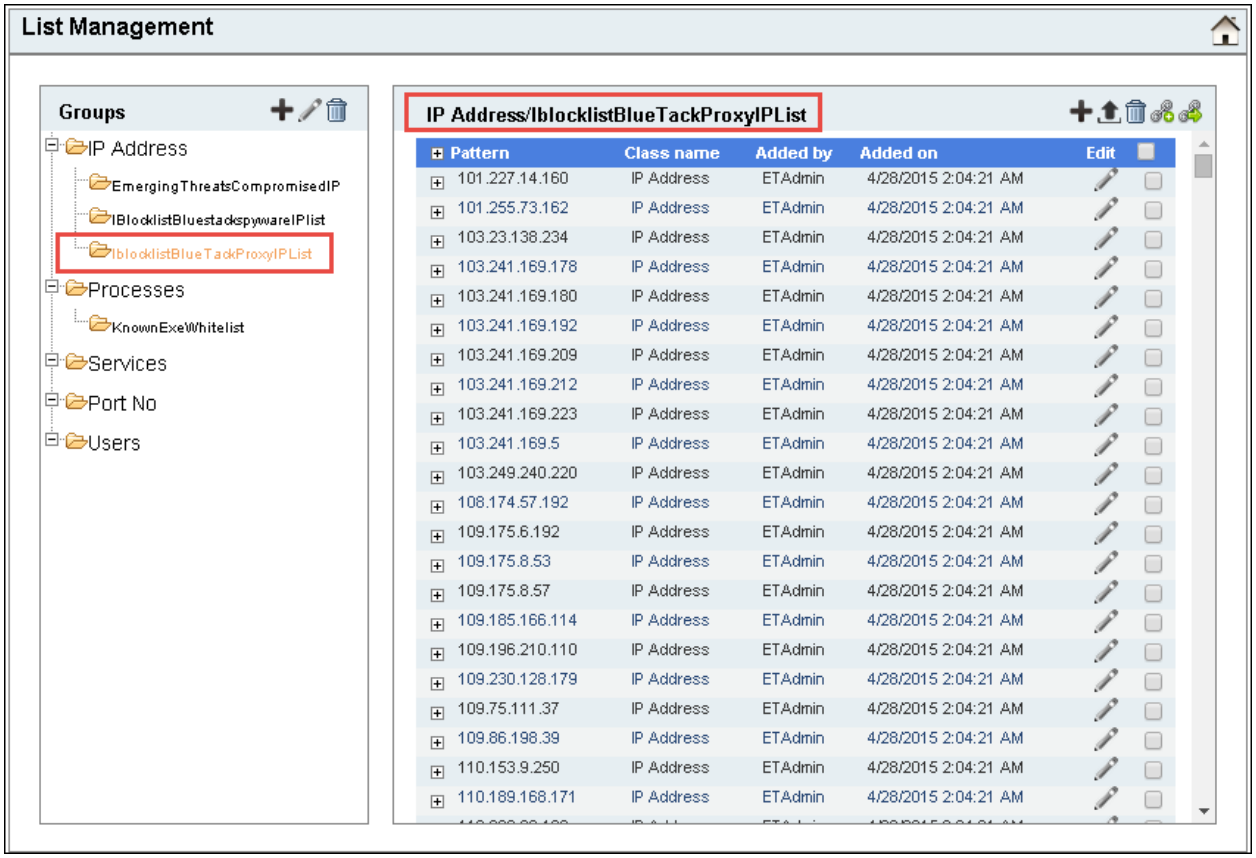

Figure: 7

Lookup the I-Blocklist BlueTack Proxy 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.
- All the IP Address in the mentioned time range gets listed in the List Lookup window.
- 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.