I-Blocklist BlueTack Spyware List Import
About this Guide:

Blutack Spyware IP list contains the list of IP address which is known for distributing spyware 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 spyware IP address list. This helps EventTracker users to detect any network communication happening from such known IP addresses.

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 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 ................................................................................................................................................. 3
Pre-requisite................................................................................................................................................ 4
How it Works?................................................................................................................................................5

Setting up I-Blocklist BlueTack Spyware List Import.............................................................................. 6
  Preparing Scripts for use as per your environment .............................................................................. 6
Scheduled Task.......................................................................................................................................... 7

Lookup the I-Blocklist BlueTack Spyware List Import in Behavior ........................................................... 9
Introduction

Blutack Spyware IP list contains the Known malicious spyware and adware IP Address ranges 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. The `IblocklistbluetackspywareIListimport` script downloads the unallocated address space from [http://list.iblocklist.com/?list=llvtlsyoyiczbkjsxpf&fileformat=p2p&archiveformat=ZIP](http://list.iblocklist.com/?list=llvtlsyoyiczbkjsxpf&fileformat=p2p&archiveformat=ZIP) daily.
Setting up I-Blocklist BlueTack Spyware List Import

Preparing Scripts for use as per your environment

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

<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IblocklistBlueTackSpyWareListImport.bat</td>
<td>4/27/2015 8:07 PM</td>
<td>Windows Batch File</td>
</tr>
<tr>
<td>IblocklistBlueTackSpyWareListImport.ps1</td>
<td>4/27/2015 7:55 PM</td>
<td>PS1 File</td>
</tr>
</tbody>
</table>

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

---

Figure 1

Figure 2
Schedule the Task

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

![Figure: 3](image)

The Script Scheduler window displays:

![Figure: 4](image)
Add the Task Name and select the `IblocklistBlueTackSpyWareListImport.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:

![Scheduled Scripts](image)

**Figure: 5**

**NOTE:** All the IP addresses will be listed under the `IblocklistBlueTackSpyWareListImport` 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 `IblocklistBlueTackSpyWareListImport` group gets created, as shown in the figure below:

![List Management](image)

**Figure: 6**
All the IP Addresses are listed as shown in the below mentioned figure:

**List Management**

- Group:
  - Emerging Threats Compromised IP
  - BlueTack Malware

- Processes
- Services
- Port No
- Users

**IP Address I-Blocklist BlueTack Spyware List Import**

- Pattern
- Class name
- Added by
- Added on
- Edit

- 198.13.132
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 4.21.117.128-159
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 4.21.149.0-31
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 4.49.4.32-63
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 4.49.119.0-127
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.179.87
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.38.47.28
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.39.29.257
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.39.29.221
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.78.86.19
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.101.162.4-255
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.101.162.31
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.135.20.116
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.135.26.255
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.135.26.168
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.135.127.88
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.114.129.51
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.116.36.99
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 5.198.109.147
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 6.281.72.111
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

- 8.154.40.255
- P Address
- ET-Admin
- 4/28/2015 2:05:28 AM

Figure: 7

**Lookup the I-Blocklist BlueTack Spyware 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.