radware

BOT RISK SCANNER

Integration Guide

(VERSION – 1.0.4)

CONTENTS

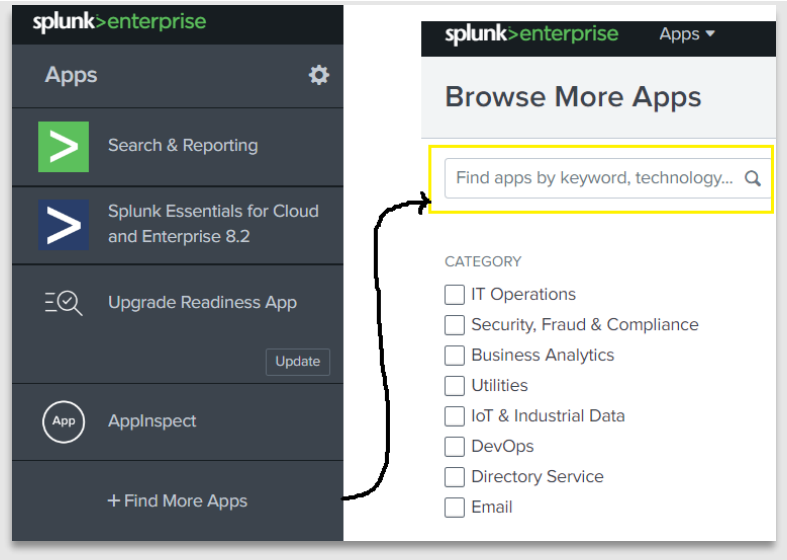
INTRODUCTION

The Radware Bot Risk Scanner (BRS) is a free, Splunk-based bot analyzer that provides comprehensive insights into an application's bad bot traffic without requiring any additional integrations. The tool is available for installation as a plugin on the Splunk Marketplace (Link) and can be easily enabled through the GUI. This plugin offers a detailed dashboard with insights into the application's traffic and the types of bots attempting to access the system. This document outlines the installation process for the Bot Risk Scanner through the Splunk Marketplace.

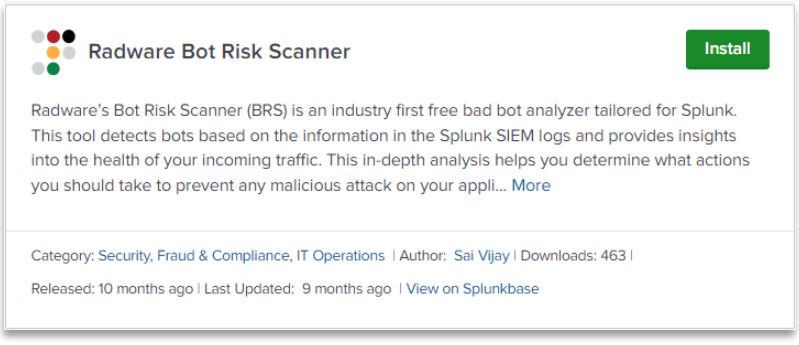
INTEGRATION GUIDELINES

To Enable Bot Risk Scanner, follow these 3 simple steps:

1. Download Bot Risk Scanner App from Splunk Marketplace



- Login to your Splunk Enterprise/Splunk Cloud account and navigate to the launcher page.
- Click on "**Find More Apps**" to access the App marketplace page.

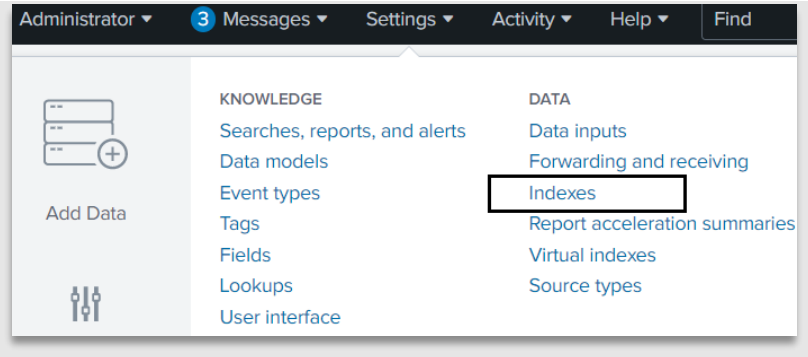


- In the App Marketplace page search for "**Radware Bot Risk Scanner**" and install through the link provided.
- Post-installation, navigate to your apps and open the "**Radware Bot Risk Scanner**"

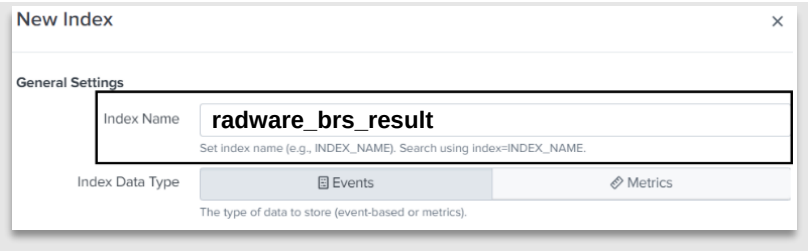
Note: *To use the Bot Risk Scanner, you need a Splunk Enterprise or Splunk Cloud account. If you encounter any errors, please refer to the FAQ section for troubleshooting information.*

2. Result Index Creation

Once the Radware Bot Risk Scanner is installed, and before configuring it, you need to create a result index in Splunk Enterprise/Cloud to store all the information processed by the Bot Risk Scanner End Point. Follow the steps below to create a new index.

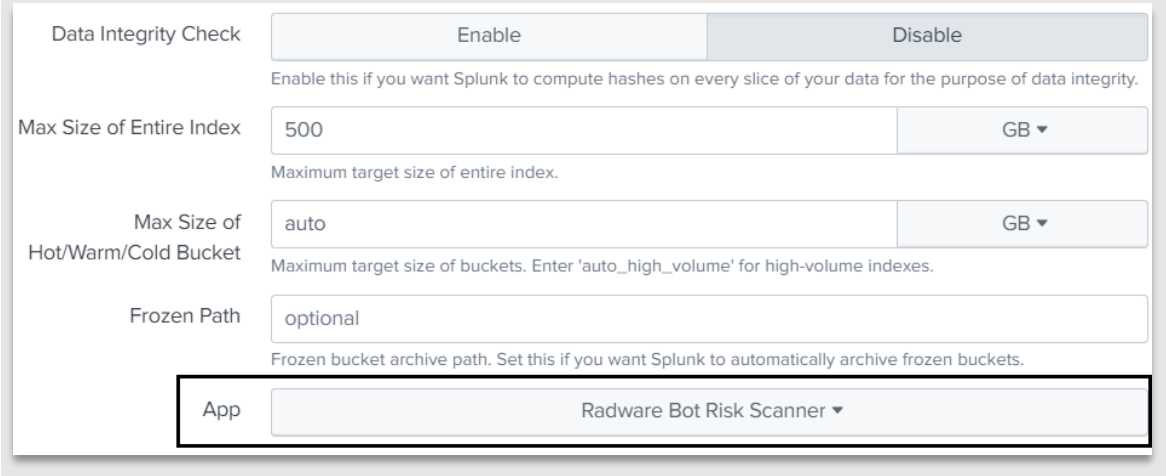


- In the Splunk UI, navigate to **Settings > Data > Indexes.**
- Click on "**New Index**" to store the information retrieved from Bot Risk Scanner Endpoint.



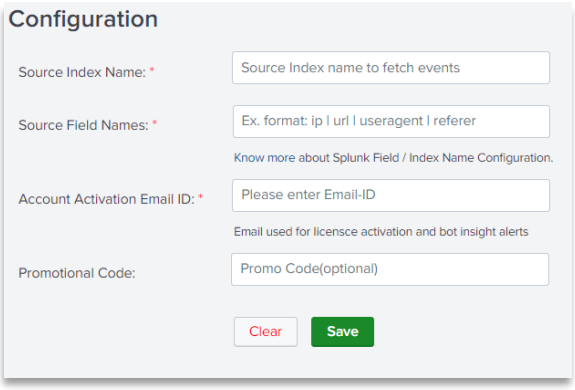
- Name the New Index as "**radware_brs_result**" and select the app name as "**Radware Bot Risk Scanner**".

Note: *Users of the Splunk Enterprise version, need to select the app as "**Radware Bot Risk Scanner**" while creating the result index. This is not required for Splunk Cloud version users.*



3. Bot Risk Scanner Configuration

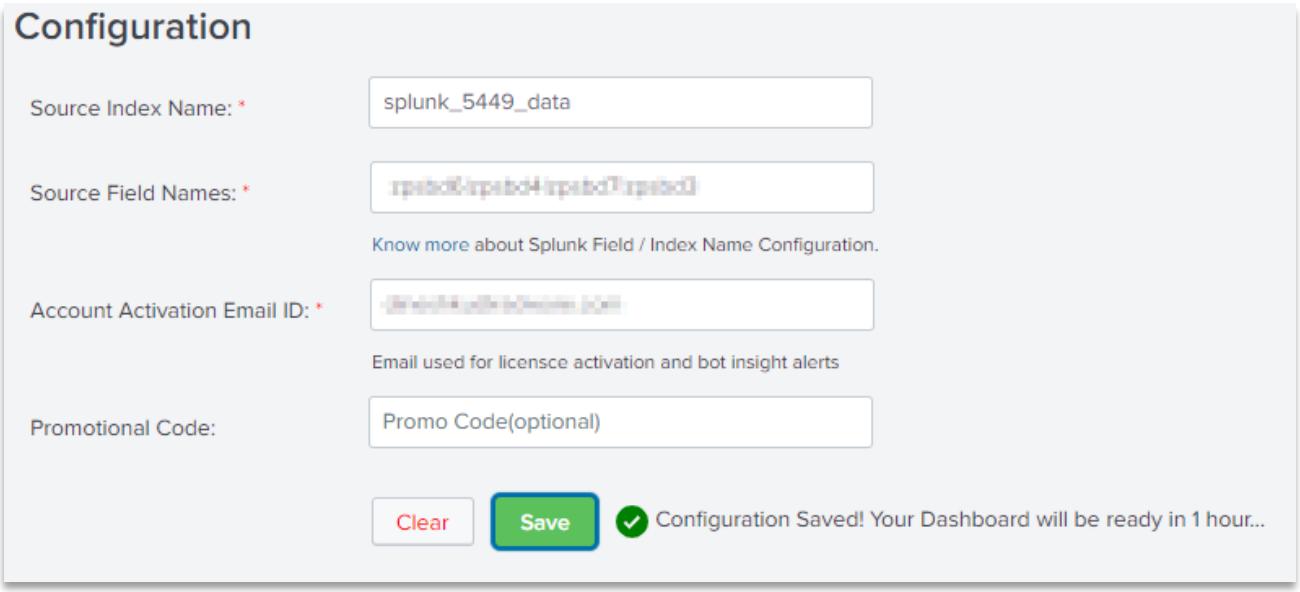
- Navigate to **Apps > Radware Bot Risk Scanner > Configuration**.



- **Source Index Name** - specify the Splunk index containing your application's access logs or web server logs for analysis.
- **Source Field Name** - Input Field from The Source Splunk Index [Field Format: IP | URL | user agent | referrer URL]
- **Email ID** - Email ID is required to activate the license.
- **Promotional Code** – This is an optional field, and if you require additional traffic to be processed/month, send your request to brs@radware.com and we will share unique promotional code to extend your limit.

Note: *The IP, URL and User Agent parameters are mandatory whereas the Referrer URL parameter is optional.*

Once configured, the saved search will run every hour, and the dashboard will be ready within an hour.



POST-INSTALL RECOMMENDATIONS

- To process more than 50K records, you need to replace the "**limits.conf**" file in the following path. You can download the "limits.conf" file from the following link.

  $SPLUNK_HOME/etc/apps/RadwareBotRiskScanner/local/limits.conf

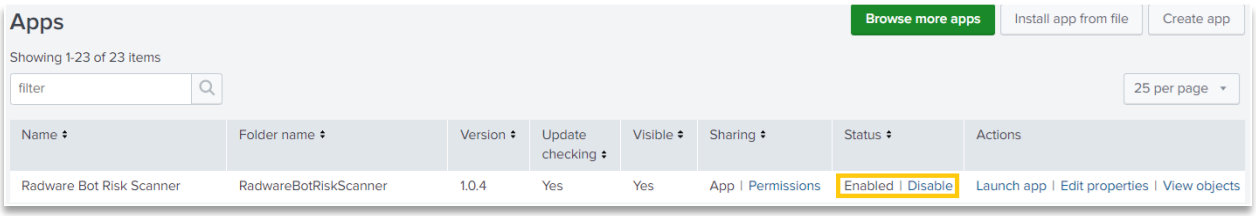
- Once Radware Bot Risk Scanner is installed, it is advised to force a refresh of Splunk Configurations.

  - For example, if your Splunk server is named Splunk and is running on port 8000, you would use the following URL: ***http://<splunk:8000>/en-US/debug/refresh***

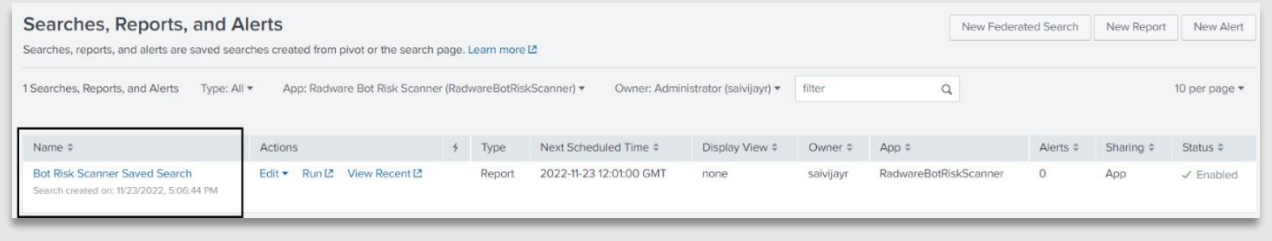
- Also, it is recommended to clear the cache before using Bot Risk Scanner.

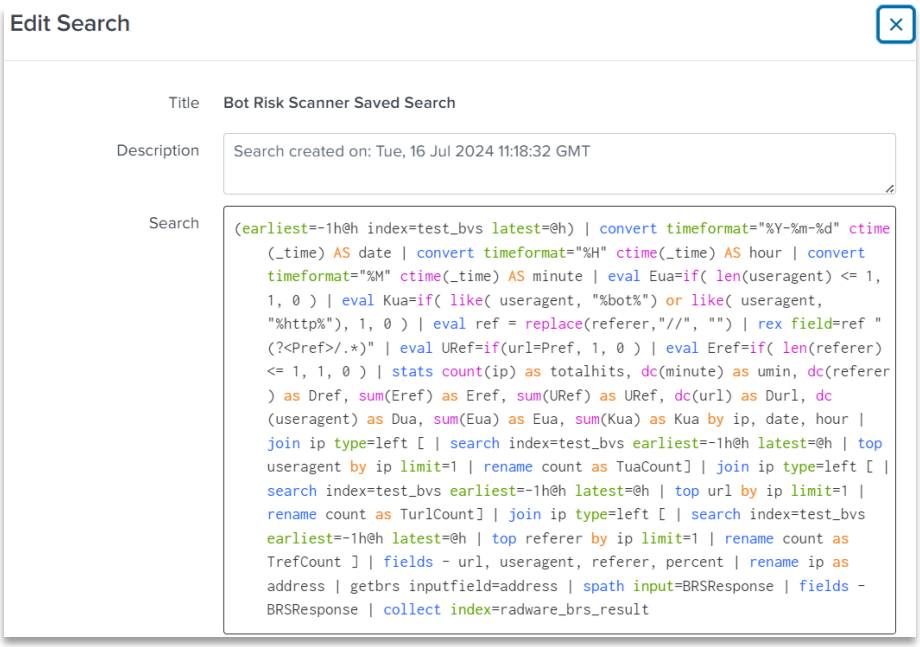
  - For example, if your Splunk server is named Splunk and is running on port 8000, you would use the following URL: ***http://<splunk:8000>/en-US/_bump***

- To check if the app is Enabled, navigate to **Apps> Manage Apps** and change the status to **enabled|disable.**



- To Validate if the saved search is created properly, Navigate to **Settings > Searches, Reports, and Alerts**. You should find "**Bot Risk Scanner Saved Search**".





↗ Navigate to **Action > Edit > Edit Search** to review the search query and validate if the below query is generated with your input field.

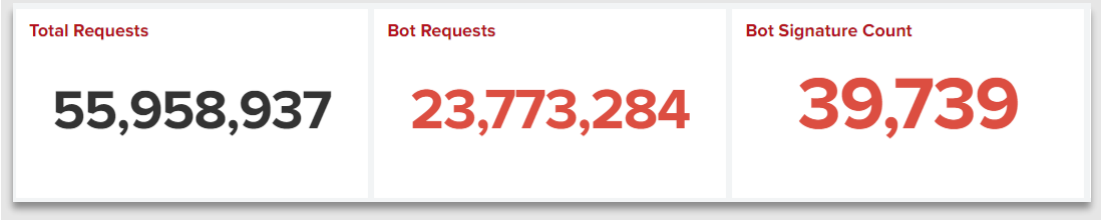
DASHBOARD & KPI DETAILS

The dashboard provides the following visualizations and key KPI Trackers:

Total Request: Total traffic in the Source Index scanned by Radware Bot Risk Scanner

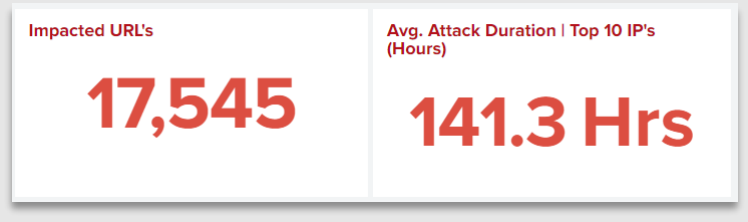
Bot Requests: Total traffic classified as bots (Includes Crawler and Aggregator) by Radware Bot Risk Scanner.

Bot Signature Count: Total number of unique signatures created against bots (Includes Crawler and Aggregator) by Radware Bot Risk Scanner.

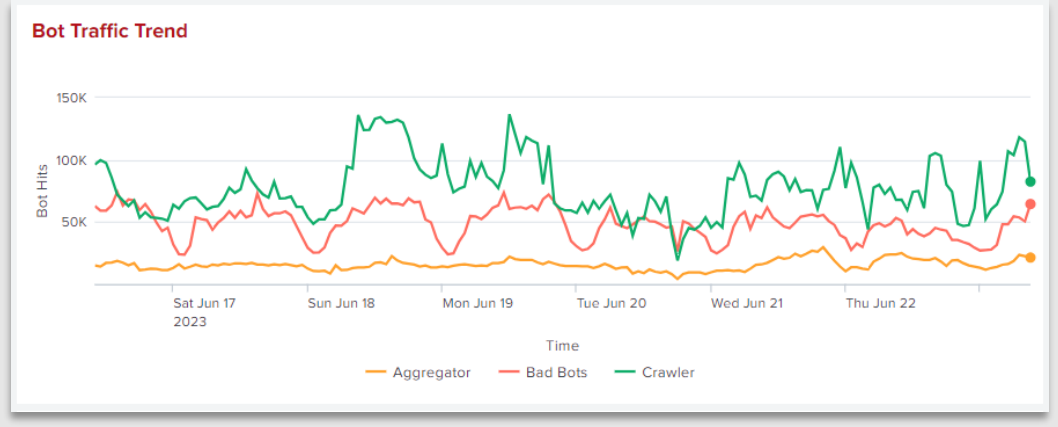


Impacted URL's: Total number of URL's being impacted by Bot Attacks

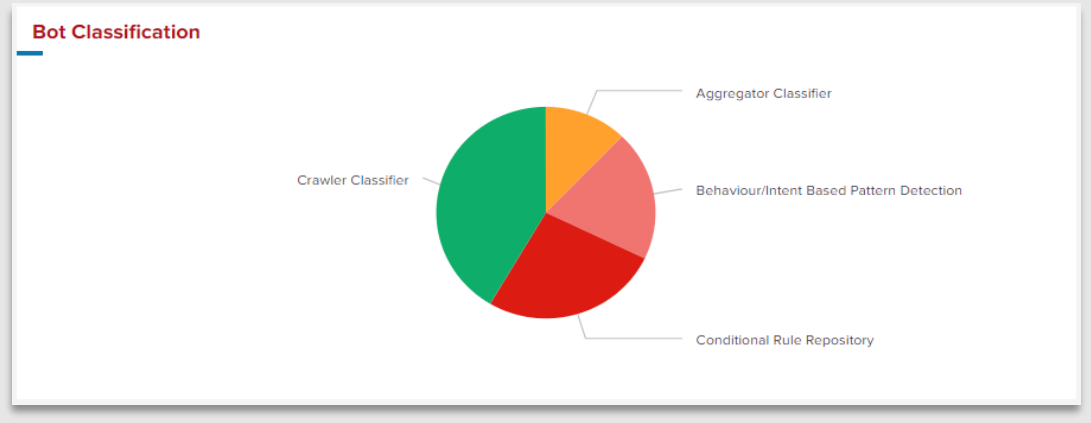
Avg. Attack Duration | Top 10 IP's: Average time spent by top 10 IP Address while performing Bot attacks.



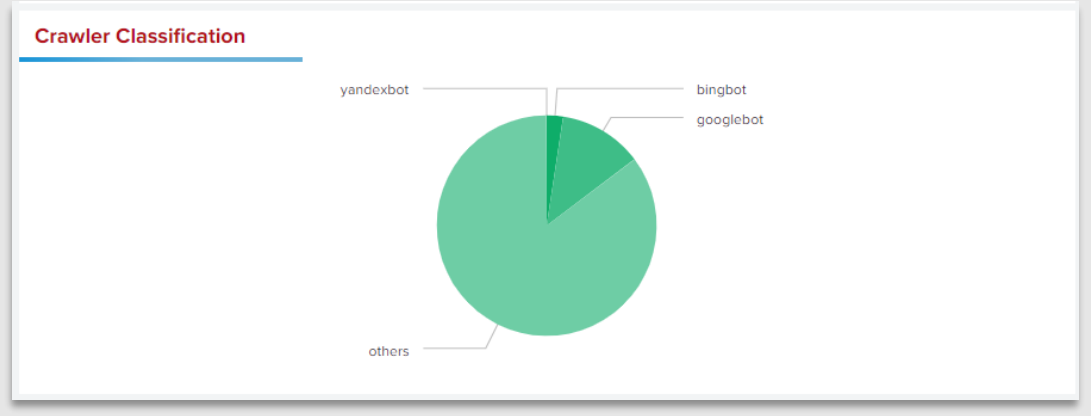
Bot Traffic Trend: Bot traffic trend per hour classified by Radware Bot Risk Scanner.



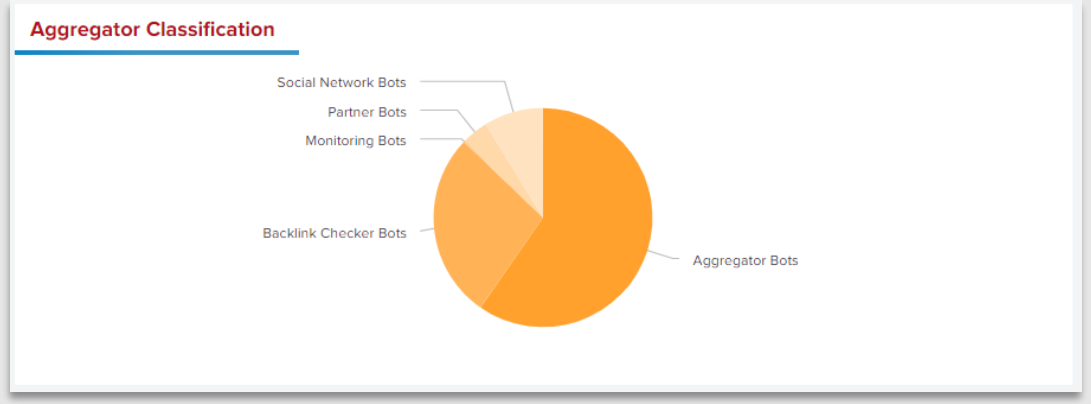
Bot Classification: Types of bots classified by Radware Bot Risk Scanner.



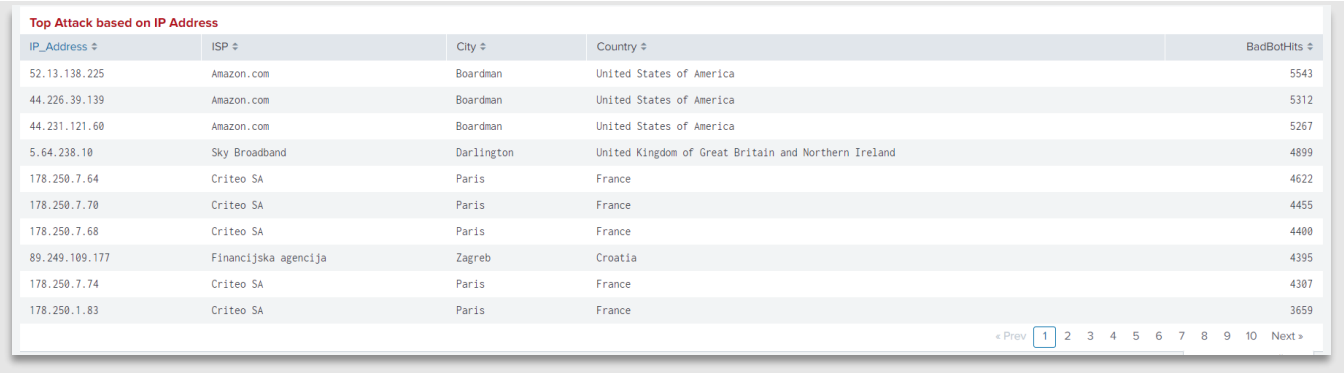
Crawler Stats: Total traffic classified as Crawlers by Radware Bot Risk Scanner.



Aggregator Stats: Total traffic classified as Aggregators by Radware Bot Risk Scanner.



Top Attack based on IP Address: List of IP's classified as bad by Radware Bot Risk Scanner along with ISP, City, Country, and Total hits made by individual IP within the selected period.

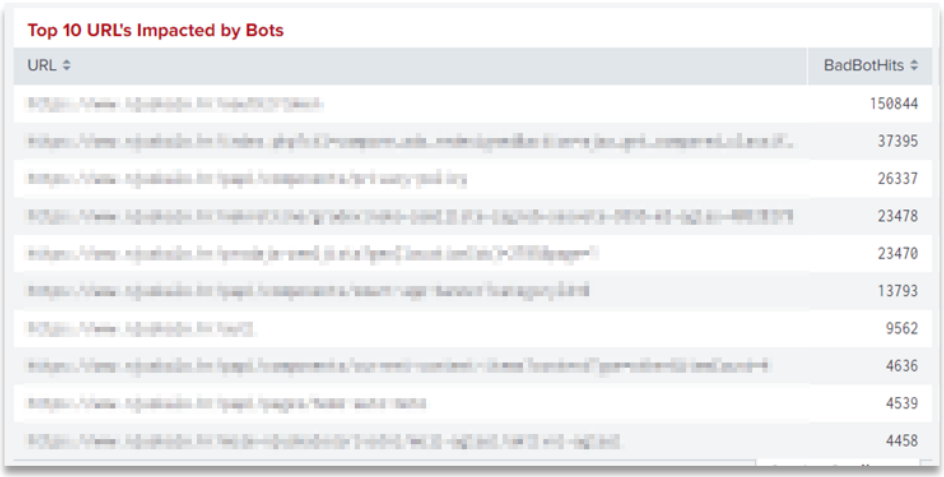


Top Attack based on IP Address

IP_Address	ISP	City	Country	BadBotHits
52.13.138.225	Amazon.com	Boardman	United States of America	5543
44.226.39.139	Amazon.com	Boardman	United States of America	5312
44.231.121.60	Amazon.com	Boardman	United States of America	5267
5.64.238.10	Sky Broadband	Darlington	United Kingdom of Great Britain and Northern Ireland	4899
178.250.7.64	Criteo SA	Paris	France	4622
178.250.7.70	Criteo SA	Paris	France	4455
178.250.7.68	Criteo SA	Paris	France	4400
89.249.109.177	Financijska agencija	Zagreb	Croatia	4395
178.250.7.74	Criteo SA	Paris	France	4307
178.250.1.83	Criteo SA	Paris	France	3659

« Prev 1 2 3 4 5 6 7 8 9 10 Next »

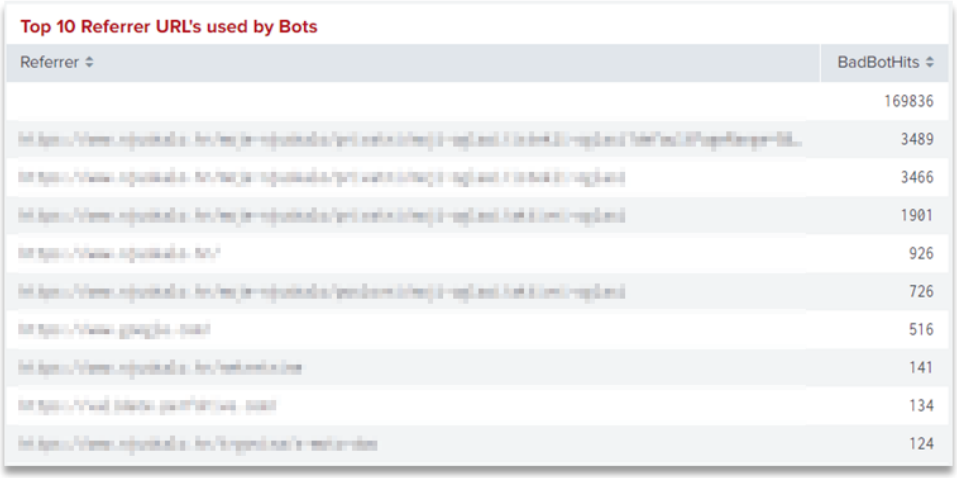
Top 10 URL's Impacted by Bots: List of the top 10 URL's and the number of bad bot hits on each URL within the selected period.



Top 10 URL's Impacted by Bots

URL	BadBotHits
[redacted]	150844
[redacted]	37395
[redacted]	26337
[redacted]	23478
[redacted]	23470
[redacted]	13793
[redacted]	9562
[redacted]	4636
[redacted]	4539
[redacted]	4458

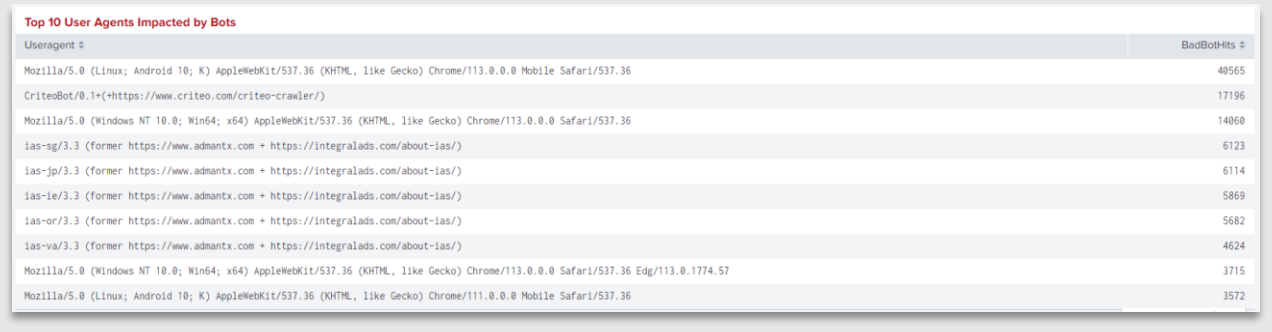
Top 10 Referrer URL's Impacted by Bots: List of top 10 Referrer URL and the number of bad bot hits on each URL within the selected period.



Top 10 Referrer URL's used by Bots

Referrer	BadBotHits
	169836
[redacted]	3489
[redacted]	3466
[redacted]	1901
[redacted]	926
[redacted]	726
[redacted]	516
[redacted]	141
[redacted]	134
[redacted]	124

Top 10 User Agents Bots:



Top 10 User Agents Impacted by Bots

Useragent	BadBotHits
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Mobile Safari/537.36	40565
CriteoBot/0.1+(+https://www.criteo.com/criteo-crawler/)	17196
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36	14060
ias-sg/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	6123
ias-jp/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	6114
ias-ie/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	5869
ias-or/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	5682
ias-va/3.3 (former https://www.admantx.com + https://integralads.com/about-ias/)	4624
Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36 Edg/113.0.1774.57	3715
Mozilla/5.0 (Linux; Android 10; K) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/111.0.0.0 Mobile Safari/537.36	3572

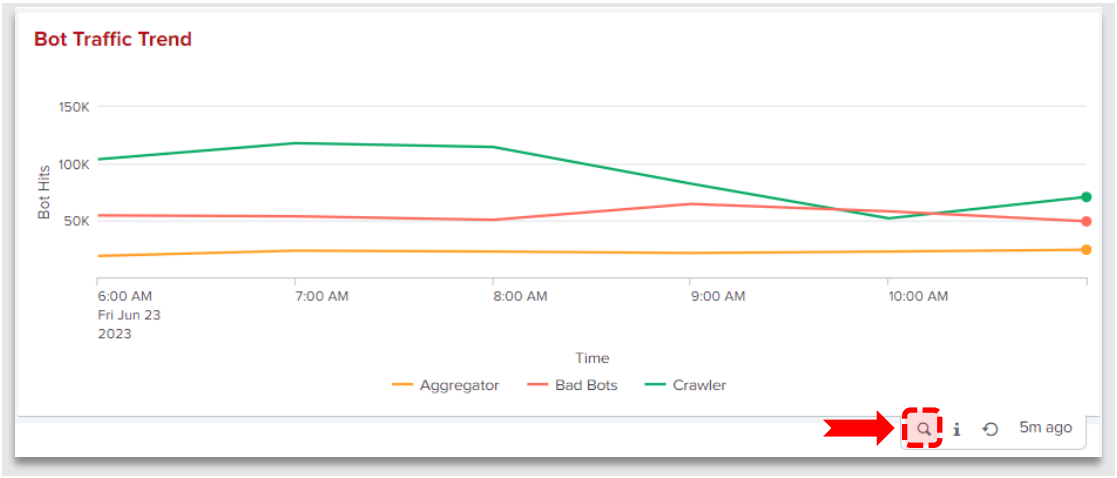
Global Distribution & Top 10 City Based on Attack:

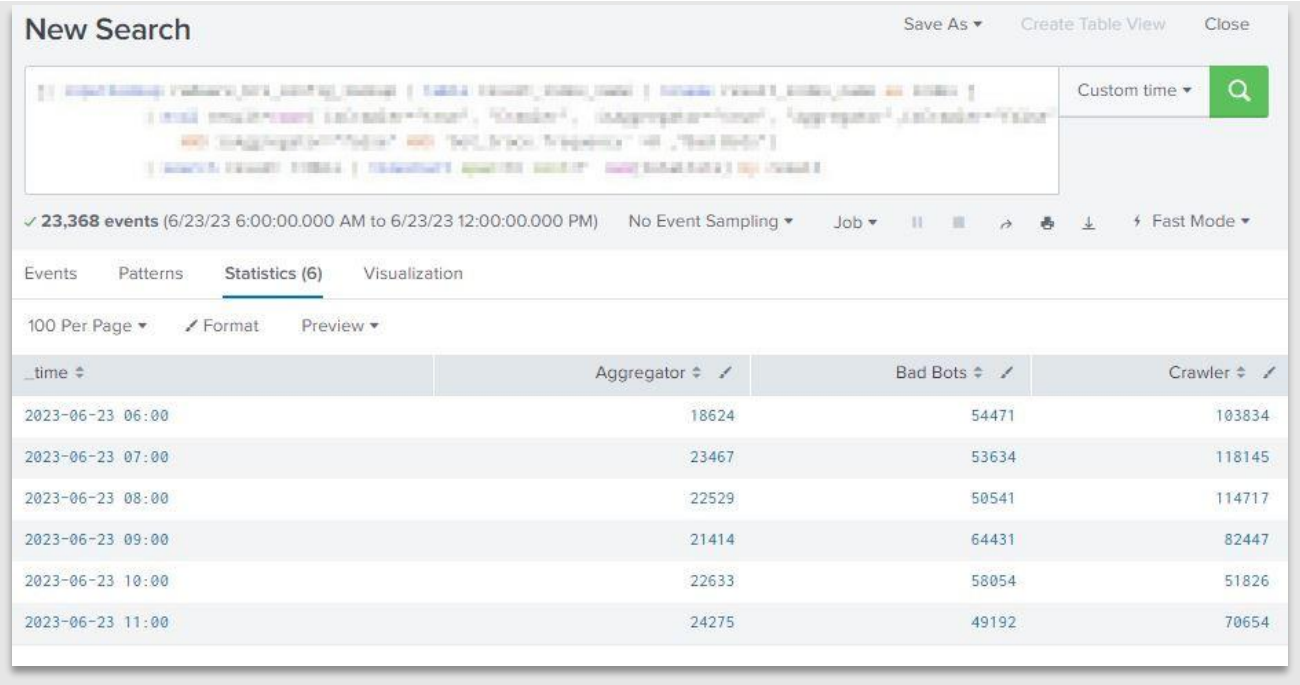
Global Distribution

Top 10 City based on Attack

City	Country	BadBotHits
Mountain View	United States of America	2242052
Boydton	United States of America	540345
Ashburn	United States of America	361679
Zagreb	Croatia	351679
Strasbourg	France	325463
Paris	France	222281
Roubaix	France	200027
St Louis	United States of America	109859
Redmond	United States of America	77202
Split	Croatia	75926

Note: *Exporting data from panels is disabled in the dashboard. To export data from a particular panel, hover over the bottom right corner of the panel and click on "Open in Search." The result will open in a new window without any additional query execution cost. A sample is shown below.*





_time	Aggregator	Bad Bots	Crawler
2023-06-23 06:00	18624	54471	103834
2023-06-23 07:00	23467	53634	118145
2023-06-23 08:00	22529	50541	114717
2023-06-23 09:00	21414	64431	82447
2023-06-23 10:00	22633	58054	51826
2023-06-23 11:00	24275	49192	70654

©2024 Radware Ltd. All rights reserved. The Radware products and solutions mentioned in this document are protected by trademarks, patents and pending patent applications of Radware in the U.S. and other countries. For more details please see: https://www.radware.com/LegalNotice/. All other trademarks and names are property of their respective owners.