Radware’s Bot Risk Scanner [BRS] –

What is Bot Risk Scanner?

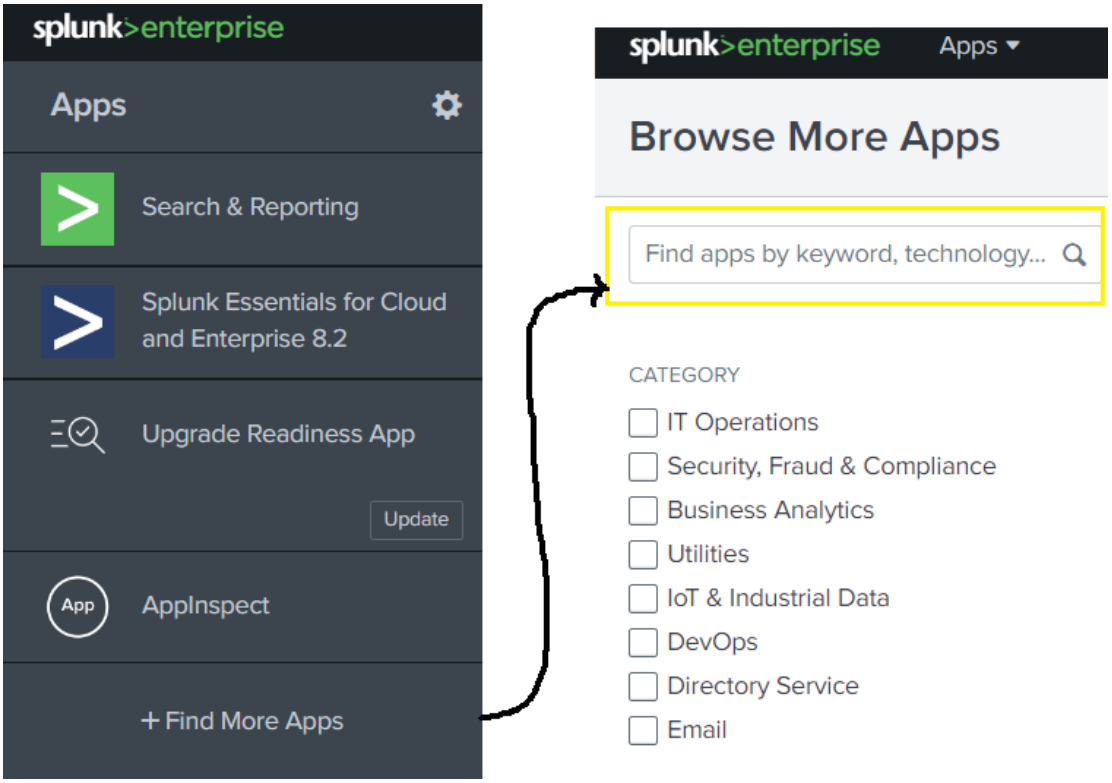
Radware's Bot Risk Scanner (BRS) provides detailed insights into your bad bot traffic without additional integration with your website or application. You can easily enable BRS through the GUI by installing the BRS plugin from the Splunk Marketplace (Link). This plugin offers a detailed dashboard with insights into your application's traffic and the types of bots attempting to access your system. This document outlines the installation process for the Bot Risk Scanner through the Splunk Marketplace.

Integration Guidelines:

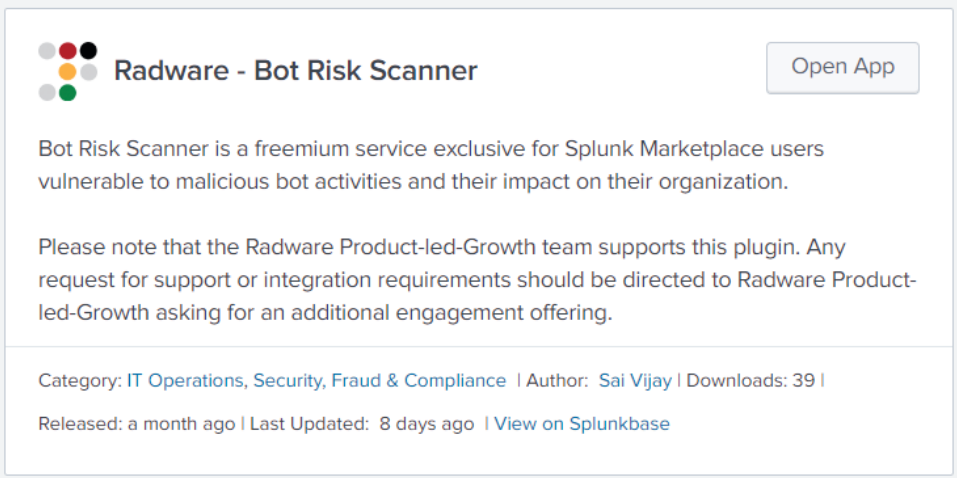
To get started with the BRS, follow these steps:

1. **Select the Radware Bot Risk Scanner App on the Splunk Marketplace:**

Login to your Splunk Enterprise 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 it in your Splunk environment. Post the installation navigate to your apps and open Radware – Bot Risk Scanner.



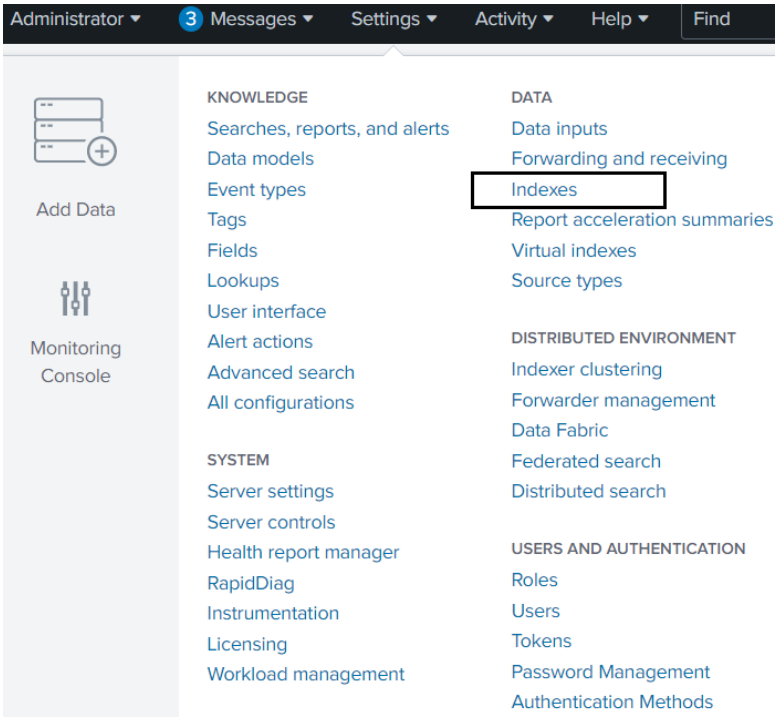
A. Save Configuration Details:

To use the Bot Risk Scanner, you need a Splunk Enterprise or Splunk Cloud account. Once you open the application, go to Settings → ‘Indexes’ section to create a new index. After the index is created, go to the configuration page to set up BRS. After installation, the user will need to fill details in the configuration page.
If you encounter any errors, please refer to the FAQ section for troubleshooting information.

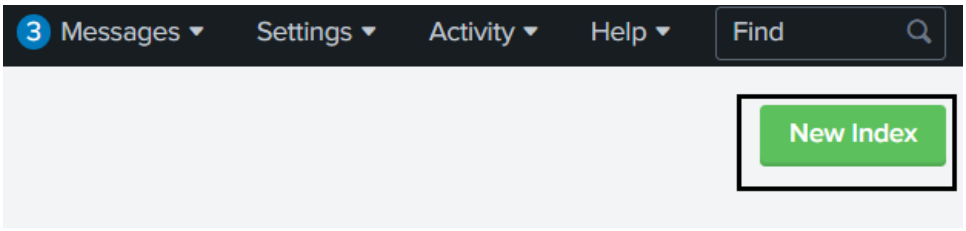
Pre-requisites for installing Bot Risk Scanner:

Result Index Creation: An index needs to be created to save all information retrieved from Radware Bot Risk Scanner End Point. Find the steps below to create a new index.

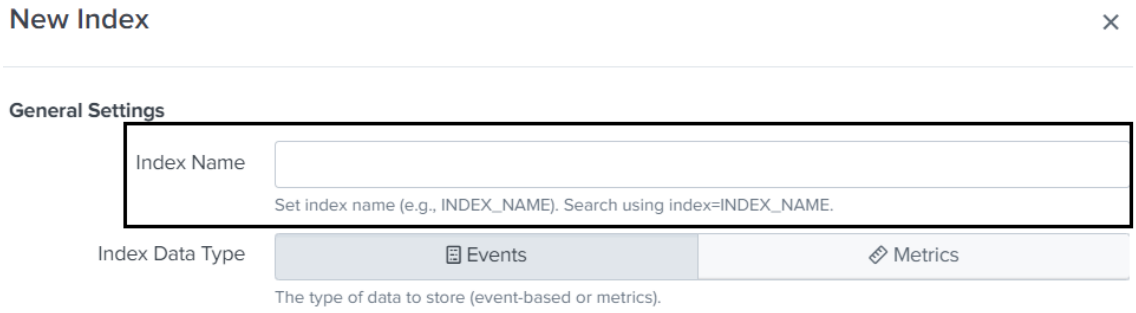
➔ 1. Navigate to Settings > Data > Indexes as illustrated below:



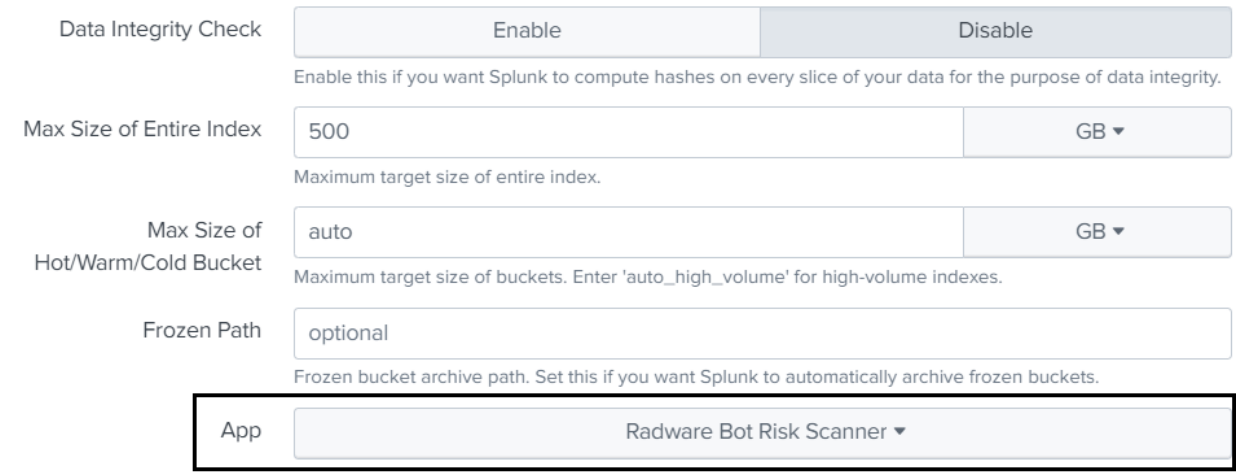
2. Click on “New Index” to create an index to store the information retrieved from BRS Endpoint.



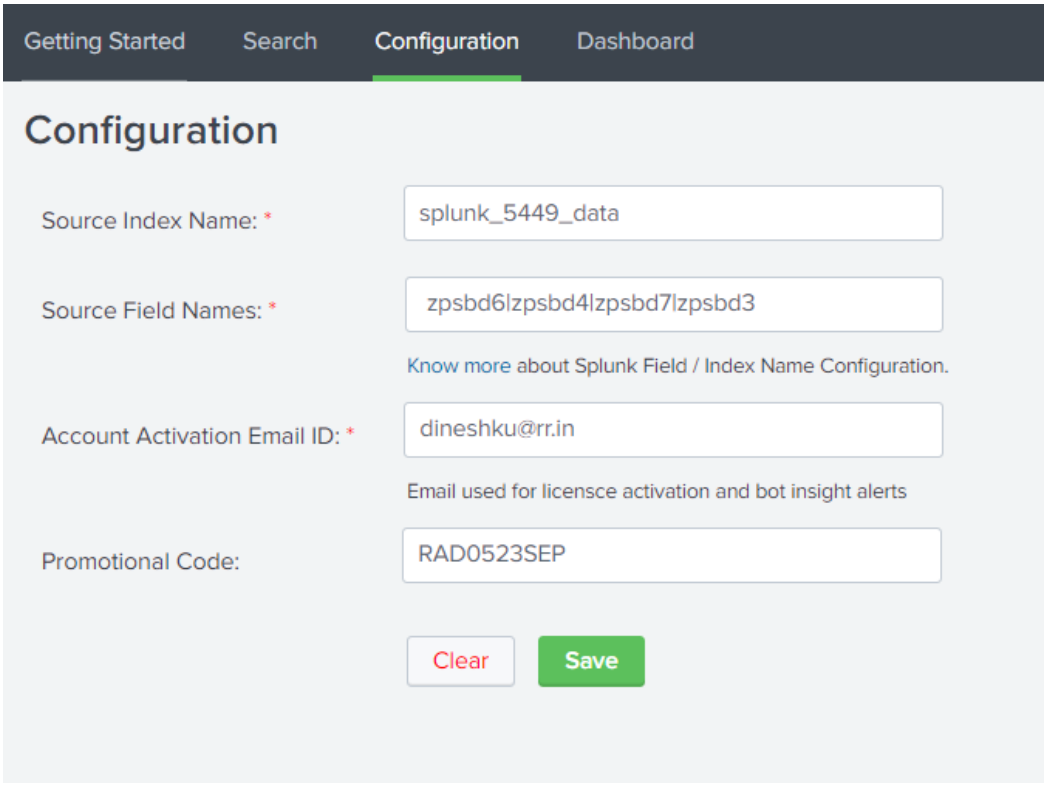
3. Keep the index name as **“radware_brs_result”** and select the app name as “Radware Bot Risk Scanner”. Please note that the Index name must be set exactly as mentioned above.



➔ 4. Ensure that App selected is mentioned as ‘Radware BRS’.



Radware BRS Configuration:



Splunk Index Name - Index Name That Points to The Data in Splunk for Analysis

Splunk Field Name – Input Field from The Source Splunk Index [Field Format: ip | url | useragent | referrer]

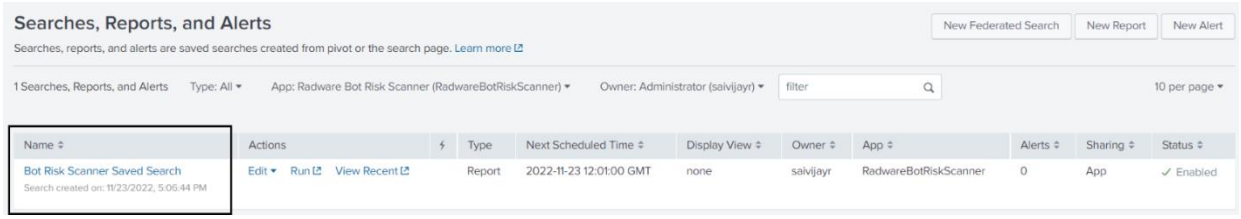
Note- IP, URL, User Agent are required parameters whereas referrer is optional

Email ID – Email ID is required to activate the license.

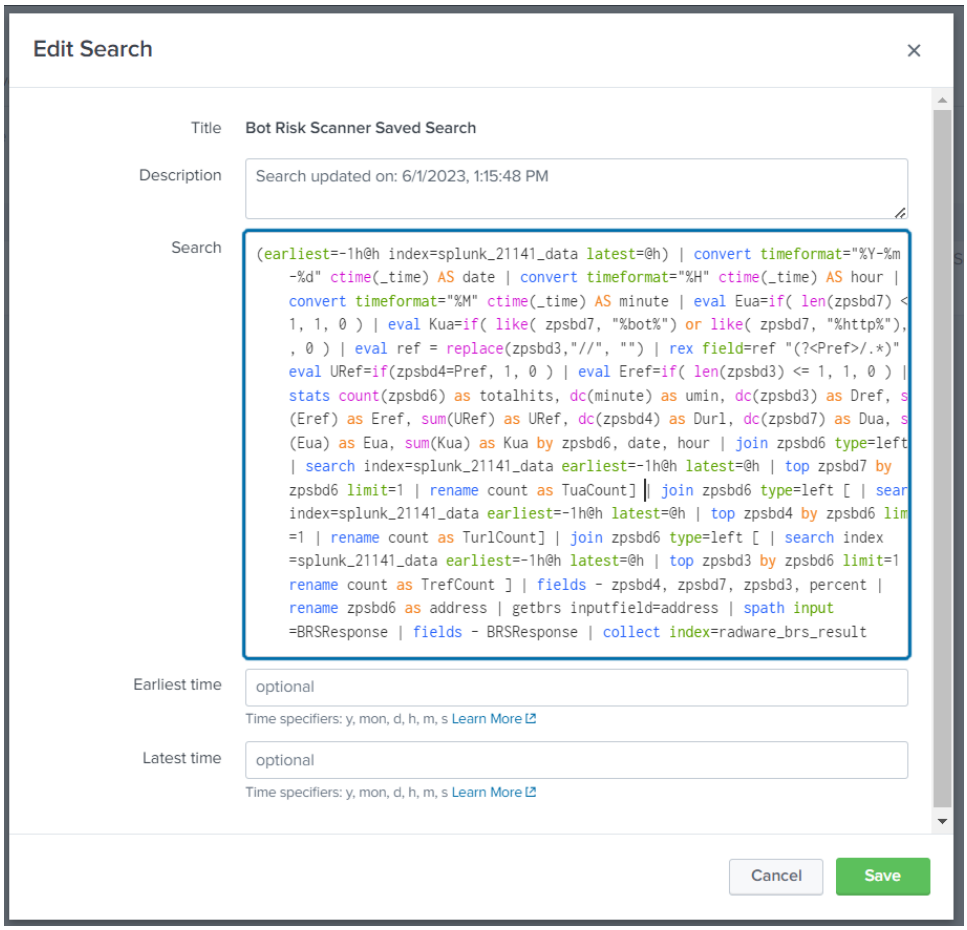
Promotional Code – This is an optional field, and if you feel you need more quotas, please send us an email to brs@radware.com and the Radware team will share the unique promotional code for your account.

B. Verify Saved Search

1. Navigate to ***Settings > Searches, reports, and alerts***. You will find a saved search created for review/as a sample.



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



Index	Description
collect index=radware_brs_result	Result data will be fetched from the source and will be stored in index='radware_brs_result' which will be used to create the visualization

Note- Modify / create the stanza in the following path to process data (more than 50k):

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

You can download the limits.conf file from following link .

3. Navigate to "**Dashboard**" tab to analyze your data.

Recommended Steps after installing Bot Risk Scanner

➔ Once Radware Bot Rist Scanner is installed it is advised to force a refresh of Splunk Configurations.

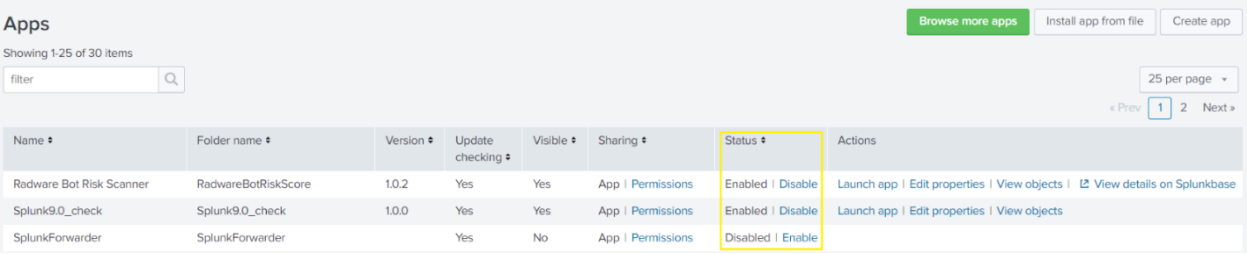
- For example, if your Splunk server is named Splunk and is running on port 8000, you would use the following URL: **http://splunk:8000/en-US/debug/refresh**

➔ Also, it is recommended to clear the cache before using Bot Rist 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**

➔ C. Disable Radware Bot Risk Scanner

➔ Navigate to ***Apps> Manage Apps>*** and change the status to enable/disable



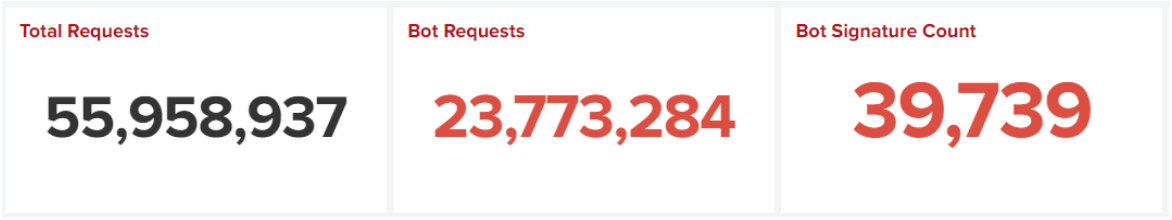
Dashboard & Visualizations

The dashboard provides the following visualizations and information:

Total Request: Total number of packets in the Source Index scanned by Radware Bot Risk Scanner

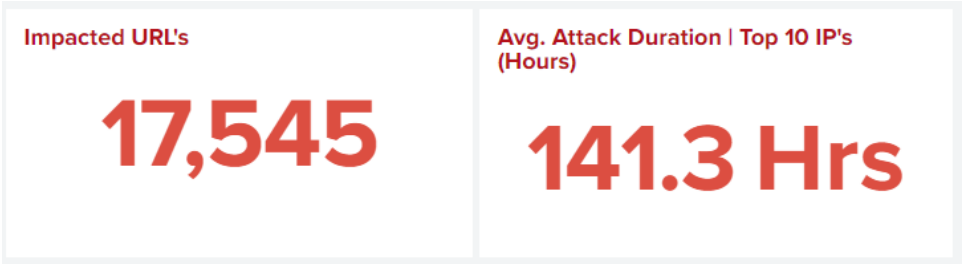
Bot Requests: Total number of packets classified as bots (Includes Crawler and Aggregator) by Radware Bot Risk Scanner.

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

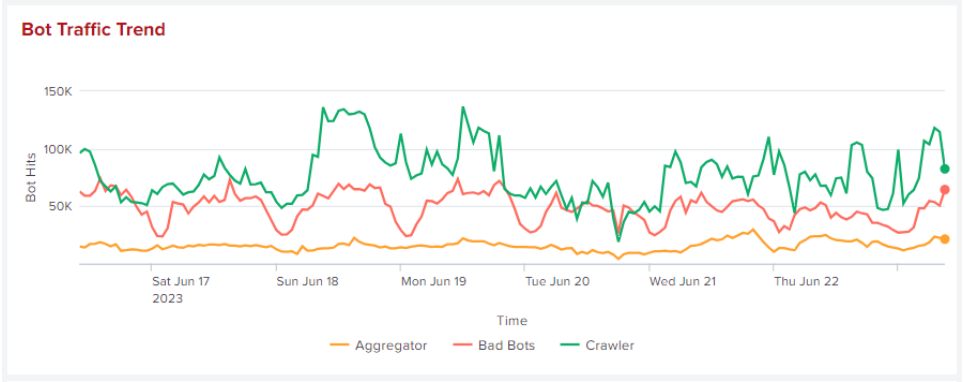


Impacted URL's: Total number of URL's being impacted by Bot Attacks

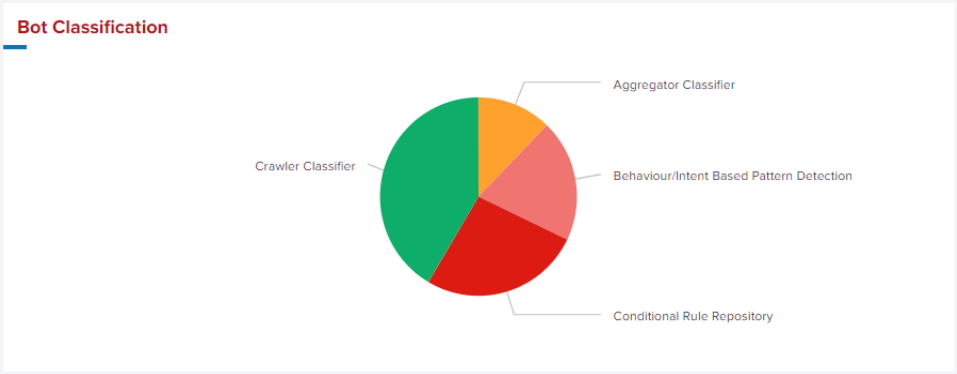
Avg. Attack Duration | Top 10 IP's: Average time spent by top 10 IP Address while performing Bot attacks.



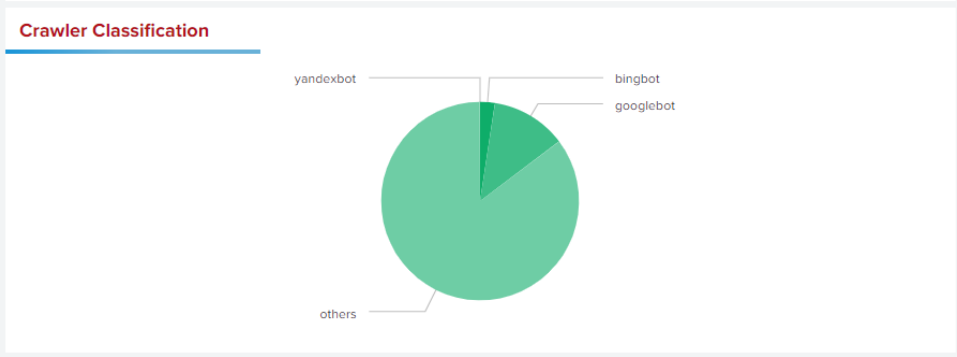
Bot Traffic Trend: Bot traffic trend per hour classified by Radware Bot Risk Scanner.



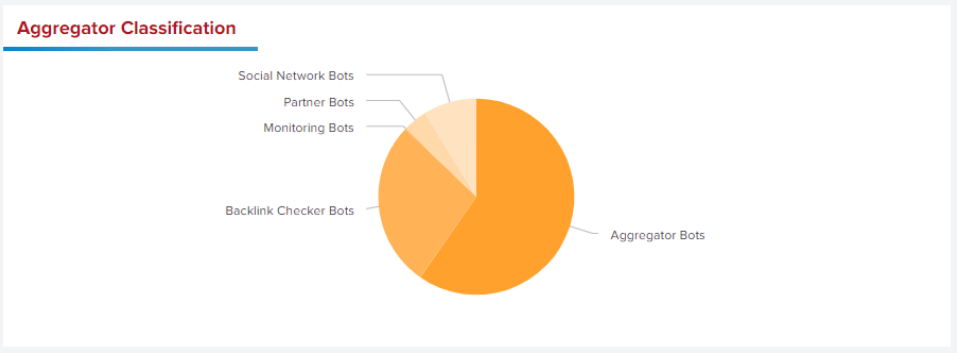
Bot Classification: Types of bots classified by Radware Bot Risk Scanner.



Crawler Stats: Total number of packets classified as Crawlers by Radware Bot Risk Scanner.



Aggregator Stats: Total number of packets 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
https://www.njuskalo.hr/oauth2/token	150844
https://www.njuskalo.hr/index.php?ctl=compare_ads_redesigned&action=ajax_get_compared_classif…	37395
https://www.njuskalo.hr/papi/components/privacy-policy	26337
https://www.njuskalo.hr/nekretnine/gradevinsko-zemljiste-zagreb-sesvete-9595-m2-oglas-40528279	23478
https://www.njuskalo.hr/prodaja-zemljista?geo[locationIds]=2785&page=1	23470
https://www.njuskalo.hr/papi/components/smart-app-banner?categoryId=0	13793
https://www.njuskalo.hr/auti	9562
https://www.njuskalo.hr/papi/components/current-content-items?contentType=other&itemCount=4	4636
https://www.njuskalo.hr/papi/pages/home-auto-moto	4539
https://www.njuskalo.hr/moje-njuskalo/privatni/moji-oglasi/aktivni-oglasi	4458

Top 10 Referrer URL's Impacted by Bots: List of top 10 referrers 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
https://www.njuskalo.hr/moje-njuskalo/privatni/moji-oglasi/istekli-oglasi?defaultPageRange=5&…	3489
https://www.njuskalo.hr/moje-njuskalo/privatni/moji-oglasi/istekli-oglasi	3466
https://www.njuskalo.hr/moje-njuskalo/privatni/moji-oglasi/aktivni-oglasi	1901
https://www.njuskalo.hr/	926
https://www.njuskalo.hr/moje-njuskalo/poslovni/moji-oglasi/aktivni-oglasi	726
https://www.google.com/	516
https://www.njuskalo.hr/nekretnine	141
https://validate.perfdrive.com/	134
https://www.njuskalo.hr/trgovina/s-moto-doo	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:

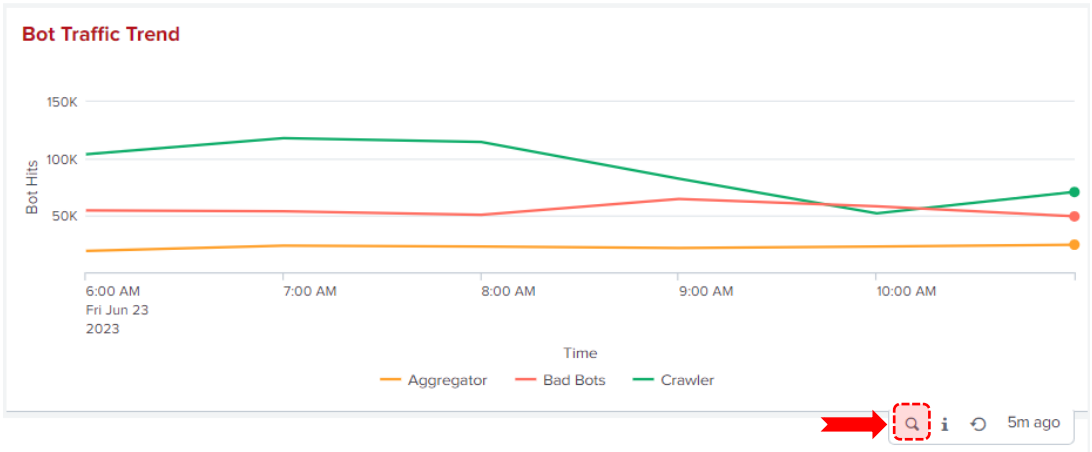
Global Distribution

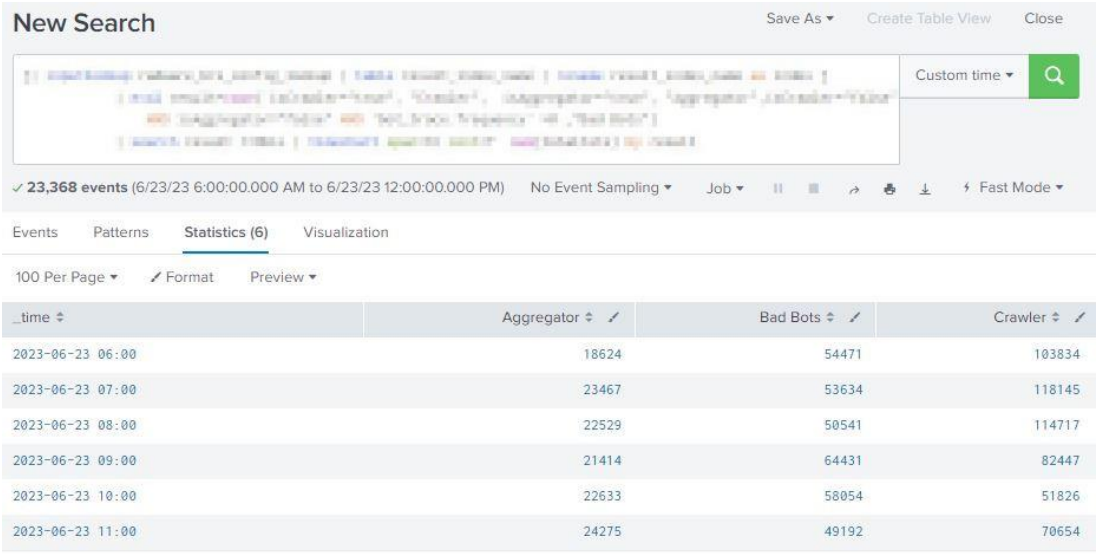
Top 10 City based on Attack

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