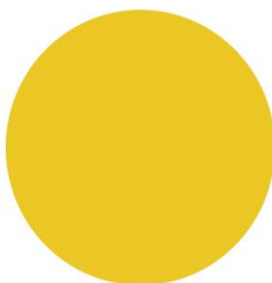




SPLUNK APP FOR BLUELIV USER GUIDE



Public Documentation

AUTHOR: Blueliv

TLP: **Green**

© 2017 Leap In Value S.L. All rights reserved.

The information provided in this document is the property of Blueliv, and any modification or use of all or part of the content of this document without the express written consent of Blueliv is strictly prohibited. Failure to reply to a request for consent shall in no case be understood as tacit authorization for the use thereof.

Blueliv® is a registered trademark of Leap In Value S.L. in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

Contents

- 1. Introduction..... 4
- 2. Setup 4
 - 2.1. Requirements 4
 - 2.2. Installation 4
 - 2.3. Configuration..... 6
- 3. Getting started 7
 - 3.1. Home 7
 - 3.2. Threat Overview..... 7
 - 3.3. Search..... 10
 - 3.4. Bot Ips..... 10
 - 3.5. Attack IPs..... 13
 - 3.6. Malware 15
 - 3.7. Hacktivism..... 17
- 4. Registration 18

1. Introduction

Splunk App for Blueliv automatically integrates Blueliv's Cyber Threat Intelligence into Splunk.

This will add Cyber Threat Intelligence to your existing data, addressing a comprehensive range of cyber threats including compromised URLs, domains, IPs, etc. to turn global threat data into predictive, actionable intelligence specifically for your enterprise and the unique threats it faces.

Our powerful networks, of specialized search engines, scour the web for up-to-the-minute data and delivers real-time actionable information.

Unsurpassed cyber threat intelligence, now at your disposal.

2. Setup

2.1. Requirements

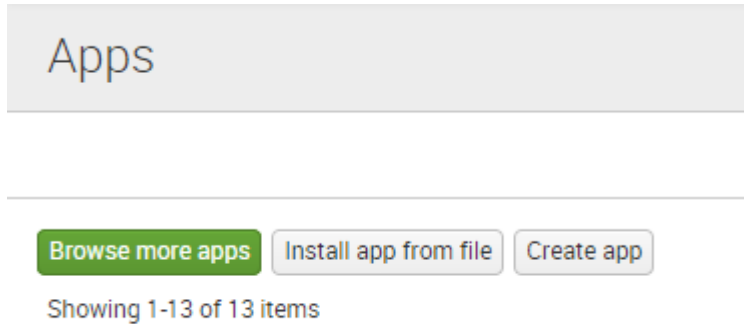
This app has been tested on a 6.2 version of Splunk® installed on a 64 bits Windows 7 Professional and a Debian 7.

This app is fully functional in Splunk 6.2 because it uses the latest feature KV Store collections only available in this version.

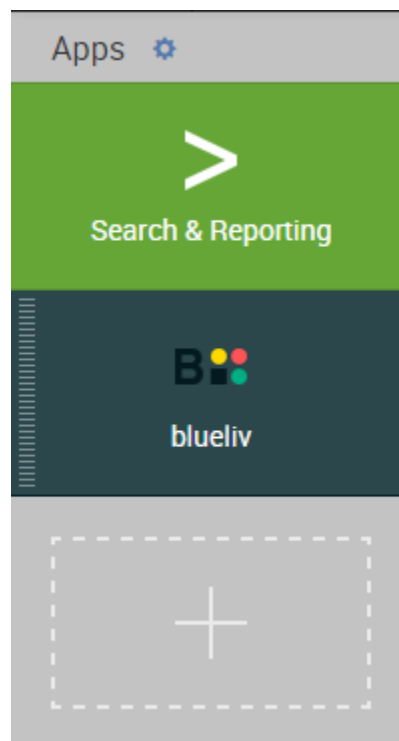
2.2. Installation

1. Download Splunk App for Blueliv. [Link?](#)

2. Open the manage Apps from your Splunk web App and click “install app from file”.



3. Upload the file downloaded on the first step.
4. Restart your Splunk and Splunk App for Blueliv. It should be available from the Splunk's main dashboard as shown below.



Note that the free installation of the Splunk App for Blueliv provides a small sample of our Threat Intelligence feed to get used to the plugin before going further.

2.3. Configuration

Firstly, you should configure an api-key and proxy settings -if needed. Inside the app, open the 'Configuration' tab. From there, set your api-key under the section API-Key, and specify the access type (COMMERCIAL/FREE). Once done, click on save and you should be able to download blueliv's crimeservers feed.

The screenshot displays the configuration interface for Blueliv, organized into three distinct sections:

- Blueliv API feed settings:** This section contains an 'API-Key' text input field with the value 'apikey', an 'Access type' dropdown menu currently set to 'COMMERCIAL', and a green 'Save' button.
- Threat Overview feed settings:** This section includes a text box stating 'This will force the download of all current ONLINE CrimeServers in the next update.' and a red 'Restart feed' button.
- Configure Proxy settings if needed:** This section features four text input fields for 'Proxy host (blank if not needed)', 'Proxy port (blank if not needed)', 'Proxy user (blank if not needed)', and 'Proxy password (blank if not needed)', followed by a green 'Save' button.

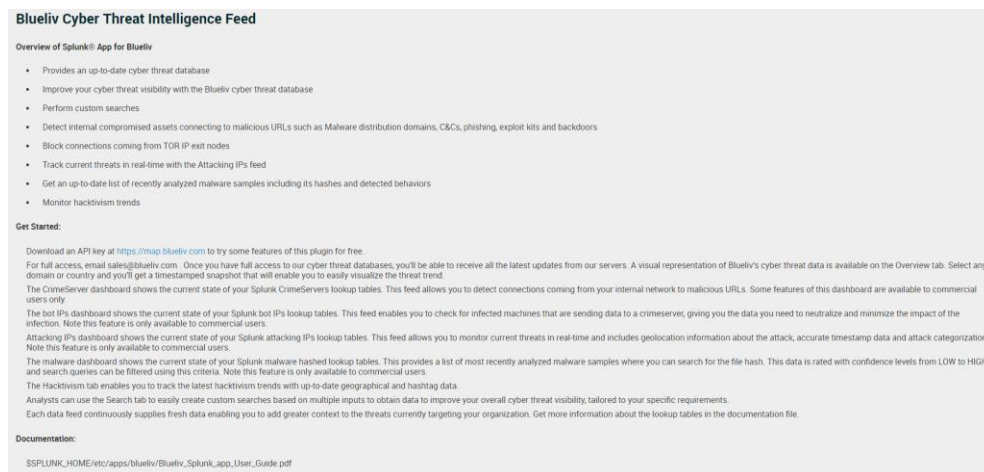
Threat Overview feed settings, allows to force the download of the whole dataset for crimeservers in the next update, otherwise it will keep receiving the normal chunked updates.

Proxy settings are optional and should only be set if a proxy is needed to access the internet. You can leave any input blank if you do not need it.

3. Getting started

3.1. Home

Once inside the Splunk App for Blueliv, the main page (Home) provides you an introduction and the steps to get full access to the Blueliv's Threat Intelligence Feed.



Blueliv Cyber Threat Intelligence Feed

Overview of Splunk® App for Blueliv

- Provides an up-to-date cyber threat database
- Improve your cyber threat visibility with the Blueliv cyber threat database
- Perform custom searches
- Detect internal compromised assets connecting to malicious URLs such as Malware distribution domains, C&Cs, phishing, exploit kits and backdoors
- Block connections coming from TOR IP exit nodes
- Track current threats in real-time with the Attacking IPs feed
- Get an up-to-date list of recently analyzed malware samples including its hashes and detected behaviors
- Monitor hacktivism trends

Get Started:

Download an API key at <https://map.blueliv.com> to try some features of this plugin for free.

For full access, email sales@blueliv.com. Once you have full access to our cyber threat databases, you'll be able to receive all the latest updates from our servers. A visual representation of Blueliv's cyber threat data is available on the Overview tab. Select any domain or country and you'll get a timestamped snapshot that will enable you to easily visualize the threat trend.

The CrimeServer dashboard shows the current state of your Splunk CrimeServers lookup tables. This feed allows you to detect connections coming from your internal network to malicious URLs. Some features of this dashboard are available to commercial users only.

The bot IPs dashboard shows the current state of your Splunk bot IPs lookup tables. This feed enables you to check for infected machines that are sending data to a crimserver, giving you the data you need to neutralize and minimize the impact of the infection. Note this feature is only available to commercial users.

Attacking IPs dashboard shows the current state of your Splunk attacking IPs lookup tables. This feed allows you to monitor current threats in real-time and includes geolocation information about the attack, accurate timestamp data and attack categorization. Note this feature is only available to commercial users.

The malware dashboard shows the current state of your Splunk malware hashed lookup tables. This provides a list of most recently analyzed malware samples where you can search for the file hash. This data is rated with confidence levels from LOW to HIGH and search queries can be filtered using this criteria. Note this feature is only available to commercial users.

The Hacktivism tab enables you to track the latest hacktivism trends with up-to-date geographical and hashtag data.

Analysts can use the Search tab to easily create custom searches based on multiple inputs to obtain data to improve your overall cyber threat visibility, tailored to your specific requirements.

Each data feed continuously supplies fresh data enabling you to add greater context to the threats currently targeting your organization. Get more information about the lookup tables in the documentation file.

Documentation:

`$SPLUNK_HOME/etc/apps/blueliv/Blueliv_Splunk_app_User_Guide.pdf`

3.2. Threat Overview

This dashboard shows you an overview based on the current data in the local Data Base. This provides geolocation information, the current top 10 affected ASN's and domains. The last trends in Cybercrime.

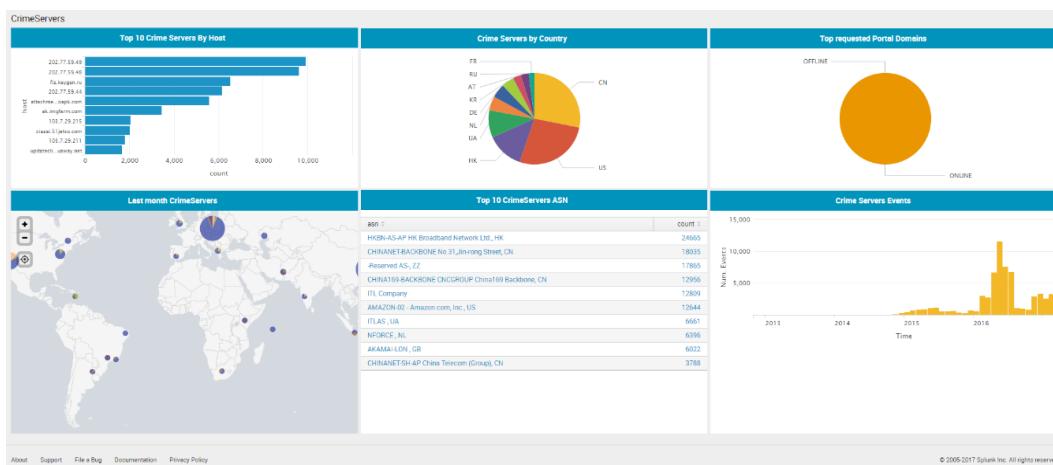
The Crime Server Events plot is linked to the results on "Crime Servers by domain" and "Crime Servers by country", so when you click on a result the events are listed over time to provide you the trending on the threat. For instance, in the figure below, China was selected to get events found in China over time, getting a deeper view on this threat in the Crime Servers Events chart.

Field Name	Description
url	Crimeserver's url
Domain	Crimeserver's domain
Host	Crimeserver's host
Type	Categorization of the crimeserver
Subtype	Sub-categorization of the crimeserver
Ip	Crimeserver's IP
Asn	Crimeserver's ASN
Lat	Crimeserver's IP latitude
Lon	Crimeserver's IP longitude
Status	Current crimeserver's activity (ONLINE/OFFLINE)
Country	Crimeserver's IP country
firstSeenAt	Date when the crimeserver was seen for the

	first time
lastSeenAt	Date when the crimeserver was seen for the last time

Check more detailed description about this feed at:

<https://apidocs.blueliv.com/#crimeservers10>



This feed is updated every 15 minutes and provide the next lookup tables to enrich your logs and help you to decide actions.

1. bl_ip_lookup: List of malicious IPs.
2. bl_domain_lookup: List of malicious domains.
3. bl_host_lookup: List of malicious hosts.
4. bl_url_lookup: List of malicious urls.
5. bl_asn_lookup: List of ASNs that are hosting malware.
6. crimeservers_lookup: The entire context needed for each ip, domain, host, url and asn.

These lookup tables will help you correlate information from other events, like a proxy, from IPlevel to url level, allowing you to decide how much accuracy your application needs.

You can force to download the full database by pressing the “Restart feed” button. This action does not delete the current data, it downloads all current online crimeservers and adds

3.3. Search

[illegible]

3.4. Bot Ips

This tap shows the current state of the Bot IPs feed. It provides information about the last inserted infected IPs, as well as trends like most infected operating systems or the top 10 portal domains that bots are reporting data to a C&C.

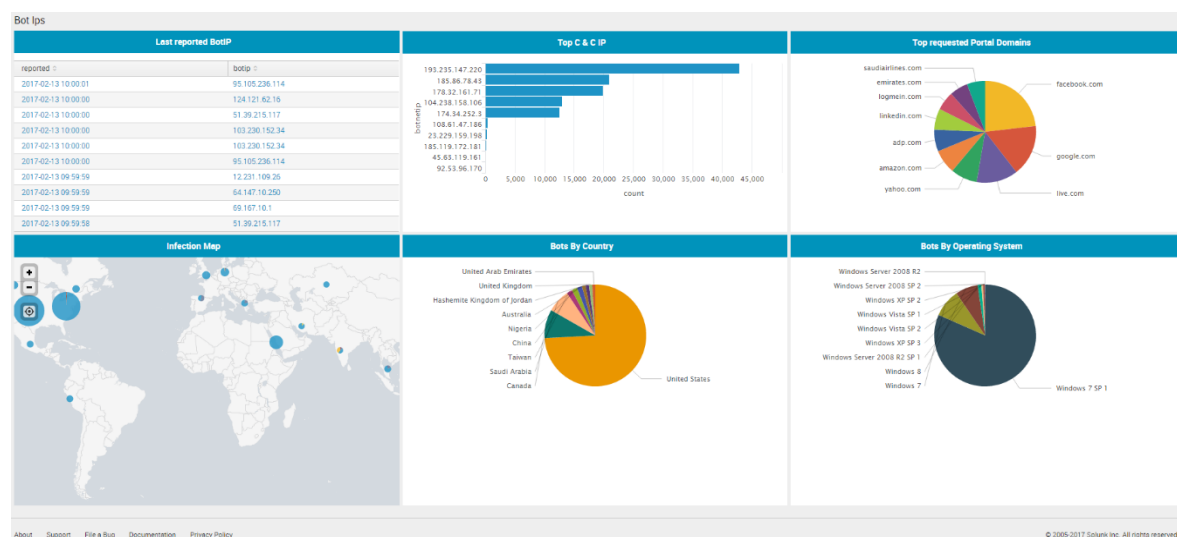
Field Name	Description
Botip	IP of the infected machine
url	Url where the bot is reporting the leaked

	data
Botnetip	IP where the bot is reporting the leaked data
Type	Botnet categorization
Portalurl	Url where the login attempt was done
Portaldomain	Domain from the portalurl
Port	Port from portalurl if present
Operatingsystem	Operating System used by the infected machine
Country	Country of the botip
City	City of the botip
Asn	ASN of the botnetip
Lat	Latitude of the botip
Lon	Longitude of the botip
seenAt	Date when the botip was detected

createdAt

Date of creation

Check more detailed description about this feed at: <https://apidocs.blueliv.com/#bot-ip11>



This feed is updated every 10 minutes and provide multiple lookup tables to improve your logs. The list below shows all the lookup tables available with the feed:

1. `bl_bot_ip_lookup`: List of the infected IPs ordered by date and the number of occurrence in the feed.
2. `bl_bot_botnetip_lookup`: List of the Command & Control IPs where the bots are sending their data.
3. `bl_bot_portaldomain_lookup`: List of domains from where data extracted from bots belong.
4. `bl_bot_portalurl_lookup`: List of urls that a bot has reported data.

All these lookup tables are available from everywhere and can be correlated with any other kind of event.

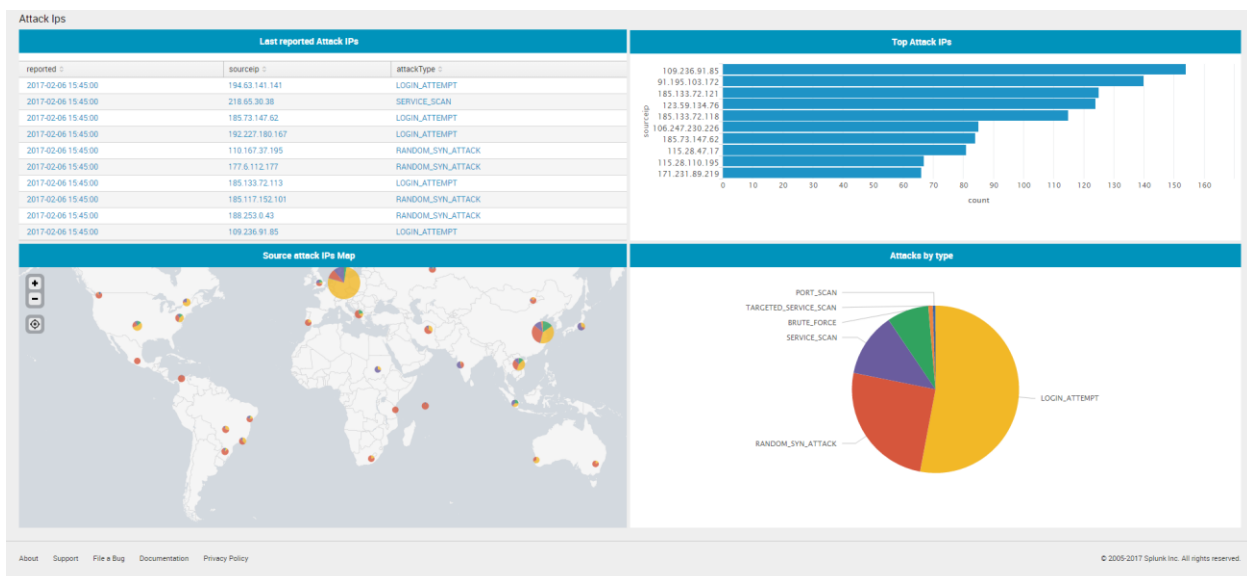
3.5. Attack IPs

This dashboard represents the current state of the Attacking IPs feed. Attacking IPs feeds provides real-time data about attacks from multiple IPs over the world. The feed is enriched with geo-location information, timestamp and attack categorization.

Field Name	Description
attackType	Attack categorization
firstEvent	Date of the first event in the attack series
lastEvent	Date of the last event in the attack series
numEvents	Number of events in the attack series
Sourceip	Source IP of the attack
Sourcecountry	Country of the attack source IP
Sourcecity	City of the attack source IP
Sourceport	Used ports at source
Sourcelatitude	Latitude of source IP

Sourcelongitude	Longitude of source IP
Destinationport	Destination ports of the attack
DestinationserviceName	Services name attacked
destinationCountry	Country of the destination IP
Destinationlatitude	Latitude of the destination IP
Destinationlongitude	Longitude of the destination IP
createdAt	Date of attack series creation

Check more detailed description about this feed at: <https://apidocs.blueliv.com/#attacking-ips13>



This feed is updated every 30 minutes and populate a KVStore collection and multiple lookup tables described below.

1. attackips_lookup: KVStore where all attacks data is stored.
2. bl_attack_ip_lookup: List of unique attacking IPs.

All these lookup tables are available from everywhere and can be correlated with any other kind of event.

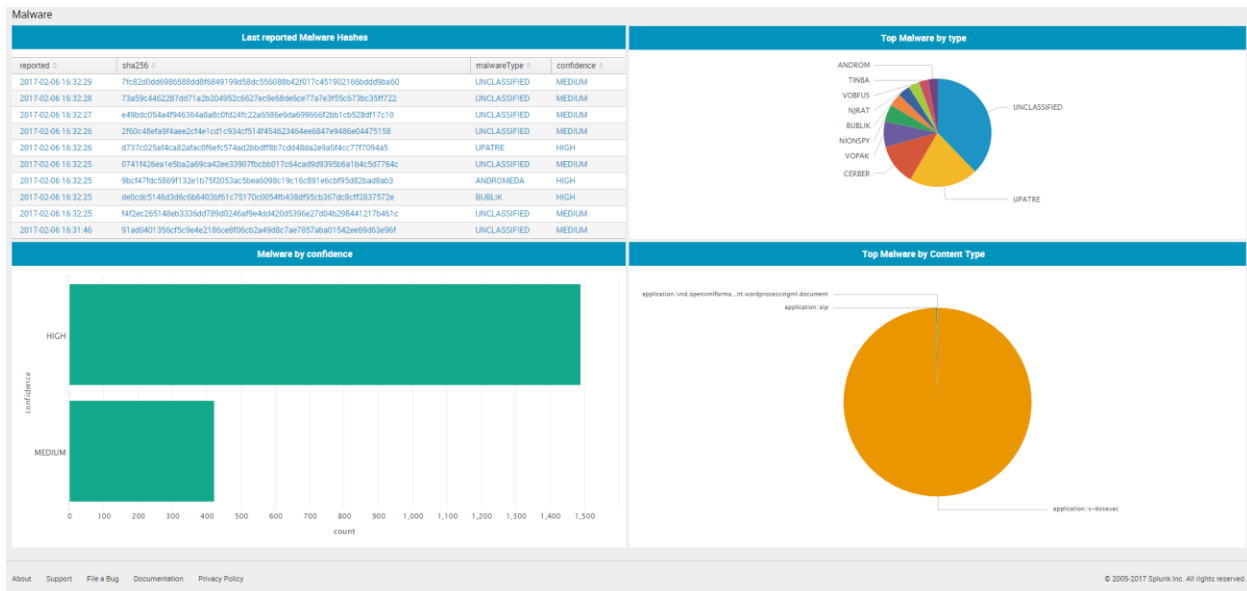
3.6. Malware

The main goal of this dashboard is to be able to check the last analyzed malwares by Blueliv Platform. It integrates the malware feed into Splunk allowing to check binary files by hash in the provided lookup tables. Every single malware has its confidence score rated as LOW, MEDIUM or HIGH. Blueliv also provides a malware behavioral categorization and some extra metadata from the malware sample itself.

Field Name	Description
filename	Original name of the malware sample
contentType	Binary content type
Md5	MD5 hash of the malware sample
SHA1	SHA1 hash of the malware sample
SHA256	SHA256 of the malware sample

analyzedAt	Date when the sample was analyzed in Blueliv platform
firstSeenAt	Date when the sample was seen for the first time
fileType	Executable type
fileSize	Original size of the malware sample
malwareType	Behavioral categorization of the malware sample (PONY, ZEUS, etc)
Confidence	Confidence extracted from Blueliv Platform rated as LOW-MEDIUM-HIGH
Architecture	Binary architecture (WIN32, WIN64, etc)

Check more detailed description about this feed at: <https://apidocs.blueliv.com/#malware12>

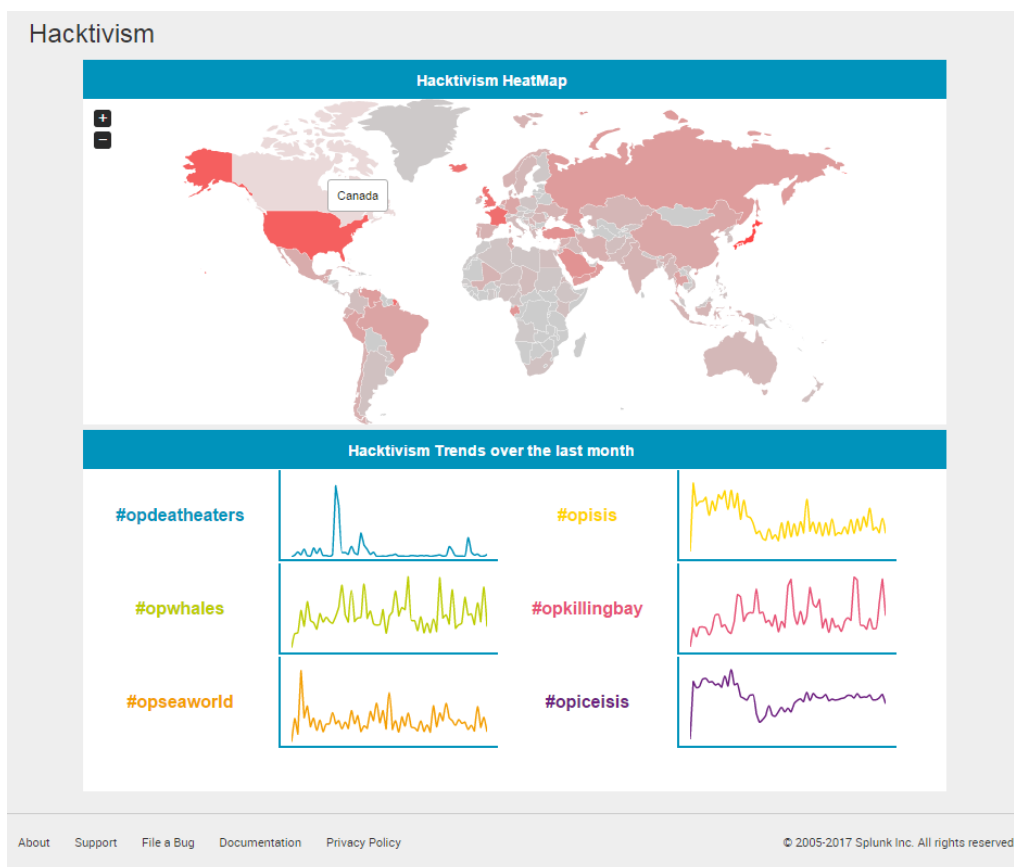


This feed is updated every 10 minutes and populates a KVStore and multiple lookup tables described below.

1. `malwares_lookup`: kvstore that keeps all the data related to this feed.

3.7. Hacktivism

Hacktivism dashboard shows graphic trends about hacktivist activity. On the top, there is a Heat Map that shows the Hacktivism threats detected around the world. At the bottom there is the TOP 6 hacktivism hashtags list, over the last month.



Check more detailed description about this feed at:
<https://apidocs.blueliv.com/#hactivism14>

4. Registration

If you are interested in getting full access to our Threat Intelligence feed, contact us at sales@blueliv.com to get your API credentials that will allow you to update Splunk App for Blueliv's local Data Base with current and real-time Threat Intelligence updates.

There are two access modes, Commercial and Free. If you are using the free access, some features will be disabled as shown in the image below and the update time will be less frequent.

