**THREAT INTELLIGENCE HUB**

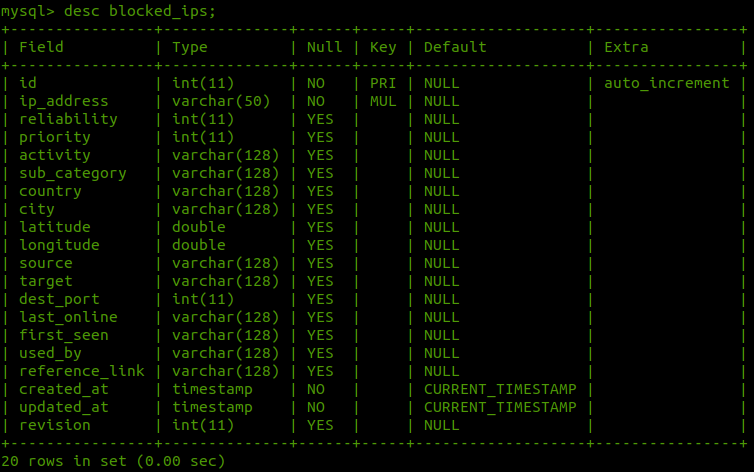
* **Introduction:**

A system to store, collect and manage blocked IP address and Malicious URLs, collected from the various global databases. Threat intelligent hub is set of database and API to access these databases. This hub includes two modules namely IP address, Ransomware database and Malicious URLs database.

* **Module – 1: IP address:**

A collection of blocked IP address and ransomware updated at specific interval with their details on following parameters.

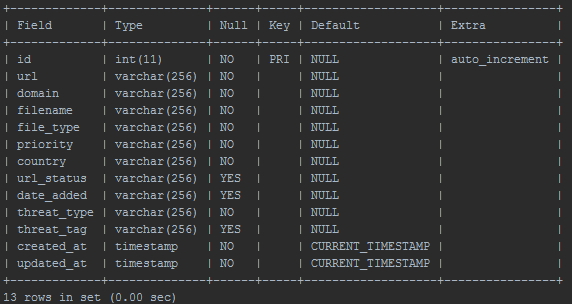
* + 1. reliability
    2. priority
    3. activity
    4. sub\_category
    5. country
    6. city
    7. coordinates
    8. source
    9. target
    10. dest\_port
    11. last\_online
    12. first\_seen
    13. used\_by
    14. reference\_link
* **Table structure:**



### **Module 2 - Malicious URLs and Ransomware**

A collection of malicious URLs and ransomware updated at specific interval with their details on following parameters.

* 1. domain
  2. file\_type
  3. priority
  4. url\_status
  5. threat\_tag
  6. filename
  7. country
  8. date\_added
  9. threat\_type
  10. date\_added
* **Table structure**



### **Note:**

* 1. Access the logs in **threat-intell-hub/logs/threat\_hub.log**
  2. Any changes in configuration must be updated in **config.py**
* **Project Directory and modules:**

This includes the following directory structure

**threat-intell-hub/**

**api/**

**commom/**

config.py

crawler.py

logger.py

targets.py

threat\_db.py

**docs/**

**ip\_address/**

driver.py

location\_updator.py

processor.py

**logs/**

threat\_hub.log

**resource/**

db\_updater.sh

GeoLite2-City.mmdb

**urls/**

driver.py

parser.py

processor.py

ipmain.py

urlmain.py

requirements.txt

README.md

* **Explaination:**

1. **api/:**
2. **common/:**

This directory contains utilities which are required for all the modules such as

* A URL crawler,
* A logger of logging purpose,
* targets module to contain source endpoints
* threat\_db is a Mysql database API for interacting with Mysql database.

1. **Docs/:**

This directory contains project documentation and necessary resources.

1. **ip\_address/:**

IP address is a python package containing ip\_address module and functionality. This code handle database comparison and storing logic.

1. **Logs/**

A directory to contain threat\_hub.log file generated and updated by logger module on project each project run.

1. **Resource/**

A directory to contain IP address city geolocation database from Maxmind and a updater shell script to update the database using cron job.

1. **Urls/**

urls is a python package containing module and functionality. This code handle database comparison and storing logic

1. **ipmain.py**

The main python executing script for blocked IP address and ransomware module

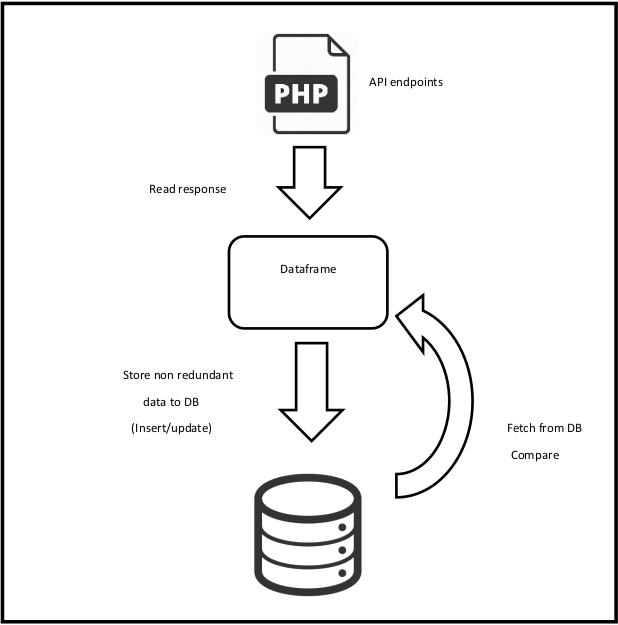
1. **urlmain.py**

The main python executing script for malicious urls module

1. **requirements.txt**

All python project dependencies to be install with **pip install -r requirements.txt**

* **Workflow:**



**INTEGRATION WITH LTS Secure (LTS Pulse Sync)**

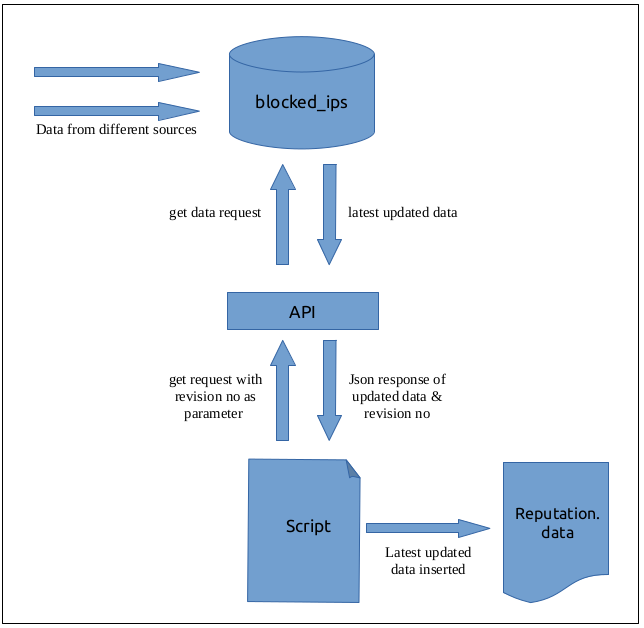
* **Introduction**

The complete central threat database information needs to be integrated with LTS secure in the form of pulse. To achieve this, there are set of APIs. These APIs are exposing threat table data to update reputation data file.

* **APIs**

1. List IP address with revision number
2. List all IP address
3. List all URLs
4. List all malware URLs
5. List all phishing URLS
6. List all ransomware URLS
7. Search IP address
8. Search URLs

* **Working:**

****

* **ListIPaddressAPIView (With Revision number):**

1. endpoint: $ curl [http://172.16.0.188/ip](http://172.16.0.188/iplist/)/list/?revision=<number>
2. type: GET
3. response:

{ "93.58.104.168":

{

"reliability":"4",

"priority":"2",

"activity":"MaliciousHost",

"sub\_category":"undefined",

"country":"IT",

"city":"Bari",

"lat":"41.1114997864",

"long":"16.8554000854",

"source":"unknown",

"target":"unknown",

"dest\_port":0,

"last\_online":0,

"first\_seeen":0,

"used\_by":"unknown",

"reference\_link":"undefined"

},…….

}

* **ListIPaddressAPIView (List All IP address):**

1. endpoint: $ curl [http://172.16.0.188/ip](http://172.16.0.188/iplist/)/list/
2. type: GET
3. response:

{ "93.58.104.168":

{

"reliability":"4",

"priority":"2",

"activity":"MaliciousHost",

"sub\_category":"undefined",

"country":"IT",

"city":"Bari",

"lat":"41.1114997864",

"long":"16.8554000854",

"source":"unknown",

"target":"unknown",

"dest\_port":0,

"last\_online":0,

"first\_seeen":0,

"used\_by":"unknown",

"reference\_link":"undefined"

},…….

}

* **ListURLAPIView:**

1. endpoint: $ curl [http://172.16.0.188/u](http://172.16.0.188/iplist/)rl/list/
2. type: GET
3. response:

{"<http://157.245.67.116/lmaoWTF/loligang.arm7>":

{

"domain":"157.245.67.116",

"filename":"loligang",

"file\_type":"arm7",

"priority":"high",

"country":"unknown",

"url\_status":"unknown",

"date\_added":"2019-09-09 12:49:02 UTC",

"threat\_type":"malware\_download",

"threat\_tag":["elf","mirai"]

},……

}

* **ListMalwareURLAPIView:**

1. endpoint: $ curl [http://172.16.0.188/](http://172.16.0.188/iplist/)url/list/?type=malware
2. type: GET
3. response:

{"<http://157.245.67.116/lmaoWTF/loligang.arm7>":

{

"domain":"157.245.67.116",

"filename":"loligang",

"file\_type":"arm7",

"priority":"high",

"country":"unknown",

"url\_status":"unknown",

"date\_added":"2019-09-09 12:49:02 UTC",

**"threat\_type":"Malware",**

"threat\_tag":["elf","mirai"]

},……

}

* **ListPhishingURLAPIView:**

1. endpoint: $ curl [http://172.16.0.188/](http://172.16.0.188/iplist/)url/list/?type=phishing
2. type: GET
3. response:

{"<http://157.245.67.116/lmaoWTF/loligang.arm7>":

{

"domain":"157.245.67.116",

"filename":"loligang",

"file\_type":"arm7",

"priority":"high",

"country":"unknown",

"url\_status":"unknown",

"date\_added":"2019-09-09 12:49:02 UTC",

**"threat\_type":"Phishing",**

"threat\_tag":["elf","mirai"]

},……

}

* **ListRansomwareURLAPIView:**

1. endpoint: $ curl [http://172.16.0.188/](http://172.16.0.188/iplist/)url/list/?type=ransomware
2. type: GET
3. response:

{"<http://157.245.67.116/lmaoWTF/loligang.arm7>":

{

"domain":"157.245.67.116",

"filename":"loligang",

"file\_type":"arm7",

"priority":"high",

"country":"unknown",

"url\_status":"unknown",

"date\_added":"2019-09-09 12:49:02 UTC",

**"threat\_type":"Ransomware",**

"threat\_tag":["elf","mirai"]

},……

}

* **SearchIPaddressAPIView:**

1. endpoint: $ curl [http://172.16.0.188/i](http://172.16.0.188/iplist/)p/search/?ip=<ip-address>
2. type: GET
3. response:

{ "93.58.104.168":

{

"reliability":"4",

"priority":"2",

"activity":"MaliciousHost",

"sub\_category":"undefined",

"country":"IT",

"city":"Bari",

"lat":"41.1114997864",

"long":"16.8554000854",

"source":"unknown",

"target":"unknown",

"dest\_port":0,

"last\_online":0,

"first\_seeen":0,

"used\_by":"unknown",

"reference\_link":"undefined"

}

}

* **SearchURLAPIView:**

1. endpoint: $ curl [http://172.16.0.188/](http://172.16.0.188/iplist/)url/search/?url=<url>
2. type: GET
3. response:

{"<http://157.245.67.116/lmaoWTF/loligang.arm7>":

{

"domain":"157.245.67.116",

"filename":"loligang",

"file\_type":"arm7",

"priority":"high",

"country":"unknown",

"url\_status":"unknown",

"date\_added":"2019-09-09 12:49:02 UTC",

"threat\_type":"malware",

"threat\_tag":["elf","mirai"]

}

}

* **Software Project Requirements**
  1. Python 3.6
  2. Ubuntu/CentOS Linux
  3. Python Packages:
  4. certifi==2019.6.16
  5. chardet==3.0.4
  6. geoip2==2.9.0
  7. idna==2.8
  8. maxminddb==1.4.1
  9. mysql-connector-python==8.0.17
  10. numpy==1.16.4
  11. pandas==0.24.2
  12. protobuf==3.9.0
  13. python-dateutil==2.8.0
  14. pytz==2019.1
  15. requests==2.22.0
  16. requests-file==1.4.3
  17. retrying==1.3.3
  18. six==1.12.0
  19. tldextract==2.2.1
  20. urllib3==1.25.3

First query to be executed by deployment team

INSERT INTO client\_details (Client\_Name, Client\_IP) VALUES ('Name', 'IP-address');