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 and 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:

```
mysql> desc blocked_ips;
+----------------+--------------+------+-----+-------------------+----------------+
| Field          | Type         | Null | Key | Default           | Extra          |
+----------------+--------------+------+-----+-------------------+----------------+
| id             | int(11)      | NO   | PRI | NULL              | auto_increment |
| ip_address     | varchar(50)  | NO   | MUL | NULL              |                |
| reliability    | int(11)      | YES  |     | NULL              |                |
| priority       | int(11)      | YES  |     | NULL              |                |
| activity       | varchar(128) | YES  |     | NULL              |                |
| sub_category   | varchar(128) | YES  |     | NULL              |                |
| country        | varchar(128) | YES  |     | NULL              |                |
| city           | varchar(128) | YES  |     | NULL              |                |
| latitude       | double       | YES  |     | NULL              |                |
| longitude      | double       | YES  |     | NULL              |                |
| source         | varchar(128) | YES  |     | NULL              |                |
| target         | varchar(128) | YES  |     | NULL              |                |
| dest_port      | int(11)      | YES  |     | NULL              |                |
| last_online    | varchar(128) | YES  |     | NULL              |                |
| first_seen     | varchar(128) | YES  |     | NULL              |                |
| used_by        | varchar(128) | YES  |     | NULL              |                |
| reference_link | varchar(128) | YES  |     | NULL              |                |
| created_at     | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| updated_at     | timestamp    | NO   |     | CURRENT_TIMESTAMP |                |
| revision       | int(11)      | YES  |     | NULL              |                |
+----------------+--------------+------+-----+-------------------+----------------+
20 rows in set (0.00 sec)
```

- **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**

```
+-------------+--------------+------+-----+--------------------+----------------+
| Field       | Type         | Null | Key | Default            | Extra          |
+-------------+--------------+------+-----+--------------------+----------------+
| id          | int(11)      | NO   | PRI | NULL               | auto_increment |
| url         | varchar(256) | NO   |     | NULL               |                |
| domain      | varchar(256) | NO   |     | NULL               |                |
| filename    | varchar(256) | NO   |     | NULL               |                |
| file_type   | varchar(256) | NO   |     | NULL               |                |
| priority    | varchar(256) | NO   |     | NULL               |                |
| country     | varchar(256) | NO   |     | NULL               |                |
| url_status  | varchar(256) | YES  |     | NULL               |                |
| date_added  | varchar(256) | YES  |     | NULL               |                |
| threat_type | varchar(256) | NO   |     | NULL               |                |
| threat_tag  | varchar(256) | YES  |     | NULL               |                |
| created_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP  |                |
| updated_at  | timestamp    | NO   |     | CURRENT_TIMESTAMP  |                |
+-------------+--------------+------+-----+--------------------+----------------+
13 rows in set (0.00 sec)
```

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

- **Explanation:**

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.

3. **Docs/:**

   This directory contains project documentation and necessary resources.

4. **ip_address/:**

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

5. **Logs/**

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

6. **Resource/**

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

7. **Urls/**

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

8. **ipmain.py**

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

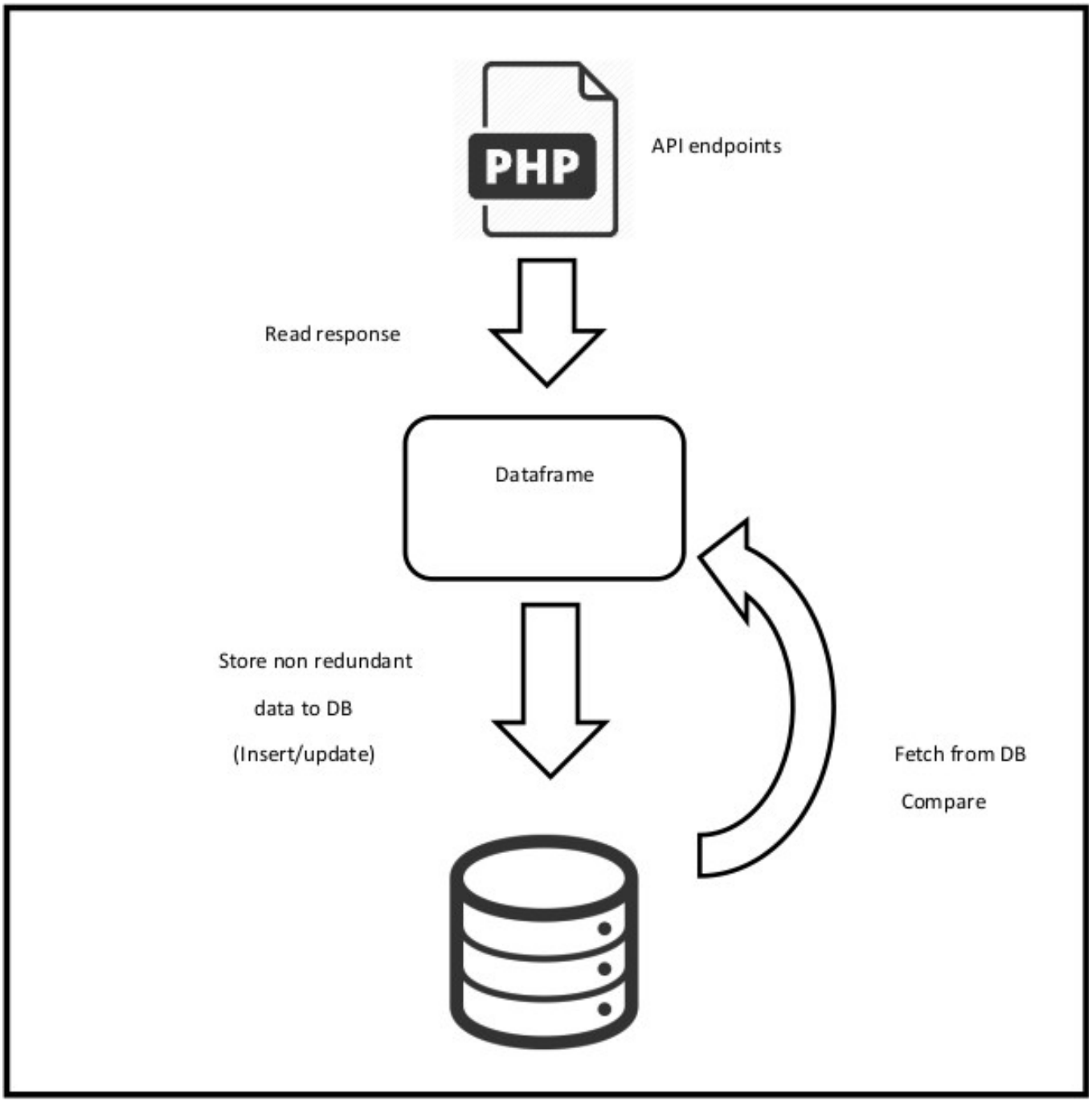
9. **urlmain.py**

   The main python executing script for malicious urls module

10. **requirements.txt**

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

- **Workflow:**


PHP
API endpoints
Read response
Dataframe
Store non redundant
data to DB
(Insert/update)
Fetch from DB
Compare

INTEGRATION WITH LTS Secure (LTS Pulse Sync)

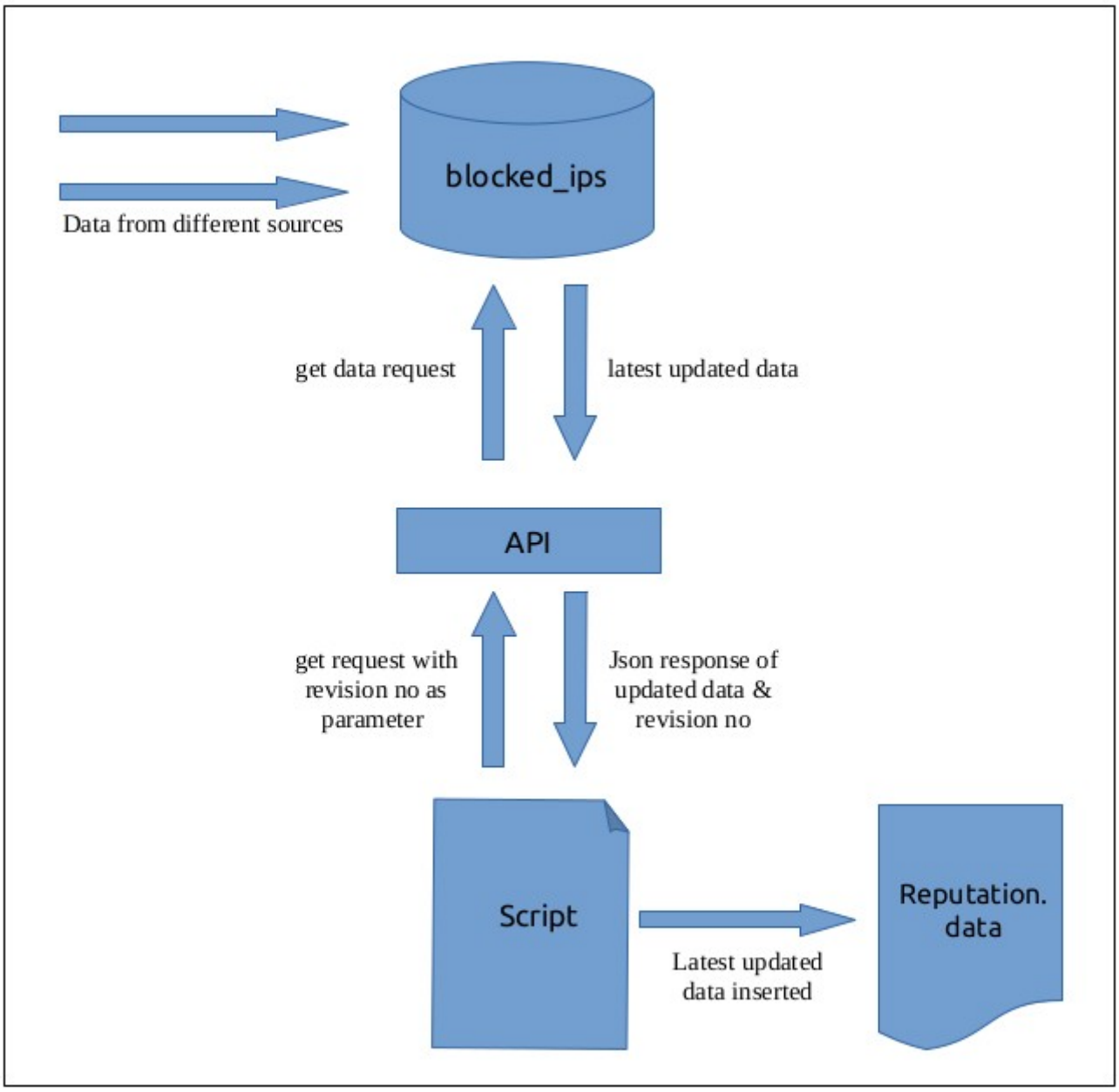
- ## Introduction

  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/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):**

4. endpoint: $ curl http://172.16.0.188/ip/list/
5. type: GET
6. 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/url/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/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/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:**

4. endpoint: $ curl http://172.16.0.188/url/list/?type=ransomware
5. type: GET
6. 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/ip/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/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:
        1. certifi==2019.6.16
        2. chardet==3.0.4
        3. geoip2==2.9.0
        4. idna==2.8
        5. maxminddb==1.4.1
        6. mysql-connector-python==8.0.17
        7. numpy==1.16.4
        8. pandas==0.24.2
        9. protobuf==3.9.0
        10. python-dateutil==2.8.0
        11. pytz==2019.1
        12. requests==2.22.0
        13. requests-file==1.4.3
        14. retrying==1.3.3
        15. six==1.12.0
        16. tldextract==2.2.1
        17. urllib3==1.25.3