PROJECT WORK
ON SECURITY OF INFORMATION M

Alessandro Vannini

CryptoNet Labs SRL

INTRODUCTION

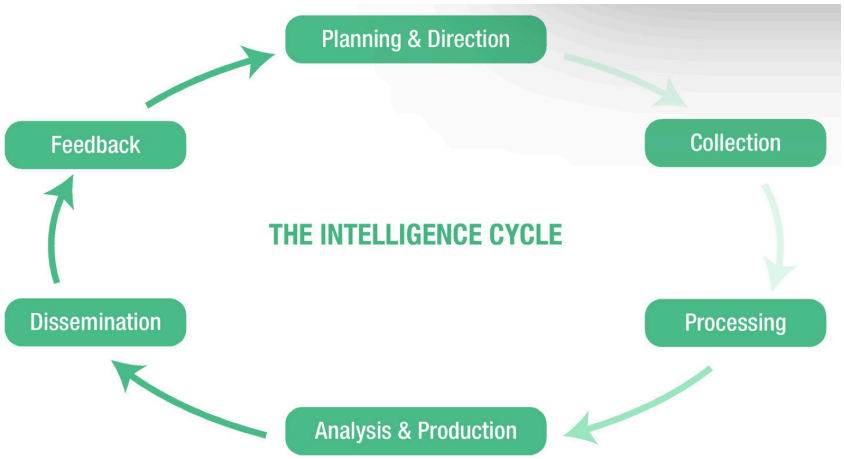
ABSTRACT

This project work involves the development of a tool able to analyze in an automated way the security posture of an IP address or URL. The tool will, once prompted with the IP or URL ,automatically execute numerous searches through many API and libraries given by websites dedicated to hosting blacklists of malicious, spam, bot and phishing URLs and IPs. The tool, based on the analysis carried out, will provide in output a score (with relative description) that classifies the level of security of the entity given in input, obtained by calculating the weighted average of the results of the various searches carried out.
The developed tool will be accompanied by this document, that defines the state of the art of the analysis of the security posture, as well as researches on eventual other available tools and detailed explanation of the functioning of the developed program.

CHAPTER 1: CTI, OSINT AND SECURITY POSTURE

WHAT IS THE CYBER THREAT INTELLIGENCE?

In the simplest possible terms, cyber threat intelligence (CTI) is the process of taking disparate pieces of information about a cyber attack and identifying the context in which it happened and what that means. The CTI process can be easily described through the Intelligence Cycle



The intelligence cycle is the process an analyst uses to collect, analyze, and report intelligence findings. The cycle is the same whether the analyst is looking at SIGINT, HUMINT, cyber, or imagery-based intelligence. The path is always the same, and when the process ends, the analyst starts again with the next requirement.

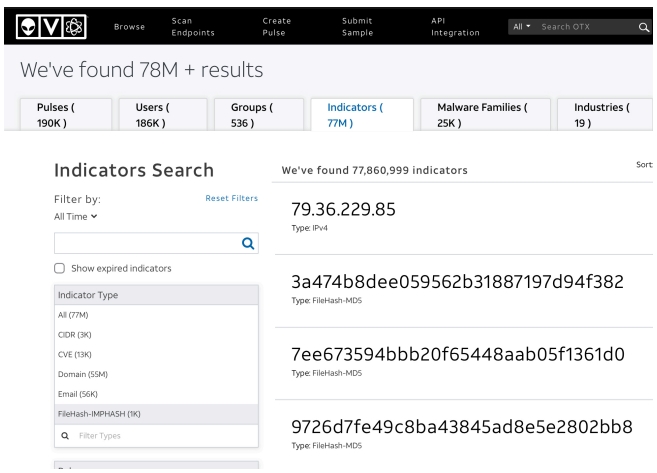
- Planning and Detection: this is where the intelligence team prioritizes their intelligence requirements; the intel team takes this requirement, establishes which tools and sources would be best placed to fulfill it, and then sets about establishing their collection for this particular area of concern.
- Collection: With the requirement established, the focus shifts to collecting relevant intelligence.This process can take considerable amounts of time, dependent on what the analyst identifies and where the trail leads them. In this point it is possible to see how useful is the concept of a cycle since, if the analyst doesn't find and information during the collection phase of the first cycle, he will still be able to find it during other cycles.
- Processing and exploitation: In CTI, this is where all the disparate information are brought into one place to enable the analysis. Depending on the size and type of the organization, it is possible to consider using a Threat Intelligence Platform (TIP) for this. TIPs are a potent tool for an analyst, since a good TIP will act as an intelligence repository of all collected information, will identify links between disparate pieces of data from multiple sources and will allow the analyst to automate large parts of the processing and exploitation part of the process.
- Analysis: This phase is where the analyst brings all the collected and processed information into one place and analyzes it for new or key information that can provide context on the threat. The analyst will look for patterns in data. This process can repeat as often as necessary until the analyst is satisfied and sure that he has all the relevant data and information needed.
- Dissemination: This phase is where the analyst takes all the new information they have identified and applies the relevant context for their customer into a finished intelligence

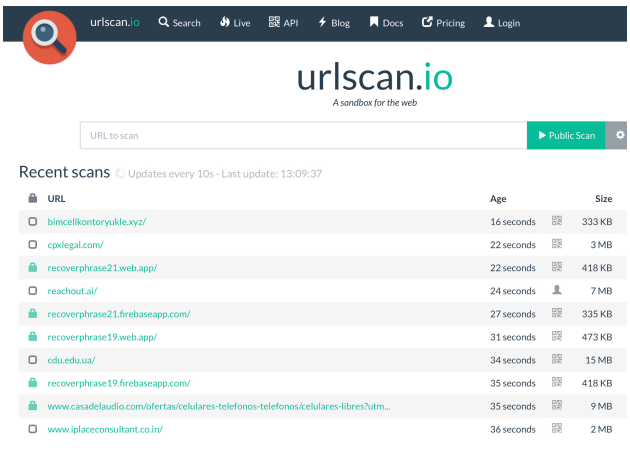
report. This finished report can come in many forms: for example, a long-form written report highlighting the trends, key TTPs, and motivations of the actor in question.

- Feedback: As with anything that's customer-facing, intelligence analysts have the same problems as anyone else: getting feedback from their customers. A good security team will provide constructive feedback on the products published by the intelligence team and the results of implementing any actions. This is vital for the intel team, so they know what products are hitting the mark and which ones don't match their customers' requirements.

WHAT IS OSINT?

The tool I've developed is useful during the Collection phase of the Intelligence Cycle. In particular, the tool is related to the concept of OSINT. At its core, OSINT(Open Source INTelligence) is information within the public domain that can be used for intelligence purposes. This differs from open source information (OSINF) in that the analyst applies the intelligence context to the data.
There are several ways and means of acquiring OSINT data, but the most common ways are through Threat Feeds and Research Platforms.
Within the world of Cyber Threat Intelligence, possibly the first place where it is possible to come across the concept of OSINT is with threat feeds.
Simply put, an OSINT feed is generally a collection of malicious entities(IP address, URL, e-mails address,…) that are usually collected from either crowdsourcing (like AlienVault OTX2) or honeypots run by security researchers (such as Abuse.ch3).
These feeds can be ingested into platforms such as a Threat Intelligence Platform (TIP) or a Security Information and Event Management (SIEM) and used to reference potential malicious activity within an organization or add further context to information already available.
Given the concept of Threat Feed, Research Platforms go a step further and ingest the Threat Feed's . This allows the possibility to offer some research functionality when investigating cyber threats. Some of these tools, such as VirusTotal, Any.run, Hybrid Analysis, URLScan and Joe Sandbox provide a range of functionality for researching files, domains, IP addresses, and URLs.. By combining these tools for a research, it is possible to perform some powerful analysis of cyber threats. In the following image is showed the threat feed of AlienValut and the search engine of URLScan.io.

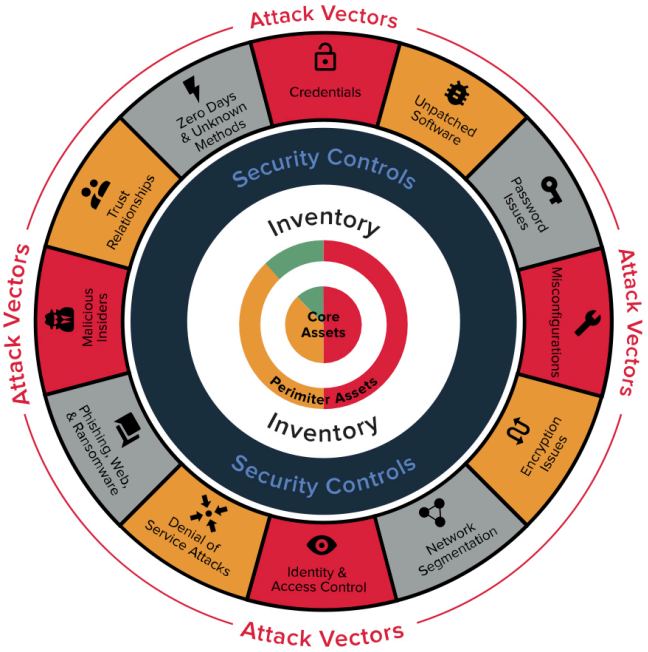




In a CTI context, one of the most common things it is likely to research is the adversary infrastructure, either in incident response or general threat actor tracking. Usually, this will

involve domains, IP addresses, email addresses, certificates, tracking/analytical cookies, hosting providers, registrars, and more.
Due to the human reluctance to change from what is known and understood, it will be very likely possible to track some adversaries through how they register domains, the details they use, and the reuse of infrastructure. Utilizing tools like VirusTotal and BuiltWith, it is possible to look at the adversaries' infrastructure, understand the underlying technologies being used, and then pivot from that to find other possible domains and campaigns. Otherwise it is also possible to take this information to discuss whether to block all connectivity to specific IP addresses if a plethora of malicious activity is found. Researching and understanding the technologies being used to create and manage malicious infrastructure can help with threat actor tracking and monitoring and potentially give a head start on blocking domains as they're registered.
To resume if few words what is written above, it is incredible the scale of things that can be achieved purely from information that is publicly accessible.

WHAT IS THE SECURITY POSTURE?
The tool I've developed can shine the most when used for defining the security posture of your organization, an adversary or a single person. According to the NIST, the security posture is defined as following:
"The security status of an enterprise's networks, information, and systems based on information security resources (e.g., people, hardware, software, policies) and capabilities in place to manage the defense of the enterprise and to react as the situation changes."



In other words, the security posture is a measure of:
- The level of visibility of asset inventory and attack surface
- The controls and processes in place to protect yourself from cyber-attacks
- The ability to detect and contain attacks
- The ability to react to and recover from security events
- The level of automation in the security program

CHAPTER 2 : STATE OF ART

WHAT IS THE STATE OF ART IN TERMS OF OSINT AND SECURITY POSTURE?

The tool I've created is, in way, the first in its kind(for now). Anyway, that of course doesn't mean that there aren't other tools available on the web regarding OSINT and Security Posture. In fact, there is a quit wide plethora of instruments of this kind, raging from web tools, free and not, downloadable python scripts and even full desktop softwares.
While doing my researches, I've come across many of this tools, like the ones described here:

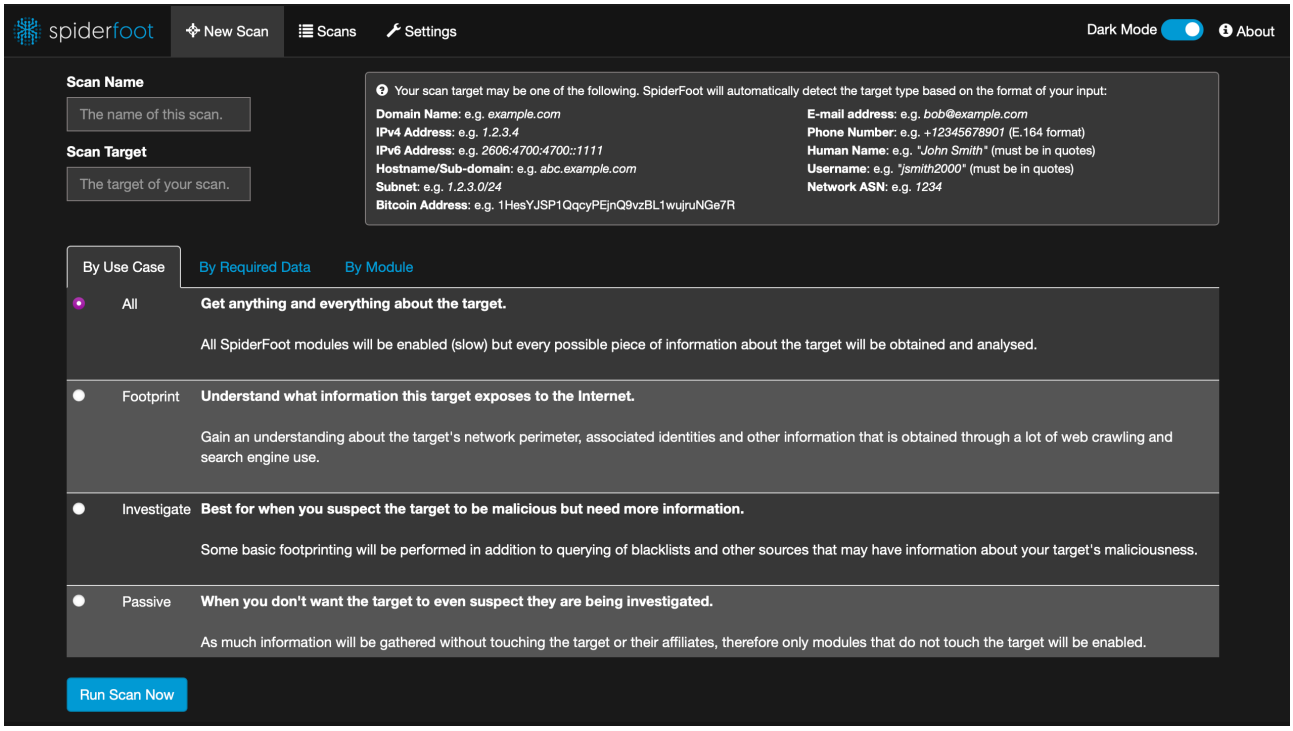
- Hook Analyzer:*"Hook Analyser is a freeware application which allows an investigator/ analyst to perform "static & run-time / dynamic" analysis of suspicious applications, also gather (analyse & co-related) threat intelligence related information (or data) from various open sources on the Internet."*
- Jeopardize:*"Jeopardize tool is developed to provide basic threat intelligence&response capabilities against phishing domains at the minimum cost as possible. It detects registered phishing domain candidates (typosquatting, homograph etc.), analyzes them and assigns a risk score to them. After then, it sends valid-looking credentials to the login forms on those phishing sites."*
- Sipi:*"This tool is aimed for Incident Response Team and anyone what's want to know the behaviour of the "suspicious" IP Address. The tools do search looking for reputation info from a set of open threat intelligence sources. Information about this IP like malware activity, malicious activity, blacklist, spam and botnet activity."*

All these tools (and many more) can be really useful during OSINT collecting or during the definition of the Security Posture of an entity. Anyway, none of the ones I've found has the same functionalities as the ones that my tool offer. In fact, only one software get really close to the tool I've defined, and that is SpiderFoot.

SPIDERFOOT

SpiderFoot is defined as following:
"SpiderFoot is a reconnaissance tool that automatically queries over 100 public data sources (OSINT) to gather intelligence on IP addresses, domain names, e-mail addresses, names and more. You simply specify the target you want to investigate, pick which modules to enable and then SpiderFoot will collect data to build up an understanding of all the entities and how they relate to each other."

In a few words, SpiderFoot is a powerful tool, that, when prompted with an IP address, domain, sub-domain, e-mail address and many more entities, will look for information about the given input in over 100 OSINT sources(also non-free sources) and provide them in output to the user. When setting up a new research the user can manually activate and deactivate the sources(called SpiderFoot modules) that he is interested in, or choose one of many presets that SpiderFoot offer. This software is free and represents the closest thing to my Tool, even if there are many difference that will be more explicit in the next chapter. Anyway, SpiderFoot is the perfect software for anyone how needs to gather as many information as possible on an computer entity. The following image show how the search engine of SpiderFoot works.


spiderfoot
New Scan
Scans
Settings
Dark Mode
About
Scan Name
The name of this scan.
Scan Target
The target of your scan.
Your scan target may be one of the following. SpiderFoot will automatically detect the target type based on the format of your input:
Domain Name: e.g. example.com
IPv4 Address: e.g. 1.2.3.4
IPv6 Address: e.g. 2606:4700:4700::1111
Hostname/Sub-domain: e.g. abc.example.com
Subnet: e.g. 1.2.3.0/24
Bitcoin Address: e.g. 1HesYJSP1QqcyPEjnQ9vzBL1wujruNGe7R
E-mail address: e.g. bob@example.com
Phone Number: e.g. +12345678901 (E.164 format)
Human Name: e.g. "John Smith" (must be in quotes)
Username: e.g. "jsmith2000" (must be in quotes)
Network ASN: e.g. 1234
By Use Case
By Required Data
By Module
All
Get anything and everything about the target.
All SpiderFoot modules will be enabled (slow) but every possible piece of information about the target will be obtained and analysed.
Footprint
Understand what information this target exposes to the Internet.
Gain an understanding about the target's network perimeter, associated identities and other information that is obtained through a lot of web crawling and search engine use.
Investigate
Best for when you suspect the target to be malicious but need more information.
Some basic footprinting will be performed in addition to querying of blacklists and other sources that may have information about your target's maliciousness.
Passive
When you don't want the target to even suspect they are being investigated.
As much information will be gathered without touching the target or their affiliates, therefore only modules that do not touch the target will be enabled.
Run Scan Now

CHAPTER 3: TOOL DEVELOPMENT AND WORKING

WHAT DOES THIS TOOL?

The tool I've developed is a python 3 script that will ask, through a terminal command line, to input an IP address or an URL. Once the entity to analyze is given, the tool will:

1) Research and output OSINT informations on the entity such as, in the case of an IP address, the corresponding domains or the geographical coordinates.
2) Define the Security Posture of the given entity, researching in many blacklists and other sources if the IP or URL, is unsafe, malicious, hacked, related to spam, phishing, bot and other threats.
3) Assign a Security Score, ideated and finely weighted by me, that goes from 0 to 100 and define the overall Security Posture of the URL or IP. Here is how the Security Score works in case of an IP address:
   - if the Security Score is equal to 100, it means that, according to all the blacklists and sources implemented in this Tool, the given IP is safe and not malicious.
   - if the Security Score is less than 100 and more than 80, it means that the given IP was found in one (or maximum two) blacklist or tool, meaning that it may be malicious.
   - if the Security Score is greater or equal to 50 and less than 80, it means that the given IP was found in more blacklists and tool, indicating that it is probably malicious and related to a threat.
   - if the Security Score is less than 50, it means that the given IP was found in multiple blacklists and tools, meaning that it is for sure malicious and related to a threat.
4) Optionally log all the output from the various phases in a text file.

The development of this tool took several time of research and coding and can be resumed in 3 different phases.

PHASE 1: RESEARCH

The first thing that had to be done was analyze the biggest possible number of blacklists and OSINT websites to understand which one were possible to implement inside my tool. Kitploit, GitHub and the SpiderFoot modules list where the biggest sources of research for this phase, that resulted in an excel document with almost 40 entries. Through a filtering operation I was then able to remove some of the entries that later resulted not possible to implement in the python script due to lacking of API or too expensive credits plan for using the available API. The final list of sources that were then implemented in my tool came out with around 28 entries. The following image show the structure of the excel document

Name	URL	Description	API	API request	API return		IMPLEMENTED	IMPLEMENTING	DROPPED
ThreatCrowd	https://www.threatcrowd.org	Obtain information from ThreatCrowd about identified IP addresses, domains and e-mail addresses.	X	import requests, json result = requests.get("https://www.threatcrowd.org/searchApi/v2/email/report/", params = {"email": "william19770319@yahoo.com"}) print result.text j = json.loads(result.text) print j['domains'][0]	{"response_code":"1","domains":["aoldaily.com","aunewsonline.com","cnndaily.com","usnewssite.com"],"references":[],"permalink":"https:\/\/www.threatcrowd.org\/email.php?email=william19770319@yahoo.com"} aoldaily.com	Same with ip= and domain=	X		
Internet Storm Center	https://isc.sans.edu	Check if an IP is malicious according to SANS ISC	X	To understand better			X		
CyberCrime	http://cybercrime-tracker.net	Check if a host/domain or IP is malicious according to cybercrime-tracker.net.							X
HackerTarget GeoIP	https://hackertarget.com/geoip-ip-location-lookup/	find the location of the IP address	X	curl https://api.hackertarget.com/geoip/?q=1.1.1.1 (in alternative with Python)			X		
HackerTarget Reverse IP lookup	https://hackertarget.com/reverse-ip-lookup/	is a way to identify hostnames that have DNS (A) records associated with an IP address.	X	https://api.hackertarget.com/reverseiplookup/?q=2.2.2.2	Plaintext				X
Fortiguard	https://www.fortiguard.com/services/ioc	Various services about IP							X

The following is a list of all the sources implemented in my script:

- Maltiverse
- ThreatCrowd
- Internet Storm Center
- HackerTarget GeoIP
- CoinBlockerList
- blocklist.de
- PhishStats
- Google Safe Browsing
- URLScan.io
- OpenPish
- Psbdmp
- PhishTank
- BuiltWith
- JsonWHOIS
- Pulsedive
- IP Quality Score
- Meta Defender
- BotScout
- AbuseIPDB
- FraudGuard
- Neutrino API
- IP registry

Many of these entries where implemented both for the URL and the IP lookup, making the count of sources implemented rise to around 28.

PHASE 2: IMPLEMENTATION AND CODING

The next phase was the implementation of all the sources above into a functioning Python 3 script. That resulted in an almost 1000 lines of code script structured as following:

- Main function: function that requests the input to the user, does some control and call one of the two functions next;

```
15
16  def main():
17      print("-------------------------------------------------------------");
18      print("WELCOME TO SECURITY TOOL!");
19      print("-------------------------------------------------------------");
20      print("Use this tool to find out the security posture of an IP Address or URL/Domain and to get some information about your target");
21      print("Security Tool searchs in more than 20 blacklists and uses several online tools to obtain all the information on the IP/Url/Domain
22      print("First insert an IP or URL when requested, then you will get:")
23      print("1)Information about the target")
24      print("2)security posture of the target")
25      print("3) A propretary Security Score about the target ")
26      print("4) OPTIONAL: a txt log file with all the ouptup about the target ")
27      print("-------------------------------------------------------------");
28
29
30      Ip_or_URL = input("Enter your IP or URL: ");
31      wantlog=input("Do you want the output to be logged on a txt file?(yes/no): ");
32      flag=0
33      if wantlog=="yes":
34          print("")
35          print("The output will be logged in a txt file called SecurityToolLog.txt, located in the same directory of this Tool.")
36          print("CAUTION: the txt log file will be overwritten at every run of this tool!")
37          sleep(5);
38          flag=1;
39          print("")
40      IPURL= list(Ip_or_URL);
41      if(IPURL[0] >= '0' and IPURL[0] <= '9'):
42          try:
43              ip = ipaddress.ip_address(Ip_or_URL);
44              print("You inserted an IP Address");
45              IpLookup(Ip_or_URL,flag);
46          except ValueError:
47              print("The given IP address is not valid");
48              exit;
49
50      else:
51          if (IPURL[0]=="h" and IPURL[1]=="t" and IPURL[2]=="t" and IPURL[3]=="p" and IPURL[4]=="s" and IPURL[5]==":"and IPURL[6]=="/"and IPURL
52              print("You inserted an URL ");
53              URLLookup(Ip_or_URL,flag);
```

- IPLookup function: function that is called by the main, with a correct IP as a parameter (and also a flag used for other purpose) and execute the program logic in case of an IP address, requesting to every API of the sources implemented and saving and evaluating the output in an useful way, decreasing the Security Score when needed.

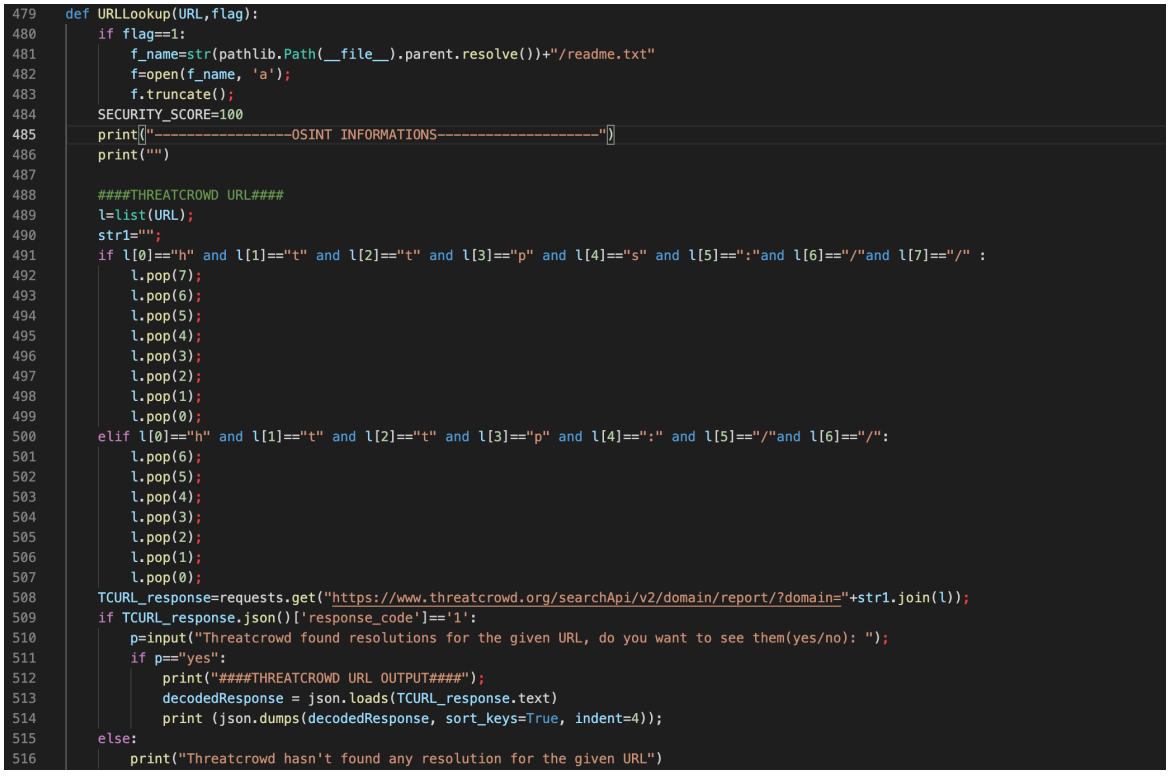
```
def IpLookup(IP,flag):
    if os.path.exists(str(pathlib.Path(__file__).parent.resolve())+"/readme.txt"):
        os.remove(str(pathlib.Path(__file__).parent.resolve())+"/readme.txt")
    if flag==1:
        f_name=str(pathlib.Path(__file__).parent.resolve())+"/readme.txt"
        f=open(f_name, 'a');

    SECURITY_SCORE=100
    print("-----------------OSINT INFORMATIONS--------------------")
    print("")
    ###THREATCROWD IP####
    TCIP_response=requests.get("https://www.threatcrowd.org/searchApi/v2/ip/report/?ip="+IP);
    if TCIP_response.json()['response_code']=='1':
        p=input("Threatcrowd found resolutions for the given IP, do you want to see them(yes/no): ");
        if p=="yes":
            print("####THREATCROWD IP OUTPUT####");
            decodedResponse = json.loads(TCIP_response.text)
            print (json.dumps(decodedResponse, sort_keys=True, indent=4));

    else:
        print("Threatcrowd hasn't found any resolution for the given IP")
    f.write("####THREATCROWD IP OUTPUT####")
    print_log(flag,TCIP_response.text,f);
    sleep(1);
    print("")

    #### HACKER TARGET GEOIP ####
    HTG_response=requests.get("https://api.hackertarget.com/geoip/?q="+IP);
    if "error" not in HTG_response.text:
        p=input("Hacker Target Geoip has found the geographical position of the given IP, do you want to see them?(yes/no):")
        if p=="yes":
            print("####HACKER TARGET GEOIP OUTPUT####");
            print(HTG_response.text);
    else :
        print("Hacker Target Geoip hasn't found the position of the given IP")
    f.write("####HACKER TARGET GEOIP OUTPUT####")
    print_log_txt_only(flag,HTG_response.text,f);
    sleep(1);
    print("")
```

- URLLookup function: function that is called by the main, with a correct URL as a parameter (and also a flag used for other purpose) and execute the program logic in case of an URL, requesting to every API of the sources implemented and saving and evaluating the output in an useful way, decreasing the Security Score when needed.



```
def URLLookup(URL,flag):
    if flag==1:
        f_name=str(pathlib.Path(__file__).parent.resolve())+"/readme.txt"
        f=open(f_name, 'a');
        f.truncate();
    SECURITY_SCORE=100
    print("-----------------OSINT INFORMATIONS--------------------")
    print("")

    ####THREATCROWD URL####
    l=list(URL);
    str1="";
    if l[0]=="h" and l[1]=="t" and l[2]=="t" and l[3]=="p" and l[4]=="s" and l[5]==":"and l[6]=="/"and l[7]=="/" :
        l.pop(7);
        l.pop(6);
        l.pop(5);
        l.pop(4);
        l.pop(3);
        l.pop(2);
        l.pop(1);
        l.pop(0);
    elif l[0]=="h" and l[1]=="t" and l[2]=="t" and l[3]=="p" and l[4]==":" and l[5]=="/"and l[6]=="/":
        l.pop(6);
        l.pop(5);
        l.pop(4);
        l.pop(3);
        l.pop(2);
        l.pop(1);
        l.pop(0);
    TCURL_response=requests.get("https://www.threatcrowd.org/searchApi/v2/domain/report/?domain="+str1.join(l));
    if TCURL_response.json()['response_code']=='1':
        p=input("Threatcrowd found resolutions for the given URL, do you want to see them(yes/no): ");
        if p=="yes":
            print("####THREATCROWD URL OUTPUT####");
            decodedResponse = json.loads(TCURL_response.text)
            print (json.dumps(decodedResponse, sort_keys=True, indent=4));
    else:
        print("Threatcrowd hasn't found any resolution for the given URL")
```

- utilities function: used for logging, if requested, the output of the various API int a txt file.

```
968    def print_log(flag,texts,f):
969        if flag==1:
970            decodedResponse = json.loads(texts)
971            f.write(json.dumps(decodedResponse, sort_keys=True, indent=4));
972
973    def print_log_txt_only(flag,texts,f):
974        if flag==1:
975            f.write(texts);
```

PHASE 3: OUTPUT REFINING AND DEFINITION OF THE SECURITY SCORE

The last part of the development of the tool was the refining of the output of every API, with the purpose of giving an output to the user that is clean human readable, and also to increasing the interactivity with the user.
Then I defined the Security Score in a way that, if a sources found some threat related to the given entity, the Security Score of that entity would decrease of a certain value (chosen based on the importance and reliability of the source). The Security Score is finally printed to the user, with the corresponding description.

```
942  print("-------------------------SECURITY SCORE RESULTS-------------------------")
943  print("")
944  print("")
945  if SECURITY_SCORE==100 :
946      print("The Security Score of the given URL is "+str(SECURITY_SCORE))
947      print("It means that, according to all the blacklists and sources implemented in this Tool, the given URL is safe and not malicious.")
948      print("CAUTION: this is Tool provides a good indicator of security, BUT this doesn't mean that the given URL is for sure safe. Other analys
949  elif SECURITY_SCORE==95:
950      print("The Security Score of the given URL is "+str(SECURITY_SCORE))
951      print("According to the sources in this tool, the given URL is not related to any threat, but has been found in a leaks database, meaning s
952  elif SECURITY_SCORE>=75 and SECURITY_SCORE<95:
953      print("The Security Score of the given URL is "+str(SECURITY_SCORE))
954      print("It means that the given URL was found in one ( or maximum two) blacklist or tool, meaning that it may be malicious.")
955  elif SECURITY_SCORE>=45 and SECURITY_SCORE<75:
956      print("The Security Score of the given URL is "+str(SECURITY_SCORE))
957      print("It means that the given URL was found in more blacklists and tool, indicating that it is probably malicious and related to a threat.
958  elif SECURITY_SCORE<40:
959      if SECURITY_SCORE < 0 :
960          SECURITY_SCORE=0;
961      print("The Security Score of the given URL is "+str(SECURITY_SCORE))
962      print("It means that the given URL was found in multiple blacklists and tools, meaning that it is for sure malicious and related to a threa
963
964  print("")
965  print("Thank you for using this Tool   -Alessandro Vannini")
966  print("-------------------------------------------------------------------------------")
967  f.close()
```

CHAPTER 4: TOOL APPLICATIONS

In this chapter, will be shown the output given by the tool both during an IP Lookup and a URL lookup, to show how the script works when prompted with real IP addresses and URLs.
The input that are requested from the script are highlighted in red.
IP lookup output:

WELCOME TO SECURITY TOOL!

Use this tool to find out the security posture of an IP Address or URL/Domain and to get some information about your target
Security Tool searchs in more than 20 blacklists and uses several online tools to obtain all the information on the IP/Url/Domain
First insert an IP or URL when requested, then you will get:
1)Information about the target
2)security posture of the target
3) A propretary Security Score about the target
4) OPTIONAL: a txt log file with all the ouptup about the target
---
Enter your IP or URL: 34.45.56.67
Do you want the output to be logged on a txt file?(yes/no): no
You inserted an IP Address
----------OSINT INFORMATIONS----------

Threatcrowd hasn't found any resolution for the given IP

Hacker Target Geoip has found the geographical position of the given IP, do you want to see them?(yes/no):yes
####HACKER TARGET GEOIP OUTPUT####
IP Address: 34.45.56.67
Country: United States
State:
City:
Latitude: 37.751
Longitude: -97.822

----------SECURITY POSTURE ANALYSIS----------
The Maltiverse search haven't produced any result

The Internet Storm Center search haven't produced any result

Coin Blocker List hasn't found the given IP in any engine.

Blocklist hasn't found any threat realted to the given IP address

Phishstats hasn't found any threat related to the given IP

How to interpret the Fraud Score:
Fraud Scores <= 40 -low risk
Fraud Scores >= 75 - suspicious - previous reputation issues or low risk proxy/VPN.
Fraud Scores >= 85 - high risk - recent abusive behavior over the past 24-48 hours.
ALERT: According to IP Quality Score, the given IP is suspicious, with a Fraud Score of 75. Do you want to see the full output?(yes/no): no
THE SECURITY SCORE IS DECREASING BY 20
IP Quality Score hasn't found anything related to the given IP

Meta Defender wasn't able to find anything related to the given IP

BotScout was not able to find any information on the given IP

According to AbuseIPDB, the given IP is probably safe, with an abuse confidence score of: 0. Do you wan to see the full output?(yes/no):no

How to interpret the FraudGuard risk level output:
1= No Risk
2 = Spam or Website Abuse (excessive scraping, resource linking or undesired site automation)
3 = Open Public Proxy
4 = Tor Node
5 = Honeypot, Malware, Botnet or DDoS Attack
According to Fortiguard, there is no risk related to the given IP

Neutrino hasn't found any threat related to the given IP

IP registry hasn't found any threat related to the given IP

----------SECURITY SCORE RESULTS----------

The Security Score of the given IP is 80
It means that the given IP was found in one (or maximum two) blacklist or tool, meaning that it may be malicious.

Thank you for using this Tool -Alessandro Vannini

URL lookup output:

WELCOME TO SECURITY TOOL!

Use this tool to find out the security posture of an IP Address or URL/Domain and to get some information about your target
Security Tool searchs in more than 20 blacklists and uses several online tools to obtain all the information on the IP/Url/Domain
First insert an IP or URL when requested, then you will get:
1)Information about the target
2)security posture of the target
3) A propretary Security Score about the target
4) OPTIONAL: a txt log file with all the ouptup about the target
---
Enter your IP or URL: https://www.unibo.it
Do you want the output to be logged on a txt file?(yes/no): no
You inserted an URL
----------OSINT INFORMATIONS----------

Threatcrowd found resolutions for the given URL, do you want to see them(yes/no): yes
####THREATCROWD URL OUTPUT####

```
{
    "emails": [],
    "hashes": [],
    "permalink": "https://www.threatcrowd.org/domain.php?domain=www.unibo.it",
    "references": [],
    "resolutions": [
        {
            "ip_address": "-",
            "last_resolved": "0000-00-00"
        },
        {
            "ip_address": "137.204.24.35",
            "last_resolved": "2021-12-12"
        }
    ],
    "response_code": "1",
    "subdomains": [],
    "votes": 0
}
```


Urlscan.io found informations relative to the given URL, do you want to see them?(yes/no):yes
####URLSCAN OUTPUT####

```
{
```

```
    "api": "https://urlscan.io/api/v1/result/7e41ffd4-7364-4e15-b0f3-944c08a18cc1/",
    "country": "it",
    "message": "Submission successful",
    "options": {},
    "result": "https://urlscan.io/result/7e41ffd4-7364-4e15-b0f3-944c08a18cc1/",
    "url": "https://www.unibo.it",
    "uuid": "7e41ffd4-7364-4e15-b0f3-944c08a18cc1",
    "visibility": "public"
}
```


*BuiltWith found information about the given URL technologies. Do you want to see them?(yes/no):*no

WhoIs hasn't found any information on the given URL.

----------SECURITY POSTURE ANALYSIS----------
The Maltiverse search haven't produced any result

Coin Blocker List hasn't found any threat related the given URL

Phishstats hasn't found any threat related to the given URL

Google Safe Browsing hasn't found any threat related to the given URL

*ALERT:PSBDMP found 9 elements in its Database, meaming that the given URL may be hacked. Do you want to see the full output?(yes/no):*no
THE SECURITY SCORE IS DECREASING BY 5

Phishtank hasn't found the given URL in its Phishing Database

Waiting for a response from Pulsedive API, this will take 15 seconds
Pulsedive hasn't found any information about the given URL OR the API request failed, you may try again.

How to interpret the Fraud Score:
Risk Scores >= 75 - suspicious - usually due to patterns associated with malicious links.
Suspicious URLs marked with Suspicious = true will indicate domains with a high chance for being involved in abusive behavior.
Risk Scores >= 85 - high risk - strong confidence the URL is malicious.
Risk Scores = 100 AND Phishing = true OR Malware = true - indicates confirmed malware or phishing activity in the past 24-48 hours.
According to IP Quality Score, the given URL is safe, with a Risk Score of 0. Do you want to see the full output?(yes/no):
no

How to interpret the status:
0 Allowlisted: URL is listed by the source in their allowlist. Note: Not all sources provide allowlists.
1 Blocklisted: URL is listed by the source in their blocklist. Refer to the source for more information regarding their blocklist.
3 Failed to scan: The results could not be retrieved from our servers
5 Unknown: The source has not listed this URL address in either their blocklist or allowlist.
Meta Defender wasn't able to find anything related to the given URL

----------SECURITY SCORE RESULTS----------

The Security Score of the given URL is 95
According to the sources in this tool, the given URL is not related to any threat, but has been found in a leaks database, meaning some information may have been leaked from that URL

Thank you for using this Tool -Alessandro Vannini
--

CONCLUSIONS

The tool I've developed can result quite helpful for anyone who is looking for information or is trying to define the Security Posture of an IP address or URL. In fact, with a single run of this tool, it is possible to understand if the given entity is safe, malicious or has some weakness.
It is possible to extend this tool in various way. Firstly by finding and implementing more of the OSINT sources, since really often it is possible to fine new ones. Otherwise, it is possible to extend this tool by expanding the kinds of input that it can receive and analyze. By that I mean that is it possible to introduce new lookups function for e-mails address, social media accounts and many more.
The code of this script is open source and available through my GitHub account (https://github.com/vonvans/SecurityTool.git).
Special thanks to CryptoNet Labs and Alfonso Solimeo that helped me through the definition and development of this tool.

REFERENCES

- *Cyber Threat Intelligence: The No-Nonsense Guide for CISOs and Security Manages. Aaron Roberts, Apress, 2021*
- *Hacking: Cyber Threat Intelligence vol.15,n°09, Hakin9 Media Sp. z o.o.*
- *PenTest magazine: OSINT on PenTest Targets, Hakin9 Media Sp. z o.o.*
- *https://csrc.nist.gov/glossary/term/security_posture*
- *https://www.balbix.com/insights/what-is-cyber-security-posture/*

Alessandro Vannini