IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10521

Analytical Study on IP Reputation Services & Automation for Traditional Method

Saraunsh Shewale[1], Prof. Leena Deshpande[2]

B. Tech Student, Computer. Engineering, Vishwakarma Institute of Information Technology, Pune, India[1]

Associate Professor, Computer Engineering, Vishwakarma Institute of Information Technology, Pune, India[2]

Abstract: A reputation score for an individual IP address is generated by an IP reputation platform, which can be used by businesses as a signal in a fraud risk scoring system. It is a common technique to identify malicious domains that are involved in spamming and phishing activities. IP reputation providers are becoming a popular risk assessment tool because they not only advise you if an IP address is hosting malicious content, but also whether it is involved in automated bot activity. Prior to the introduction of IP reputation services, organizations relied on solutions that linked the universal resource locator (URL) to malicious content such as spam, phishing emails, and viruses. URL-based solutions, on the other hand, were useless since they were sluggish to identify attacks and were easily circumvented by fraudsters. IP reputation services are now facing similar issues, as fraudsters leverage new tools and technologies to avoid detection.

Keywords: IP Reputation, Security, Threat Intel Feeds, Blacklists, Automation, Web Scraping.

I. INTRODUCTION

As Internet is being consumed and extensively used by the end users worldwide, today's network is challenged by large diversified cyber-attacks causing huge interruptions and loss in global organizations. To effectively tackle the attack vectors happening on larger scale, proactive measures are employed to detect such attacks in real time. An effective way to prevent users from cyber-attacks and limit the fraudsters, IP reputation services were developed. IP reputation services manages huge list of IP addresses with their reputation credibility score and all sort of WHOIS information related to the specific domain. IP reputation credibility score can be identified based on the behavior of the domain and malicious activities (Phishing, spamming, adware, etc.) carried out by them are flagged as blacklisted and saved in the repository of malicious threat vectors. These list of malicious vectors gets updated and managed by multiple public/private threat intel services. [1]

Almost all organizations rely on email as a key communications tool. They are constantly searching for spam filtering options as more and more spam messages arrive in their inboxes. IP reputation is an excellent solution in this context; the organization's mail servers check the IP reputation of the sending server during the SMTP handshake. This gives the receiving server an opportunity to reject incoming emails if the source IP of sending server is flagged as malicious in threat intel feeds. [2]

However, there are several issues related to IP based blacklists approach. Some of the threat intel databases are not being updated and managed in real time, they just hold static values and thus lacks in providing full-fledged security mechanism against new malicious vectors. Also, there might be the case that some authorized legitimate domains are being mistakenly added into the blacklist database and causing false positive paradigm. [3]
There are hundreds of both free and paid threat intel services that provide anyone with non-contextual lists of malicious IP addresses. The problem with IP address lists is that they do not renew rapidly, and not all malicious IPs are generated using the same criteria; some may simply send spam email, while others may be linked to ransomware activity. Also, there is lack of address space for number of devices because of certain limitations on IPv4 addresses and thus a single public IPv4 address is being shared by multiple users through a concept called NATING (Network Address Translation). So, it is possible that some legitimate users utilizing a domain can be flagged as blacklisted due to some other user having the same public IP address carrying out unintended malicious activity. [4]

II. THREAT INTEL FEEDS

Threat intelligence feeds keep track of continuous sources of real-time threat information, including IoCs (the Indicators of Compromise). They are, however, more than just data or external information on emerging or actual threats and malicious IP vectors which are modified on a regular basis. [5]

Third-party security vendors are typically paid for and provided with private feeds. They are normally created by an organization's internal staff. The majority of the important sources for governmental cyber threat research can be found here. However, end-users are normally given access to public feeds over the internet without paying any substantial cost. It is widely held that in order to achieve the best outcomes, feeds from various sources must be integrated. [6]

Threat intelligence is certainly a valuable investment in any company's security posture since it has considerable advantages. Large-scale analytics are used in Threat Intelligence Feeds, making it far easier for companies to prioritize security threats from various sources in a timely manner. When Threat Intelligence Feeds are incorporated with SIEM applications, the feed entries are automatically compared to internal telemetries like firewall and DNS logs, and warnings are generated for the incident response team. Rather than viewing each feed individually, a successful Threat Intelligence Platform will merge hundreds of them into a single feed. More significantly, a company should keep track of previous threats and accidents, allowing for a more effective counter-threat identification and prevention mechanism. [7]

The following are some of the most widely available public threat intelligence services:

VirusTotal
AbuseIPDB
IPVoid
Threat Intel Feeds
Cisco Talos Intelligence
BrightCloud
MxToolbox

Figure 1: Public Threat Intelligence Feeds

- VirusTotal: It is one of the most widely used and popular threat intel service. Inspects IP/URL with over 80 threat intel feeds for reputation credibility. Also, provides inspection of files for checking if it is malicious or not. Allows end users to integrate their API into the SIEM (Security Information & Event Management) tool to automate the process in real time as data flows through the network.

- IPVoid: Provides the ability to search an IP address against various DNS-based blacklists (DNSBL) and IP reputation services in order to detect IP addresses involved in malware and spamming incidents. This service scans an IP address in real time against more than eighty DNSBL and reputation feeds.

- BrightCloud: The service can detect, analyse, and identify 600,000 new malicious IP addresses and URLs every day by monitoring and dynamically scoring addresses across the entire IPv4 and in-use IPv6 address space.

- MxToolbox: Used to check the IP address of a mail server against over 100 DNS-based email blacklists. (Also known as Realtime blacklist, DNSBL, or RBL.)

- Cisco Talos Intelligence: It provides world's largest and most comprehensive real-time IP and domain reputation service. Categorizes IP traffic based on the geographic location, attack vector type, time of incident and other technical details. File reputation, email & spam protection and malware database are the additional key features of Talos intelligence.

- AbuseIPDB: AbuseIPDB is a project focused on helping the fight against the spread of malware, spams, and the pursuit of abusive behaviour on the Internet. Offers a centralized blacklist for webmasters, server administrators, and other concerned parties to monitor and locate IP addresses linked to malicious internet activity.

III. AUTOMATION FOR TRADITIONAL METHOD

According to a new research, for every 1 hour on the job; security analyst teams waste around 15 minutes on false positive alarms rather than being able to tackle the real findings. Due to lack of automation and integration of automated tools in the environment, security analysts are not able to deal with humongous volume of data. [8]

The conventional method used by many security analyst's teams for identifying IP reputation credibility score is to manually visit public threat intelligence feeds and input one IP address at a time. On an average it takes around 3-5 seconds for an analyst to manually check an IP address for its reputation score. This may sound not a big deal for couple of IP addresses but imagine if an analyst had to check around thousands of IPs in a day, it would be a tedious and less efficient task for a security analyst considering huge volume of data. [9]

The alternative for the conventional method can be achieved by automation of the repetitive tasks. Instead of manually checking each IP on threat intel feed, multiple IP addresses can be given inside a file to the program and get it done in less time. With the help of multi-threading capabilities of CPU, the task can be done in an efficient manner. [10]

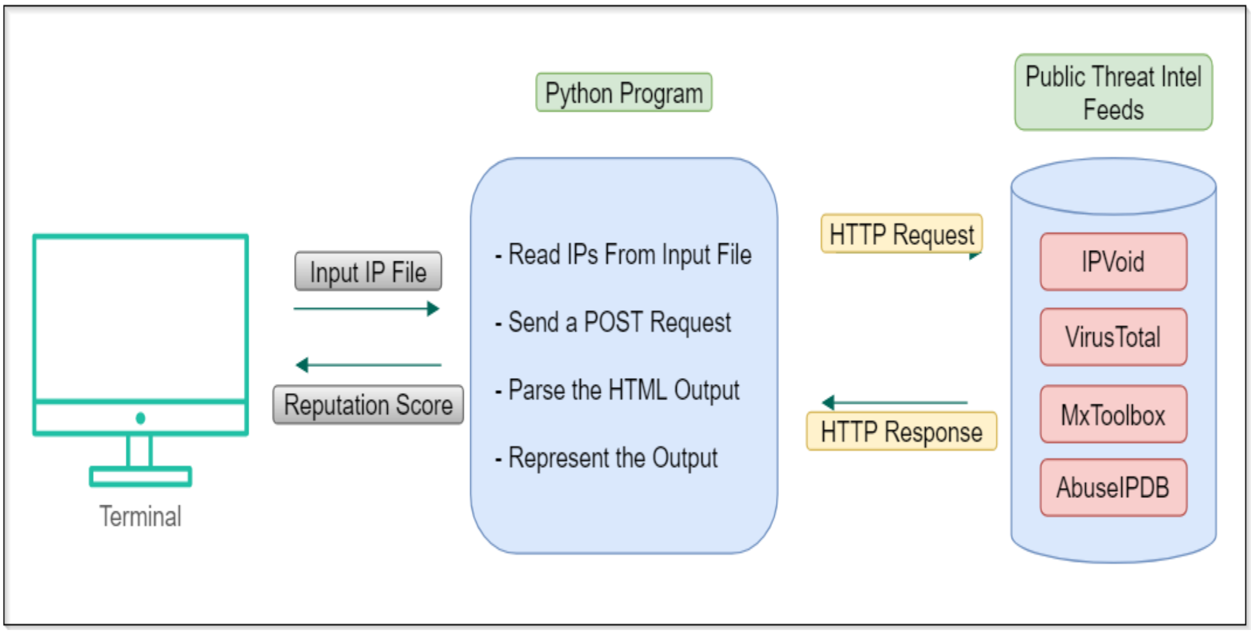


Figure 2: Program Flow Architecture

The proposed automation for identifying IP reputation credibility score can efficiently reduce the huge time spent on manual checks performed by a security analyst. The program is developed in Python language, it parses an input file containing IP addresses before requesting public threat intelligence feeds for their IP reputation endpoint. It scrapes the content from the web page using regex, matching the reputation score field and returns the output to the terminal after receiving a successful HTTP status code. To ensure that the program parses the input file correctly, the analyst must categorize all of the IP's line by line in a text file and pass it as the first argument to the program. [11]

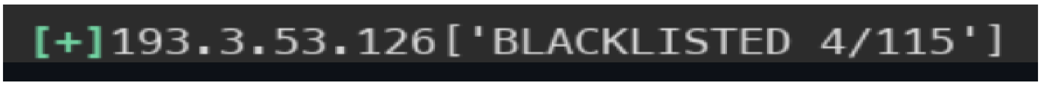
The program returns the blacklisted IP address as well as its threat intel feed-identified credibility score. [12]

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 5, May 2021

DOI 10.17148/IJARCCE.2021.10521



```
[+]193.3.53.126['BLACKLISTED 4/115']
```

Figure 3: Output

IV. CONCLUSION

The aim of this paper is to learn how IP credibility services function, how to find reliable public threat intel feeds, and how to reduce the time spent on manual checks by using an automated software that performs the same tasks as a security analyst. The results show that the developed program is the most efficient way to quickly determine IP reputation scores for multiple IP addresses. [13]

Moreover, relying entirely only on the IP reputation services can be ineffective while carrying out critical security operations, as a result, using entity behavior analytics in conjunction with reputation services would provide a comprehensive security framework. To broaden the scope of this program, multiple private threat intel services can be integrated to provide protection against newly released attack vectors. [14]

REFERENCES

[1] Nighat Usman, Saeeda Usman, Fazlullah Khan, Mian Ahmad Jan, Ahthasham Sajid, Mamoun Alazab, Paul Watters, “Intelligent Dynamic Malware Detection using Machine Learning in IP Reputation for Forensics Data Analytics” in Science Direct Future Generation Computer Systems, Jan 2021.

[2] Abel Yeboah-Ofori, Shareeful Islam, Ezer Yeboah-Boateng, “Cyber Threat Intelligence for Improving Cyber Supply Chain Security” in IEEE 2019 International Conference on Cyber Security and Internet of Things (ICSIoT), Apr 2020.

[3] Jared Lee Lewis, Geanina F. Tambaliuc, Husnu S. Narman, Wook-Sung Yoo, “IP Reputation Analysis of Public Databases and Machine Learning Techniques” in IEEE 2020 International Conference on Computing, Networking and Communications, March 2020.

[4] Arya Renjan, Karuna Pande Joshi, Sandeep Nair Narayanan, and Anupam Joshi, “DAbR: Dynamic Attribute-based Reputation scoring for Malicious IP Address Detection” in IEEE 2018 Intelligence and Security Informatics, Nov 2018.

[5] Ajay Modi, Zhibo Sun, Anupam Panwar, Tejas Khairnar, Ziming Zhao, Adam Doupé, Gail-Joon Ahn, Paul Black, “Towards Automated Threat Intelligence Fusion” in IEEE 2nd International Conference on Collaboration and Internet Computing (CIC), Jan 2017.

[6] Marc Antoine Gosselin-Lavigne, Hugo Gonzalez, Natalia Stakhanova, Ali A. Ghorbani, “A Performance Evaluation of Hash Functions for IP Reputation Lookup Using Bloom Filters” in IEEE 10th International Conference on Availability, Reliability and Security, Oct 2015.

[7] Jernej Porenta, Mojca Ciglarič, “Empirical comparison of IP reputation databases” 8th Annual Collaboration, Electronic messaging, Anti-Abuse and Spam Conference, Sep 2011.

[8] Yoshiro Fukushima, Yoshiaki Hori, Kouichi Sakurai, “Proactive Blacklisting for Malicious Web Sites by Reputation Evaluation Based on Domain and IP Address Registration” in IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, Nov 2011.

[9] Holly Esquivel and Aditya Akella, “On the Effectiveness of IP Reputation for Spam Filtering” in Second International Conference on COMmunication Systems and NETworks (COMSNETS 2010), Jan 2010

[10] Ashley Thomas, “RAPID: Reputation based approach for improving intrusion detection effectiveness” in IEEE Sixth International Conference on Information Assurance and Security, Oct 2010.

[11] Automated Bulk IP Checker [Online] Available: https://github.com/an0ndb9/BulkCh3ck

[12] DNS Whitelist - Protect against false positives, [online] Available: http://www.dnswl.org/