Scamsweep: An Open-Source Toolkit for Online Brand Protection

by

Priyanka Banik

This thesis has been submitted in partial fulfillment for the degree of Master of Science in Cybersecurity

in the
Faculty of Engineering and Science
Department of Computer Science

August 2023

Declaration of Authorship

This report, "Scamsweep: An Open-Source Toolkit for Online Brand Protection", is submitted in partial fulfillment of the requirements of Master of Science in Cybersecurity at Munster Technological University Cork. I, Priyanka Banik, declare that this thesis titled, "Scamsweep: An Open-Source Toolkit for Online Brand Protection" and the work represents substantially the result of my own work except where explicitly indicated in the text. This report may be freely copied and distributed provided the source is explicitly acknowledged. I confirm that:

- This work was done wholly or mainly while in candidature Master of Science in Cybersecurity at Munster Technological University Cork.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at Munster Technological University Cork or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this project report is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: Priyanka Banik

Date: 16/08/2023

MUNSTER TECHNOLOGICAL UNIVERSITY CORK

Abstract

Faculty of Engineering and Science
Department of Computer Science

Master of Science

by Priyanka Banik

The rapid growth of e-commerce has led to an increase in counterfeit products being sold online, causing significant financial losses and reputational damage to brands. This project aims to address this problem by developing an open-source online brand protection toolkit called "Scamsweep" that is capable of detecting counterfeit products across the world-wide web.

The proposed toolkit leverages strategies and techniques from the field of cyber security to identify and analyze counterfeit products across various online platforms such as: social media, e-commerce sites, online playstores and more. The project encompasses several key components, including data collection, web-reconnaissance, domain infringement check, social media monitoring, image processing, trademark violation check, malware analysis, brand risk assessment and incident management.

To enhance the accuracy of the detection process, a risk assessment model is developed to classify suspicious listings based on various features, such as product descriptions, product images, seller profiles and pricing information.

Finally, the tool incorporates Snort rules for incident management to generate insightful alerts, helping brands understand the scope and impact of counterfeiting activities on their reputation and revenue.

The online open-source brand protection tool developed in this project aims to provide an accessible and effective solution for brands of all scales to combat counterfeit products in the digital landscape, irrespective of budget constraints. Its open-source nature encourages collaboration and continuous improvement within the cyber security community.

Acknowledgements

First, I would like to thank my project supervisor, Dr. Brian Murphy, for his unwavering guidance and support throughout this journey. Thank you for taking the time to meet face-to-face on campus to resolve my doubts and for answering my emails with detailed reviews and comments.

Sincere thanks to my second reader Dr. Kapal Dev for providing a feedback on this project.

I would like to express my gratitude to Dr. Saqib Rasool Chaudhry and Dr. Anila Mjeda for acquainting me with the captivating realm of Incident Response, Digital Forensics and Malware Analysis. I want to acknowledge the direct application of their module teachings from "COMP9038_25942 - Incident Response & Forensics" and "COMP9047 - Malware Investigations" in shaping various aspects of this project.

I wish to credit my peers Ms. Shraddha Shelar and Mr. Sayantan Chowdhury for being incredibly helpful with my Python related queries. I acquired a wealth of new knowledge through our collaboration and will forever cherish our shared accomplishments.

I would also like to acknowledge the support and resources provided by Munster Technological University throughout the research process. Special thanks to the librarians of MTU for helping me find good books in the field of security governance, risk and compliance and issuing them for me.

I extend my gratitude to our course coordinator, Mr. Vincent Ryan for his significant contributions to MTU's Cybersecurity program and the delivery of the final year project module.

Furthermore, I would like to express gratitude to the professionals and authorities, who's papers and articles available on Google Scholar gave insightful information. Their knowledge-sharing abilities and experience have been crucial in raising the quality and reliability of this project.

Lastly, I want to thank my family and friends for their constant support and understanding during the completion of this project. Their encouragement and belief in my abilities have been vital in overcoming challenges and reaching the finish line.

While it is not possible to individually name everyone who has contributed, I sincerely thank each and every person who has played a part, no matter how small, in the completion of this project. Your support has been invaluable and I am truly grateful.

Contents

List of Figures

List of Tables

Abbreviations

AI	**A**rtificial **I**ntelligence
API	**A**pplication **P**rogramming **I**nterface
APK	**A**ndroid **P**ackage **K**it
ASIN	**A**mazon **S**tandard **I**dentification **N**umber
ATT&CK	**A**dversarial **T**actics **T**echniques and **C**ommon **K**nowledge
CPU	**C**entral **P**rocessing **U**nit
CSF	**Cyber Security Framework**
CSV	**C**omma **S**eparated **V**alues
DBMS	**D**atabase **M**anagement **S**ystem
DGA	**D**omain **G**eneration **A**lgorithms
DKIM	**D**omain **K**eys **I**dentified **M**ail
DLT	**D**istributed **L**edger **T**echnologies
DMARC	**D**omain-based **M**essage **A**uthentication, **R**eporting and **C**onformance
EU	**E**uropean
Union	
FAIR	**F**actor **A**nalysis of **I**nformation **R**isk
GB	**G**iga **B**ytes
	GDPR
General	**D**ata
Protection R	

egulation

GUI **G**raphical **U**ser **I**nterface

HTML **H**yper **T**ext **M**arkup **L**anguage

HTTP **H**ypertext **T**ransfer **P**rotocol

ICANN **I**nternet **C**orporation for **A**ssigned **N**ames and **N**umbers

IDS **I**ntrusion **D**etection **S**ystem

IOC **I**ndicators **O**f **C**ompromise

IoT **I**nternet **o**f **T**hings

IP **I**nternet **P**rotocol

ISO **I**nternational **O**rganization for **S**tandardization

JPEG **J**oint **P**hotographic **E**xperts **G**roup

JSON **J**ava **S**cript **O**bject **N**otation

MSDN **M**icro**S**oft **D**eveloper **N**etwork

NIST **N**ational **I**nstitute of **S**tandards and **T**echnology

NLP **N**atural **L**anguage **P**rocessing

OS **O**perating **S**ystem

OSINT **O**pen **S**ource **I**ntelligence

PoC **P**roof **o**f **C**oncept

PNG **P**ortable **N**etwork **G**raphics

QR **Q**uick **R**esponse

RAM **R**andom **A**ccess **M**emory

RFID **R**adio **F**requency **I**dentification

RMF **R**isk **M**anagement **F**ramework

SIEM **S**ecurity **I**nformation and **E**vent **M**anagement

SLA **S**ervice **L**evel **A**greement

SMTP **S**imple **M**ail **T**ransfer **P**rotocol

SPF **S**ender **P**olicy **F**ramework

SSL **S**ecure **S**ocket **L**ayer

SQL **S**tructured **Q**uery **L**anguage

TLD **T**op **L**evel **D**omain

TLS **T**ransport **L**ayer **S**ecurity

TOR **T**he **O**nion **R**outer

TTP **T**actics, **T**echniques and **P**rocedures

URL **U**niform **R**esource **L**ocator

VaR **V**alue **a**t **R**isk

VM **V**irtual **M**achine

WFH **W**ork **F**rom **H**ome

WTO **W**orld **T**rade **O**rganization

This thesis is dedicated to my loving parents. Thanks for always believing in my abilities and wholeheartedly supporting my decision to move outside India for pursuing my Master's degree in Cyber Security. Papa and Mummy, you inspire me everyday to become a better version of myself...

Chapter 1

Introduction

This project seeks to counter a unique cyber attack, known as "Brandjacking". Brandjacking refers to the malicious practice of using a well-known brand's name, logo or other distinctive elements without authorization to deceive and defraud consumers [1]. This can involve creating fake websites, social media profiles or advertisements that mimic the legitimate brand's appearance. The goal of brandjacking is often to trick customers into sharing sensitive information, making unauthorized purchases or engaging in other harmful activities. It undermines consumer trust, damages brand reputation and poses significant legal and financial risks to the targeted brand.

Preventing and addressing brandjacking requires proactive online brand protection measures and rapid responses to mitigate its impact. Online brand protection encompasses a suite of strategies and measures aimed at safeguarding a company's reputation, intellectual property and consumer trust in the virtual realm. This project delves into the pivotal role of online brand protection in mitigating risks, preserving brand integrity and ensuring sustained growth through an open-source toolkit named "Scamsweep". The toolkit is typically used to identify threats to various brands by performing activities such as: data collection, web-reconnaissance, URL analysis, text analysis, image processing, social media monitoring, malware reverse engineering, brand risk assessment, alert creation and taking down the detected Indicators Of Compromise (IOC) pertaining to the brand being investigated.

1.1 Motivation

The growth of internet has led many enterprises to take their business online. This change in paradigm accelerated during the COVID-19 pandemic, where people were

forced to shift to a remote working module. The pandemic also changed online shopping behaviour (refer Figure 1.1) by increasing the percentage of online sale under every product category by 6 to 10 percentage points [2]. With the proliferation of digital transformation, as more data becomes available on the web, cybercriminals find new sophisticated ways to breach the data. Majority of these cyber attacks have a motive of financial gain. One such way of making money illegally is by using the intellectual assets of a reputed organisation to create counterfeit products of inferior quality and selling them at a cheaper price. In other words, abusing the keywords, logos, trademarks and copyrights that define brand value of the organization. Most companies are unaware that their brand is being abused unless notified by an unhappy customer. This not only leads to revenue leakage, but also leads to loss of brand reputation alongside legal consequences.

FIGURE 1.1: Percentage of online shoppers making at least one online purchase every two months [2]

Another pain point to be addressed is the high pricing of the current existing solutions available in the market. Small scale organizations that do not have the budget to buy these expensive tools tend to work internally to mitigate customer escalations. The aim of this project is to come up with toolkit leveraging open-source intelligence that would help such organizations run proof-of-concepts to assess the threats to their brands and also evaluate the risks to their attack surface beyond the security perimeters of the organization. The name proposed for the toolkit is "Scamsweep". Such an assessment using the Scamsweep toolkit could prove to be beneficial before investing in a commercial solution with more advanced features for online brand protection.

Overall, this project is relevant for every online brand protection focused individual - be it at the brand owner or a vendor-side trusted advisor. It is meant to be pertinent to any individual with an interest in safeguarding the revenue, security and reputation of

any online business and its consumers. It outlines the key areas of importance for those creating a strong online intellectual property and brand protection plan. The project offers an informative breakdown of each area of infringement by providing information on the tactics and techniques used by cybercriminals to impersonate a brand. It gives an overview of brand protection methods and strategies implemented to detect and mitigate the threats and set the standards for best practice concerning a reputed brand name.

1.2 Contribution

This section consists of 3 segments: one focusing on the research area of the project and the other concentrating on project goals and their corresponding deliverables.

1.2.1 Research Area

Using open-source tools to evaluate the need for brand protection in an online commercial setup is the main area of research in this project. Various data collection methods are performed systematically to build a profile of a company that requires a brand protection strategy to prevent loss of revenue and reputation. This project takes a look at how to leverage open-source intelligence tools to crawl through the internet and gather indicators pertaining to the online presence of a company. Several tools and techniques shall be analysed to perform activities such as: active web scanning or reconnaissance, URL analysis, IP reputation validation, image processing for distinguishing real and counterfeit logos, content analysis (detecting similar marketing keywords, trademarked descriptions), malware reverse engineering and others to check whether the particular brand being investigated has been infringed.

1.2.2 Project Goals

1. Perform market research and do a case study on an organisation, which has been impacted severely due to brand abuse.

2. Build a database containing list of digital assets of a brand such as: designs, logos, trademarks, copyrights, domain names, IP addresses, social media accounts, applications available on App-store, authorised resellers on online marketplaces, marketing keywords, descriptors and other details.

3. Experiment with open-source tools and technologies in a reasonable and efficient manner to gather intelligence associated to the brand being investigated.

4. Research and develop a Python script that conducts text analysis to compare strings for identifying trademark infringements by brand abusers.

5. Research and develop a Python script that conducts image processing to distinguish between real and counterfeit logos being used by brand abusers.

6. Analyse the Indicators of Compromise (IOC) detected through investigation methods like URL analysis, IP or domain reputation analysis, trademark analysis, social media engagement analysis and malware reverse engineering.

7. Allocate a risk rating (High, Medium, Tolerable, Low) to the threats posed on a brand to prioritise enforcement in case the issue identified is critical and the volume of brand abuse incidents for the target brand or company is too high.

8. Send an alert with appropriate message on detecting a true positive event by capturing the metadata for brand abuse in real-time.

9. Analyse and compare the investigation results obtained from these open-source tools with commercial solutions to arrive at a conclusion whether the target brand has been infringed or not.

1.2.3 Research Questions

1. Can open-source tools be used to deliver actionable intelligence and enforcement solutions pertaining to online brand management?

2. What method would be used to collect data such as: logos, marketing keywords, trademarks, copyrights, description or any form of intellectual property that defines a particular brand name?

3. How to build a risk register with a logical metric system that would allocate a threat score to an incident pertaining to brand abuse?

4. Are there any limitations on what can or should be automated while developing a brand protection strategy?

5. Are pre-existing solutions in the market suitable for online brand protection or is there more work to be done?

1.2.4 Deliverables

1. Case study on any company that has been a victim of brand abuse on public domain.

2. Data inventory of legitimate digital assets of a brand such as: designs, logos, trademarks, copyrights, domain names, IP addresses, social media accounts, applications available on App-store, authorised resellers on online marketplaces, marketing keywords, descriptors and others details.

3. Reconnaissance results containing domains, sub-domains and their corresponding IP addresses for the brand under investigation. The volume of data generated in the reconnaissance phase is significantly high.

4. Domain analysis capability to investigate malicious URLs, domains and IP addresses.

5. Python script capable of conducting text analysis.

6. Image processing capability to differentiate between real and fake images. This deliverable shall be met by developing a Python script.

7. List of suspicious social media accounts associated with the target brand name and a open-source tool to calculate the user engagement metrics pertaining to the identified fake accounts.

8. Sandbox environment to conduct malware analysis on detecting malicious applications impersonating the target brand.

9. Risk register containing security scores and risk ratings (High, Medium, Tolerable and Low) tagged with every threat detection.

10. Snort rule to generate alerts with appropriate messages for customers on detecting a true positive event of brand abuse in real-time.

1.3 Structure of This Document

Chapter 1 - Introduction: This chapter introduces the project.

- **1.1 Motivation:** This section outlines the driving forces that inspire the pursuit of this research.
- **1.2 Contribution:** Section 1.2 elaborates on the valuable contributions made by this research endeavour.

  1.2.1 Research Area: Within this sub-section, the specific research domain is discussed.

1.2.2 Project Goals: Sub-section 1.2.2 expounds on the overarching goals of the project.

1.2.3 Research Questions: This sub-section highlights the pivotal research questions addressed in the project.

1.2.4 Deliverables: The anticipated outcomes and deliverables of the research are detailed in this sub-section.

- **1.3 Structure of This Document:** This section provides an overview of the document's organization and structure.

Chapter 2 - Literature Review: This chapter presents a summary of background research conducted to develop an open-source online brand protection toolkit, i.e., Scamsweep.

- **2.1 Need for Online Brand Protection:** This section highlights the critical importance of safeguarding brands within the digital realm.
- **2.2 Online Brand Abuse Tactics:** Within this section, the various tactics employed to exploit brands in cyberspace are examined.

  2.2.1 Trademark and Copyright Infringements: Sub-section 2.2.1 focuses on the abuse of trademarks and copyrights within the online sphere.

  2.2.2 Domain Name Infringements: Sub-section 2.2.2 delves into the misuse of domain names as a form of brand abuse.

  2.2.3 Counterfeit Products in Online Marketplaces: This sub-section explores the presence of counterfeit goods in digital marketplaces.

  2.2.4 Social Media Impersonations: Within sub-section 2.2.4, the act of impersonating brands on social media is discussed.

  2.2.5 Rogue Mobile Applications: This sub-section sheds light on the threats posed by rogue mobile applications.

- **2.3 Data Collection using Kaggle's Repository of Simulated Datasets:** Section 2.3 focuses on data collection methods involving Kaggle's simulated datasets.
- **2.4 Effective Methods of Mitigating Online Brand Abuse:** This section reviews strategies to effectively combat online brand abuse.

  2.4.1 Detecting Fraudulent Websites Using an Anti-Phishing Model: Sub-section 2.4.1 examines the use of anti-phishing models to identify fraudulent websites.

2.4.2 Reconnaissance Using Open-Source Intelligence Tools: Sub-section 2.4.2 explores the application of open-source intelligence tools for reconnaissance.

2.4.3 Developing a Statistical Model to Detect Counterfeit Logos: Sub-section 2.4.3 focuses on creating statistical models to identify counterfeit logos.

2.4.4 TinEye: The role of TinEye in brand protection and reverse image search is explored in this sub-section.

2.4.5 Identifying Trademark Infringements Using Gerben Trademark Library: Sub-section 2.4.5 discusses the use of Gerben Trademark Library for identifying trademark infringements.

2.4.6 Marcaria: This sub-section examines the significance of Marcaria in detecting trademark abuse.

2.4.7 Phlanx's User Engagement Calculator for Social Media Analytics: Sub-section 2.4.7 reviews the use of Phlanx's User Engagement calculator for analysing the social media activity of an account.

2.4.8 Reverse Engineering of Malicious Applications: This sub-section explores the practice of reverse engineering malicious applications.

2.4.9 Alert Generation or Rule Creation Using Snort: Sub-section 2.4.9 discusses the generation of alerts or rules using the Snort tool.

- **2.5 Risk Analysis in Online Brand Management:** This section delves into risk analysis methodologies within online brand management.

  2.5.1 Risk Management Frameworks: The role of risk management frameworks is explored in this sub-section.

  2.5.2 ISO 31000: ISO 31000's contribution in risk management is examined within this sub-section.

  2.5.3 NIST RMF: Sub-section 2.5.3 discusses the significance of NIST RMF in risk analysis.

  2.5.4 FAIR: The relevance of FAIR framework in risk analysis is highlighted in this sub-section.

  2.5.5 MITRE ATT&CK Framework: Sub-section 2.5.5 focuses on the role of the MITRE ATT&CK Framework in risk analysis.

  2.5.6 Risk Assessment Plan: This sub-section outlines a risk assessment plan, including methodologies and risk matrix models.

- **2.6 Current Existing Solutions in the Market:** This section reviews current solutions available in the market for online brand protection.

2.6.1 ZeroFOX: Sub-section 2.6.1 examines the features and capabilities of the ZeroFOX platform.

2.6.2 RiskIQ: The RiskIQ platform's offerings are discussed within this sub-section.

2.6.3 BrandShield: Sub-section 2.6.3 focuses on the contributions of the BrandShield platform in brand protection.

2.6.4 Comparative Analysis: ZeroFOX vs RiskIQ vs BrandShield: This sub-section conducts a comparative analysis of ZeroFOX, RiskIQ and BrandShield.

- **2.7 Conclusion:** This section encapsulates the key insights drawn from the literature review.

Chapter 3 - Design: This chapter focuses on the design, architecture and overall workflow of Scamsweep.

- **3.1 Problem Definition:** This section is a clear articulation of the project's core challenges to be addressed comprehensively.
- **3.2 Objectives:** This section states the goals guiding the project's purpose, ensuring focused and meaningful outcomes.
- **3.3 Requirements:** This section states essential conditions for shaping the project scope and development of direction for effective implementation.

  3.3.1 Functional Requirements: This sub-section highlights the key operational specifications defining project functionality and user interactions.

  3.3.2 Non-functional Requirements: This sub-section highlights the vital quality and performance expectations ensuring user satisfaction and system reliability.

- **3.4 Architecture Diagram of Scamsweep:** This section is a detailed blueprint illustrating optimal arrangement and functionality of project workflow both on front-end and back-end.

Chapter 4 - Implementation: This chapter focuses on implementation lifecycle of Scamsweep.

- **4.1 Important Features: Executing the Vision** This section discusses the implementation process of important features or capabilities of Scamsweep. It

also highlights the challenges faced during implementation, the impact of those challenges on the project and the steps followed for successful implementation of Scamsweep.

4.1.1 Data Collection: This sub-section is on compilation of a company's intellectual property assets through comprehensive data gathering techniques.

4.1.2 Web-reconnaissance: This sub-section is on thorough scanning of the internet to identify and create a list of suspicious domain names.

4.1.3 URL Analysis: This sub-section is on evaluation of domain or IP address reputation to assess potential risks.

4.1.4 Text Analysis: This sub-section is on utilization of various methods for string comparison and analysis in a Python script to detect trademark infringements.

4.1.5 Image Processing: This sub-section is on using a Python script to discriminate between authentic and counterfeit logos through computer vision and image analysis techniques.

4.1.6 Social Media Analysis: This sub-section is on computation of user engagement ratio on diverse social media platforms.

4.1.7 Malware Analysis: This sub-section is on in-depth study involving reverse engineering of suspicious applications.

4.1.8 Risk Assessment: This sub-section is on development of a robust framework for comprehensive risk analysis critical to brands.

4.1.9 Alert Generation: This sub-section is on implementation of Snort rules to trigger alerts for potential security breaches.

Chapter 5 - Testing and Evaluation: This chapter focuses on the testing and quantitative evaluation of features implemented in Scamsweep.

- **5.1 Use Case 1:** This section focuses on testing of Data Collection feature of Scamsweep.

  5.1.1 Test Case 1.0: This sub-section assesses Kaggle's efficiency for Nike's logo collection.

  5.1.2 Test Case 1.1: This sub-section assesses Gerben Trademark Library's suitability for gathering Nike's trademarks.

- **5.2 Use Case 2:** This section focuses on testing of Web-Reconnaissance feature of Scamsweep.

5.2.1 Test Case 2.0: This sub-section evaluates Maltego Community Edition 4.3.1 for web-reconnaissance.

5.2.2 Test Case 2.1: This sub-section tests OTX Alienvault's performance in conducting web-reconnaissance.

5.2.3 Test Case 2.2: This sub-section assesses Microsoft Defender Threat Intelligence's efficiency for web reconnaissance.

5.2.4 Test Case 2.3: This sub-section assesses Recon-ng's performance in conducting web-reconnaissance.

- **5.3 Use Case 3:** This section focuses on testing of Domain Infringements feature of Scamsweep.

  5.3.1 Test Case 3.0: This sub-section tests Nike's URL using URLScan.io.

  5.3.2 Test Case 3.1: This sub-section reviews Cisco Talos Intelligence for Nike's IP/domain reputation.

- **5.4 Use Case 4:** This section focuses on testing of Trademark Infringements feature of Scamsweep.

  5.4.1 Test Case 4.0: This sub-section tests trademark_infringement.py Python Script on Google Colab.

- **5.5 Use Case 5:** This section focuses on testing of Image Processing feature of Scamsweep.

  5.5.1 Test Case 5.0: This sub-section evaluates counterfeit_logo_detection.py Python Script on Google Colab.

- **5.6 Use Case 6:** This section focuses on testing of Social Media Monitoring feature of Scamsweep.

  5.6.1 Test Case 6.0: This sub-section evaluates Phlanx's User Engagement Calculator for analysing suspicious Nike Instagram accounts.

- **5.7 Use Case 7:** This section focuses on testing of Rogue Applications feature of Scamsweep.

  5.7.1 Test Case 7.0: This sub-section evaluates HashCalc's utility in analyzing rogue applications.

  5.7.2 Test Case 7.1: This sub-section evaluates PEStudio examination for analyzing suspicious applications.

- **5.8 Use Case 8:** This section focuses on testing of Brand Risk Assessment feature of Scamsweep.

5.8.1 Test Case 8.0: This sub-section examines the applicability of the developed customised Risk Assessment Framework for Scamsweep.

- **5.9 Use Case 9:** This section focuses on testing of Alert Generation feature of Scamsweep.

  5.9.1 Test Case 9.0: This sub-section tests the developed Snort rules for alert generation.

Chapter 6 - Discussions and Conclusion: This chapter constitutes a fundamental analysis of the efforts invested in this project. It succinctly presents the degree to which the research objectives and inquiries were achieved or addressed.

- **6.1 Discussion:** This section is a critical discussion on the degree to which the project solution aptly tackles the predefined challenges.
- **6.2 Conclusion:** This section gives an overall conclusion on all the chapters discussed in this document.
- **6.3 Future Work:** The section is a discussion on the future scope of work to enhance the proposed solution.

Bibliography: This chapter gives a list of references of all the research papers, articles, blogs, books and journals that have helped in conducting the research for this project. There are 94 references in total and the referencing style used is IEEE.

Appendices: This is an additional chapter consisting of 4 sections given below:

- **Appendix A:** This section showcases a case study on Nike, i.e., target brand for testing of Scamsweep.
- **Appendix B:** This section showcases 2 Python scripts developed during the implementation phase of this project. One for detecting trademark infringements and the other for differentiating between real and fake brand logos.
- **Appendix C:** This section showcases the Linux commands and their corresponding outputs generated while running the Recon-ng tool for performing reconnaissance.
- **Appendix D:** This section showcases incident management, i.e., initiation of takedown process on determining a high level risk. It also includes a sample email template that can be edited and sent to client, when reporting the findings of Scamsweep.

-

Chapter 2

Literature Review

This chapter aids in ascertaining the fundamental comprehension of the project being carried out and fosters trust in the general calibre of the results and analysis. It is vital to look at the following four research areas to build an understanding of how the project implementation should be done:

- Need for Online Brand Protection
- Online Brand Abuse Tactics
- Effective Methods of Mitigating Online Brand Abuse
- Current Existing Solutions in the Market

These sections are not examined in isolation since there is opportunity for additional research, particularly in relation to particular facets of threat intelligence, incident detection, response and risk management.

2.1 Need for Online Brand Protection

The acceleration of digital innovation has led to rapid adoption of internet-enabled devices that hangs as a double-edged sword over the cyber security threat landscape [3]. As companies pursue digital transformation to compete, they expose more of their business to potential cyber risk and disruption. The problem is that for every new technology being deployed in the business world, i.e., Artificial Intelligence (AI), Internet of Things (IoT), Distributed Ledger Technology (DLT) and Cloud Computing, the threats associated with these emerging technologies are also evolving. The tactics and techniques

used by cybercriminals to facilitate attacks have reached a level of sophistication as never seen before [4].

The COVID-19 pandemic forced organizations to shift to a remote working module introducing new attack vectors. Both businesses and consumers started providing and purchasing their goods and services online leading to growth of trade via e-commerce. According to Forbes, "E-commerce jumped 55% during COVID to hit $1.7 trillion" [5]. While this was a good way to counter the economic downturn, it came with its own set of challenges. The facilitation of Work-From-Home (WFH) arrangement and online businesses has only broadened the attack surface of an organization. The paper "Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19" [6] critically analyses "changes in offline and online routine activities are associated with a shift in crime opportunities from physical space to cyberspace (Miró-Linares & Moneva, 2019; Newman & Clarke, 2003; Pyrooz et al., 2015)" [6]. The attack surface of an organization is no longer restricted to its network security perimeters. Therefore, only strengthening the defences and monitoring the internal environment of an organisation is not sufficient to cease online scams.

With the acceleration of digital transformation, cyber criminals now have access to the digital footprints and assets of an organization floating free on the world-wide web. The paper [6] also describes the "fraud attributable to the misrepresentation of a product advertised for sale through an internet auction site" [6]. The brand of an organization is its most valuable asset. It leaves a strong message about the vision and mission of the organization and gives a clear understanding of what the product of that company is all about. "Shopping online has been identified as a potential predictor of online fraud victimization (e.g., Leukfeldt & Yar, 2016; Reyns & Henson, 2016)" [6]. Therefore, with the proliferation of Internet and acceleration of online shopping, the brand name becomes an attractive target for threat actors trying to misuse it for monetary gains or obtaining sensitive information. Infringing the intellectual property by imitating a company's logo and trademark, selling counterfeit products on e-commerce platforms at cheaper price, impersonating an executive on social media are few examples of external threats that goes beyond the scope of the firewall. The negative impact of such online scams on businesses includes, but not limited to: revenue leaks, reputation loss and legal liabilities [6]. With this comes the need for an online brand protection solution that proactively detects and eliminates the attack vectors associated with the brand value and reputation of an organization on cyberspace.

2.2 Online Brand Abuse Tactics

Brand Abuse also known as "brand exploitation" or "brandjacking" is an umbrella term often used to describe a third party who violates a brand's intellectual property in an effort to profit from its reputable image. In cybersecurity, brand abuse is a very complicated, yet a frequent problem [7]. Many brands are unaware that they are being exploited and have no idea that their brand name and intellectual property rights are being exploited illegally.

The paper "Online Social Networks Misuse, Cyber Crimes, and Counter Mechanisms" [7] presents a systematic review of "malicious users and third-party apps to perform various kind for cyber-crimes like social engineering attacks, cyber espionage, extortion-malware, drug-trafficking, misinformation, cyberbullying, hijacking clicks, identity theft, phishing, mistrusts, fake profiles, and spreading malicious content" [7]. This sub-section describes various online brand abuse tactics and techniques commonly used by cyber criminals to damage the brand reputation of an organization, i.e., Domain Name Infringements, Trademark and Copyright Infringements, Counterfeit Products in Online Marketplaces, Social Media Frauds, Rogue Mobile Applications and Executive Impersonations. There are other possible fraudulent techniques used by cybercriminals, such as: unauthorised product sale on the Dark Web, which lies outside the present scope of this project.

2.2.1 Trademark and Copyright Infringements

Any word, phrase, symbol, design or combination of these that distinguishes the products or services might be considered a trademark. Customers use it to recognize a branded product or service in the marketplace to set it apart from its competitors present in the commercial industry. Copyright is defined as "a form of intellectual property protection" [8] in the paper "Criminal Copyright Infringement and the Copyright Felony Act" which is wilfully infringed "for the purpose of commercial advantage or private financial gain" [8]. When copyright is asserted in a trademark, it may be shown using the internationally recognized copyright symbol © and infringement of this symbol is treated as counterfeiting or piracy, thereby imposing sanctions.

Cybercriminals imitate the logos, symbols, slogans and misuse the marketing keywords of a reputed brand to give a legitimate look and feel to their counterfeit products in the digital marketplace. There is an immediate need for an online solution that monitors such infringements to protect the intellectual property rights and brand value of the victim organization.

2.2.2 Domain Name Infringements

When using client software to access a website, a domain name is a textual phrase that corresponds to an alphanumeric Internet Protocol (IP) address. In simple terms, text that a user types into a browser window to access a certain website is known as the domain name [9]. The process of purchasing and reserving a name on the internet through a domain name registrar, such as: Google Domains or Domain.com, is known as domain name registration. When a person or company uses a domain name that is registered under someone else's trademark, they are engaging in domain name infringement.

It is possible to find out who owns a domain and how to contact them using the widely used Internet record listing tool known as Whois. This database of domain name registration and ownership is regulated by Internet Corporation for Assigned Names and Numbers (ICANN). The purpose of Whois as described in paper "The who, what, where, when, and why of Whois: Privacy and accuracy concerns of the Whois database" is to help both businesses and consumers research on the availability of a particular domain to purchase or determine the owner of that domain [10]. Domain name registrars are responsible for collecting valid data, but registrants do not always provide accurate and complete contact information. Giving incorrect information allows domain name registrants to remain untraceable by law and government entities while committing crimes via the Internet [10].

The most frequent and alarming form of domain infringement is cybersquatting. No clear, universal definition of cybersquatting exists. Although no definite, single definition of cybersquatting exists, but it occurs when someone registers a domain name with the intent of selling it, thus prohibiting the legitimate trademark holder from using the name or tries to divert traffic by redirecting visitors away from the trademark holder's website. To understand the concept of internet traffic redirection better, the anatomy of a hypothetical Uniform Resource Locator (URL) "https://mail.scamsweep.com/ssmail" is studied.

As shown in Figure 2.1, "scamsweep.com" is the domain name and "mail.scamsweep.com" is the sub-domain. Everything that follows the dot after a domain name is referred to as the Top Level Domain (TLD) as this is installed in the root zone of the domain name space. Here, ".com" is the TLD. It is more likely for a URL to break trademark rules if another company's trademark appears before the slash than if it is in the URL's post-domain path (the text that comes after the slash) [11]. For instance, it would be illegal if another business registered a domain for commercial gain using the name Scamsweep, which is a trademark of that business, i.e., www.scamsweep.com. A trademark may not be illegally used if it is present in the post-domain route of a URL [11], such as

www.scamprotect.com/scamsweep because it still re-directs to the original website, i.e., www.scamsweep.com.

FIGURE 2.1: Anatomy of URL

Threat actors create fake websites hosting the copyrights, trademarks and other intellectual properties, i.e., logos, images, marketing keywords of a reputable organization to attract consumers. For a product-based company, they use these illegal domains as a means to sell counterfeit products leading to major risks such as: revenue loss, distribution relation crisis, grey market flood, brand reputation loss, brand reputation loss, data leakage and legal liabilities.

2.2.3 Counterfeit Products in Online Marketplaces

In discussions of international trade, the grey market has been defined as a parallel market [12]. The paper "What is Grey about the Grey Market?" [12] discusses that "parallel markets are not illegal, but the objects they move are unauthorised for sale in a particular jurisdiction by their manufacturers, who have developed different versions of the product for different global markets" [12].

There are over 5000+ e-commerce platforms worldwide processing close to 30 million listings per day [13]. Amazon, eBay, Alibaba, Shopee are some of the most indispensable marketplaces in the industry.

The paper "From Amazon's Domination of E-Commerce to its Foray into Patent Litigation: Will Amazon succeed as The District of Amazon Federal Court?" [14] conducted a study of 10 websites where Amazon stands fourth in the rank of sales of counterfeit products. As a result of Amazon's counterfeit product problem, the company is encountering several lawsuits from brands and consumers who believe that the company should be held liable for not taking the necessary measures to eliminate counterfeit products from its website. The counterfeit products are not only an inferior version of the authentic

counterpart creating health and safety risk to consumers, but are also a violation of the intellectual property rights of a legitimate seller or manufacturer [14].

In May 2017, Amazon launched its Brand Registry Program as its first attempt in curbing the sale of counterfeit products. In order to register with Amazon, brands must provide a government-registered trademark number, a list of product categories, and a list of nations where their products are produced and marketed. An Amazon Standard Identification Number (or "ASIN") will be given to a brand once it has been verified and given the go-ahead by Amazon. The ASIN can then be assigned by brands to each product unit they produce, and Amazon will utilize this code to verify the products during the company's product fulfilment and shipment process. Investigators from Amazon will react and take action if they discover a probable violation. Currently, Brand Registry has more than 60,000 registered brands, and these brands report 99% fewer suspected infringements than they did before Brand Registry was introduced [14].

In February 2019, Project Zero emerged as the company's second attempt at eradicating counterfeit listings. Through a self-service counterfeit takedown tool, Project Zero gives brand owners the ability to instantly remove fake listings without having to get in touch with Amazon. In addition, Project Zero makes proactive use of machine learning to automatically search the Marketplace for potential counterfeit items and delete them without the involvement of brand owners [14].

Although Brand Registry and Project Zero have successfully eliminated counterfeit products using machine learning to identify them as such, the speed at which these listings are taken down is insufficient to protect brands from infringement given how quickly counterfeiters can open a new Amazon account, produce and market counterfeits online. Therefore, to protect businesses from such online scams, it is essential for victim organizations to have its own online brand protection tool that is integrated with the security solution like Security Information and Event Management (SIEM) or any ticketing tool, which would not only detect brand infringements, but also send alerts to security analysts to take further action as per the defined Service-Level Agreement (SLA). One such tool that is capable of integrating its Application Programming Interface (API) with a SIEM solution is an Israeli product named BrandShield [15].

2.2.4 Social Media Impersonations

Impersonation occurs when users create social media accounts that mimic authentic accounts, often with malicious intent. For instance, imposters or impersonators may create profiles that pose as well-known individuals or representatives of well-known brands, businesses, etc. These impersonators are widespread throughout all significant social

media networks [15]. Instagram is widely used by celebrities, influencers, businesses and public figures of all popularity levels. Although many impersonators could be harmless, there are also phony identities that are intentionally malicious. These frequently have well-defined strategies, including making accounts appear to be more popular than they actually are, producing pre-planned unreliable content, abusing brands or creating phony engagements.

Personal employee, customer accounts, official C-Level pages or sales or communication channels on corporate pages with clients, suppliers and partners are all potential victims of social fraud [15]. Social scams are challenging to spot and guard against because of sophisticated social engineering and the widespread trust in social media. Hence it is important to monitor social media platforms for C-level impersonation or phishing accounts and delete them before they can be used to trick workers into giving personal or sensitive information, like login credentials of a corporate network or to give a partner new fake payment information or even to instigate any controversy on any executive's name. Here are some common use cases listed below:

- Consumer Facing Phishing
- Employee Facing Phishing
- Executive Impersonation
- Online Fraud

The paper "Impersonation on Social Media: A Deep Neural Approach to Identify Ingenuine Content" [16] compares a legitimate user profile with its corresponding fake account through deep neural network approach to segregate the imposters into two categories, i.e., fans and bots. For example, there are many social media handles for the famous football player Christiano Ronaldo. Only one of these accounts is a verified one that originally belongs to him. Rest of the accounts are mostly created by his fan followers who support him and mean no harm. However, some of these accounts are created by bots with a malicious intent of propagating misinformation. Although this data engineering methodology is efficient is detecting the imposters, the disadvantage of this approach lies in the manual validation of accounts before arriving at a solid conclusion [16].

2.2.5 Rogue Mobile Applications

Mobile applications known as "Rogue apps" are created to spoof well-known businesses to obtain illegal access to data that may be used to carry out fraudulent operations.

These dangerous apps have the ability to set up malware, ransomware or fool users into giving attackers their financial information.

The dissertation "Rogue apps, hidden web tracking and ubiquitous sensors" examines the privacy risks posed by embedded sensors, web tracking, and mobile apps [17]. An undercover investigation is presented, probing whether app vendors comply with transparency obligations prescribed by EU's (European Union) General Data Protection Regulation (GDPR). It contributes to the academic discussion and scientific literature regarding potential privacy threats coming from consumer devices and highlights how inadequate the current legal framework is to safeguard our privacy. The privacy concerns associated with rogue apps are discussed further by concentrating on fake transport applications available on Google or Apple Playstore for booking cabs or taxis online in the paper "Rogue Smartphone Applications for Taxicabs and Limousines: Innovation or Unfair Competition?" [18]. This paper throws light on how threat actors use counterfeit apps to charge unfair fairs, sell the user data on dark-web, refuse services after taking the money from customers and impose an overall threat to the physical security of the customer due to lack of proper regulation. Such cases not only abuse the brand integrity of the victim organization but also threatens consumer protection rights. For companies like Uber, FreeNow and others it is extremely important to monitor the App Store and takedown fake mobile applications to avoid penalties due to breach of data integrity. This use case once again highlights the need for an online brand protection tool which online businesses running on mobile applications should adopt to safeguard their brand value and the authenticity of the services offered.

2.3 Data Collection using Kaggle's Repository of Simulated Datasets

Kaggle is a prominent data science platform [19] that has revolutionized collaborative data analysis and predictive modeling. Its extensive dataset repository, competitions and forums have fostered a dynamic community of data enthusiasts. Researchers emphasize Kaggle's influence in advancing machine learning techniques and sharing knowledge. This makes it an extremely useful platform for gathering information during the data collection phase of this project.

2.4 Effective Methods of Mitigating Online Brand Abuse

The key to effective brand risk management is to take a proactive approach to identifying potential dangers to the brand and putting emergency measures in place to deal with any issues that might develop. Because so much of the communication about a brand is done by external stakeholders — consumers, competitors, etc. — online brand activities are significantly harder to manage. Although brands cannot control what is said about them online, there are steps that can be taken to monitor, manage, lower risks and have a positive impact on the online activities that affect a brand's reputation.

2.4.1 Detecting Fraudulent Websites Using an Anti-Phishing Model

The paper "Mitigating Online Fraud by Anti-phishing Model with URL & Image based Webpage Matching" [20] proposes an effective scheme to detect phished website which can be leveraged for this research project aiming to propose an anti-counterfeiting model for online brand protection. The proposed system in this paper [20] detects phished sites in two phases as shown in Figure 2.2. The operational details of the two phases are as follows:

2.4.1.1 URL and Domain Identity Verification:

The input for this phase is URLs for the detection process. The majority of these input URLs are very similar to approved URLs, with very small variations that are invisible to normal users. A list of approved URLs that are frequently targeted by phishers are maintained in a database and examined using an approximating string search algorithm against the input provided. On finding similar looking URLs, the next step is to figure out the IP addresses associated with these suspicious input URLs. If the IP addresses of the Authorized URLs and the entered (input) URL do not match, the URL may be an indicator of a phishing attempt. This illegitimate URL is taken into consideration as an input for the second phase, which is based on the web page's image matching. To verify the identity of the URL and Domain, the following tools can be utilised:

Tool 1: URLScan.io for URL Analysis

URLScan.io, a web security service that has gained attention for its role in identifying malicious URLs and analyzing potential threats [21]. Researchers highlight its effectiveness in providing real-time insights into the safety of web addresses. Utilized by

cybersecurity professionals, URLScan.io aids in threat detection, prevention and incident response. Its significance in bolstering web security and aiding in risk mitigation can be useful for implementing the URL analysis feature in Scamsweep.

Tool 2: Cisco Talos Intelligence for Domain or IP Reputation Check

Cisco Talos Intelligence is a renowned threat intelligence platform, widely recognized for its domain and IP reputation checks [22]. Researchers emphasize its role in proactively identifying and mitigating advanced threats, including malware and vulnerabilities. With a vast network of sensors, it provides real-time threat intelligence to businesses and organizations. Cisco Talos Intelligence is praised for its crucial contribution to enhancing cyber defense strategies, making it a valuable addition to the Scamsweep toolkit.

Tool 3: Iris Investigate

Iris Investigate, developed by DomainTools, is a widely noted investigative platform acclaimed for its capabilities in domain research [23]. Scholars underscore its effectiveness in delving into domain ownership, historical records and connections, facilitating the identification of potential risks. Significantly utilized in cybersecurity, this commercial tool aids in threat detection, incident management and digital forensics. The literature underscores its role in advancing domain-related investigations and elevating proactive security strategies, making it a suitable choice for testing and evaluation of domain infringement feature implemented in Scamsweep.

2.4.1.2 Image Based Webpage Matching:

The input for this phase is a snapshot of the suspicious webpage whose URL was flagged as a possible phishing URL in the previous step. This snapshot is treated as an image throughout the detection procedure in the second phase. This image is geometrically analysed to calculate the key points. In image processing, key point is a distinctive spatial point that is invariant to rotation, scale and distortion. Key points are unique and can be used to assess the authenticity of an image when compared to a forged pattern that has undergone various changes such as shifting, lighting variation, etc. This technique makes use of descriptors to capture invariant information around discriminative key points on the suspect page. Then compares the descriptors to the legitimate page descriptors that are already present in the descriptors' database. A suspect page and an authentic page's similarity level can be determined by correlating the descriptions. Finally, a similarity degree is calculated between the two pages to determine whether the suspected page is a counterfeit. If the similarity degree between a suspected page

and an authentic one is greater than a certain pre-determined threshold, the suspected page is considered to be phished.

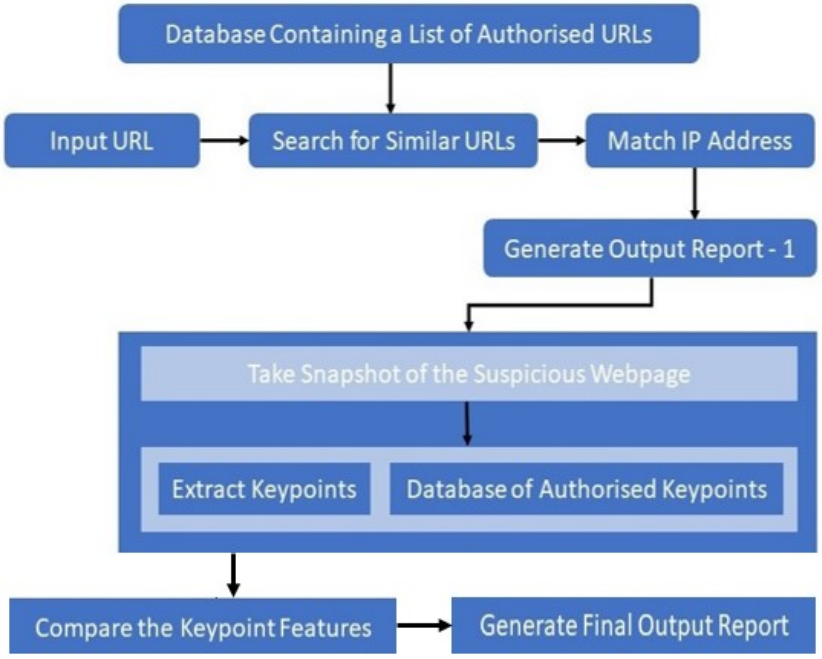


FIGURE 2.2: Anti-phishing Model with URL & Image Webpage Matching [20]

Cumulatively, these two methods described above can be effective in this research project pertaining to online brand protection. A well-strategized amalgamation of the above methods can be used to detect malicious URLs, phished websites, fake products being showcased in social media platforms and online marketplaces that threatens the overall authenticity of a brand.

2.4.2 Reconnaissance Using Open-Source Intelligence Tools

Reconnaissance in cybersecurity refers to the process of covertly gathering information online to use for future operations. This can be with both pure and impure intentions. The MITRE ATT&CK Framework defines reconnaissance as a adversary tactic (TA0043) to actively or passively gather data that would layout the scope of the attack [24].

The paper "Open Source Intelligence (OSINT) for Reconnaissance: A Systematic Review" by Tugce Karatas and Huseyin Cavusoglu explores the effectiveness of open-source intelligence (OSINT) for threat intelligence gathering, including reconnaissance. The study identifies the various OSINT sources used for reconnaissance, such as social media platforms, web archives and news websites. It provides an overview of the OSINT tools and techniques used for reconnaissance. These tools were further used to analyze a set

of malicious domain names and IP addresses and then gathering information about the associated threats. The researchers found that OSINT was able to provide useful information about the threats, such as indicators of compromise (IOCs) and the identities of threat actors.

The paper also explores the benefits and challenges of using OSINT for reconnaissance, including the need for manual analysis of the gathered information to ensure its accuracy and reliability and avoid the potential for false positives. The researchers also noted that OSINT tools are constantly evolving and require regular updates to remain effective.

For conducting web-reconnaissance, following open-source tools can be utilised:

Tool 1: Maltego

Maltego is a Windows-based comprehensive open-source intelligence and forensics tool developed by Paterva from South Africa [25] to conduct reconnaissance. This tool uses real-time data mining as an information gathering method from dispersed sources and presents this information through a graphical link analysis. Users can easily manage and manipulate different types of entities such as people, organizations, email addresses, phone numbers and websites on Maltego. The tool has an interesting graphical feature of presenting each piece of information as a node and then uses arrows to make patterns and establish connection between each node or source of information. The main source of information is known as the parent node and the data extracted from main source of information as regarded as child node. The automatic merging and matching of data collected to create to create a visually mapped data landscape is a unique-selling point for this tool and this feature also makes Maltego very user-friendly.

Tool 2: Recon-ng

Recon-ng is a powerful web reconnaissance OSINT tool with its native platform as Linux. It is a command-line tool with an interface similar to Metasploit [26]. This tool is written entirely in Python. Running Recon-ng on command-line increases the speed of the reconnaissance process as it automates the data collection from open-sources. Recon-ng consists of independent modules, interactive databases, in-built functions, command completion features, interactive help and various other configuration options that can be used to scan an entity and then export the output results in different file types. One of the most commonly used modules of this tool is the HackerTarget module. The API of HackerTarget has the capability to perform DNS lookups, reverse DNS lookups, port scans, traceroute, IP address resolutions, extract HTTP headers and more [27]. Therefore, HackerTarget shall be an appropriate choice of Recon-ng module to facilitate web-based reconnaissance activity for this project.

Tool 3: OTX Alienvault

The paper "Acing the IOC Game: Toward Automatic Discovery and Analysis of Open-Source Cyber Threat Intelligence" [28] delves into the efficacy of OTX Alienvault, which addresses the escalating challenge of handling vast volumes of cyber threat Indicators of Compromise (IOC) shared across diverse sources. By automating IOC extraction from technical articles, the proposed iACE solution employs novel graph mining techniques to identify tokens and their context. With a precision of 95% and over 90% coverage, iACE outperforms conventional Natural Language Processing (NLP) methods and industry IOC tools, including Alienvault. The tool's swift analysis of thousands of articles and correlation of IOCs across extensive timeframes contribute to a comprehensive understanding of evolving attack strategies and their implications on cybersecurity.

Tool 4: Microsoft Defender Threat Intelligence

Microsoft Defender Threat Intelligence is a potent web-reconnaissance tool which provides valuable data and insights for identifying and thwarting cybersecurity threats [29]. Formerly known as RiskIQ PassiveTotal, Microsoft rebranded and enhanced the tool after acquiring RiskIQ [29]. Microsoft Defender Threat Intelligence offers extensive capabilities to monitor and investigate potential risks across the web. It helps security teams to proactively look for Indicators of Compromise (IOCs), recognize malicious domains, monitor suspicious IP addresses and discover other threat-related information. Microsoft Defender Threat Intelligence enables organizations to stay ahead of cyber threats, strengthen their security posture and efficiently handle future incidents by utilizing its vast threat intelligence database and cutting-edge algorithms. It offers a full solution for web-based threat and reconnaissance because of its integration into the Microsoft security ecosystem.

2.4.3 Developing a Statistical Model to Detect Counterfeit Logos

By employing methods like image processing, pattern recognition and statistical analysis to find visual inconsistencies and irregularities in logos, it is possible to create a statistical model in Python that can recognize fake logos.

2.4.3.1 Recognising Logos Using OpenCV and NumPy Libraries in Python

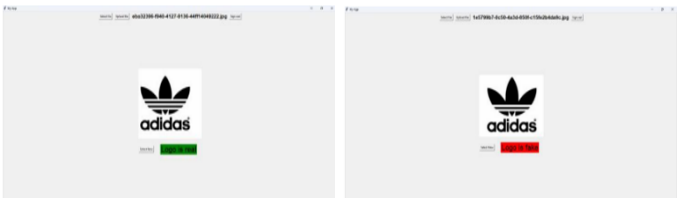
The paper "Real Time Object Recognition Using OpenCV and Numpy in Python" [30] suggests incorporation of the some basic concepts defined in open-source Python libraries like OpenCV and NumPy into image processing units to achieve accurate results easily while processing images based on characteristics like color, shape and size. Both

libraries offer extensive functionality for image processing, computer vision and numerical computations. OpenCV and NumPy libraries have multiple pre-built functions that can be used to recognise logos and extract their features easily. Below is a list of few such functions:

- cv2.imread(): Loads an image from a file.
- cv2.imshow(): Displays an image in a window.
- cv2.cvtColor(): Converts an image from one color space to another.
- cv2.resize(): Resizes an image to a specified size.
- cv2.imwrite(): Saves an image to a file.
- cv2.calcHist(): Calculates color histogram of an image.
- np.reshape(): Changes the shape of an array.

2.4.3.2 Calculating the Degree of Dissimilarity between Two Images Using Chi-square Distance Formula

The paper "GLCM–based chi–square histogram distance for automatic detection of defects on patterned textures" [31] by V. Asha, N.U. Bhajantri and P. Nagabhushan proposes a new machine vision algorithm for automatic defect detection on patterned textures. Motivated by the fact that texture discrimination by human vision system is based on second–order statistics, this algorithm uses chi-square distance as one of the metrics that can be used to identify differences between histograms of Grey Level Co–occurrence Matrix (GLCM) of two images. GLCMs are computed after quantising the gray-scale range from 0-255 [0 is black (darkest) and 255 is white (brightest)] to 0-63 (web-safe color saturation range [32]) to keep the size of the GLCM minimal and to speed up computation. Input faulty images are divided into numerous periodic blocks. In order to automatically identify faulty and defect-free blocks, hierarchical clustering is applied to the dissimilarity matrix produced from the chi-square distances of the GLCMs.



(a) Figure A (b) Figure B

FIGURE 2.3: Real and Fake Logo Images [31]

Through trials on real and fake logos extracted from multiple sources such as: Kaggle dataset, official company website and suspicious social media account, the effectiveness of the suggested strategy is demonstrated as seen in Figure 2.3.

2.4.4 TinEye

The paper "Search by Image: A Novel Approach to Content Based Image Retrieval System" describes TinEye [33] as a prominent and extensively utilized reverse search engine. Unlike conventional methods relying on keywords, metadata, or watermarks, TinEye employs pioneering image recognition technology. This platform permits users to either upload images (limited to 1MB) or provide links, prompting the tool to scour for similar visuals. Employing image recognition, TinEye traces the origin, usage, variations and even offers higher-resolution alternatives. It excels in locating both identical and modified versions, accommodating various alterations like cropping, color adjustments, resizing and minor rotations. TinEye recognizes complete images holistically, not specific elements within. Moreover, it serves as a means to identify unlawful utilization of copyrighted or pilfered images, which makes it a good choice for testing the image processing capability of Scamsweep.

2.4.5 Identifying Trademark Infringements Using Gerben Trademark Library

Gerben Perrott PLLC is a specialized trademark, patent and intellectual property (IP) legal business with offices in Washington DC, founded in 2008 [34]. Gerben Law Firm has filed more than 4000 trademarks, earning the recognition as a top trademark filer by the World Trademark Review [35]. The firm has also been mentioned in various national newspapers and news outlets, including Bloomberg BNA, CNBC, The New York Times and The Wall Street Journal [35]. The company currently works with clients from all 50 states as well as more than 30 different nations. According to the paper, "Plotting Course" by Mark Hansen [36] Gerben's strict assembly-line approach to trademark filings and a strategic investment of more than $30,000 in search engines to create a well-categorised database that is pulled on a regular basis [37] is its real key to success. Therefore, this comprehensive open-source repository of intellectual property assets can be used in Scamsweep to detect any abuse of trademarks, copyrights, marketing keywords or descriptors exclusively registered by an organization.

2.4.6 Marcaria

As the number of registered trademarks and applications continues to rise, ensuring the accuracy of trademark validation processes becomes progressively complex and prone to human errors. Moreover, determining a brand's eligibility for registration often hinges on subjective interpretations of local regulations. The paper "Opportunities and challenges in the application of Artificial Intelligence to TradeMark Validation processes" discusses the integration of Artificial Intelligence (AI) technology to develop a commercial solution named "Marcaria" for enhancing brand validation and trademark registration procedures [38]. Employed by businesses and legal professionals, Marcaria aids in making informed trademark registration decisions. This article outlines the conventional brand validation process, highlighting its inherent challenges, while also exploring the potential benefits and obstacles associated with AI implementation in these processes.

2.4.7 Phlanx's User Engagement Calculator for Social Media Analytics

In the paper titled "Social Media as Communication Strategy for Susi Pudjiastuti to Build Maritime Security Awareness in Indonesia" [39], the authors employ Phlanx, a social media analytics tool, to analyze Susi Pudjiastuti's Instagram engagement. As of June 2019, her Instagram followers exceeded 2.3 million, marking her as the most followed Indonesian minister on the platform. The research highlights Engagement Rate, a crucial metric measured using a mathematical formula involving interactions like likes, comments, impressions and shares. This utilization of Phlanx exemplifies the tool's role in assessing user engagement and performance of digital content on social media platforms. It is to be noted that The term "Social Engagement" describes how engaged a user's followers are on the social media app. An individual's level of social engagement is indicated by their "Like", "Comment", or "Tag" on a post. [40], [41].

2.4.8 Reverse Engineering of Malicious Applications

Reverse engineering of malicious applications involves dissecting their code and structure to uncover their functionalities, vulnerabilities and potential risks. This process aids in understanding the threat landscape, enhancing cybersecurity measures, and developing effective countermeasures.

Tool 1: HashCalc

The paper titled "Impact of Device Jailbreaking or Rooting on User Data Integrity in Mobile Forensics" [42] explores the use of Hashcalc tool in mobile forensics to address

internet crimes like phishing. By adopting the National Institute of Standards and Technology (NIST) methodology, the study focuses on robust data acquisition via Wireshark, subsequent HashCalc examination and analysis. The paper underscores the significance of ensuring data integrity in the context of device vulnerabilities. It responds to the increasing threat of phishing via messaging apps and emphasizes the need for systematic digital evidence analysis to counter cybercrimes. Therefore, HashCalc has the ability to offer value to Scamsweep's final toolbox.

Tool 2: PEStudio

The study "Learning the Basic Structure of Several Ransomwares Using Static Analysis Technique" [43] by Amiruddin Amiruddin, Candra Kurniawan, Eka Hero Ramadhani1 and Julio Rinaldi investigates a systematic approach for ransomware analysis through a mix of Virustotal scanning, PEStudio examination and results analysis. To check uploaded files for malware or ransomware traits, the study makes use of Virustotal's large antivirus databases. In addition, PEStudio is used to investigate strings, libraries and signatures. The interaction between PEStudio and Virustotal improves the confidence of results. In order to verify and support the findings, the authors stress the importance of cross-referencing data from various instruments. This paper seeks to identify commonalities in ransomware structures through a comparative examination of samples. It can be possible to use this method to gain a deeper understanding of malware behaviour in malicious mobile or computer applications hosting content that may impact the brand integrity of an organization. Therefore, PEStudio has the potential to become a valuable addition to the final toolkit of Scamsweep.

2.4.9 Alert Generation or Rule Creation Using Snort

Snort is a free open-source Intrusion Detection System (IDS) that uses rules to define malicious network activity. It uses these rules to find network packets that match the defined conditions and then generates alerts for users. The book "Snort Cookbook: Solutions and Examples for Snort Administrators" [44] explains the basics of Snort installation and gives clear instructions on how to configure the rules to detect and prevent network-based attacks. The book is a collection real-world scenarios on common security issues with step-by-step guide on creating and testing of Snort rules, and also integrating it with other security solutions. Snort has a wide range of features and capabilities that can be leveraged to customize rules fitting the security needs for an effective online brand protection.

2.5 Risk Analysis in Online Brand Management

According to IBM, "Risk management is the process of identifying, assessing and controlling financial, legal, strategic and security risks to an organization's capital and earnings [45]." It involves analyzing potential threats, determining the likelihood of those threats occurring, and implementing measures to mitigate or avoid them. Therefore, to assess and evaluate the exposure of an organisation to brand risks, it is essential to implement a robust risk management framework.

2.5.1 Risk Management Frameworks

A strong foundation of risk management framework is crucial for any organization. A Risk Management Framework (RMF) aims to safeguard the organization's capital base and revenue generation capability without hindering growth. Businesses can balance accepting risks and minimizing them using a risk management framework.

The purpose of risk management frameworks is to provide a structured and systematic approach for organizations to identify, assess, and manage risks in their operations. These frameworks help organizations to proactively identify potential risks and develop strategies to mitigate or avoid them. By implementing a risk management framework, organizations can improve their decision-making processes, reduce the likelihood of negative events occurring, and increase the likelihood of achieving their objectives as well as comply with the legal and regulatory requirements of the land. Effective risk management enables an organization to function properly in a volatile environment.

There are several risk management frameworks available in the market. We shall explore some of these in the next sub-sections.

2.5.2 ISO 31000

ISO 31000 is a general risk management standard that is primarily concerned with managing risks that may have an impact on societal, environmental or professional outcomes as well as economic performance and professional reputation.

Most recent version of ISO 31000 is ISO 31000:2018 [46], which is revised once every few years like other standards. It outlines principles, structure and procedure for managing risk. It also provides guidelines and can be utilized in organizations of any size, activity or sector because it is a standard. Organizations that apply ISO 31000 are more likely to achieve their goals, better identify opportunities and threats, allocate and deploy resources for risk management in an efficient manner.

ISO 31000 defines risk as the effect of uncertainty on objectives and it emphasizes the importance of considering both positive and negative aspects of risk in decision-making [46]. As shown in Figure 2.4, the key principles of ISO 31000 are: establishing a risk management framework, communicating and consulting with stakeholders, identifying and analyzing risks, evaluating risks, treating risks, monitoring and reviewing the effectiveness of the risk management process and continually improving the process over time.

Table 4.1 highlights the key areas addressed by ISO 31000:

TABLE 2.1: Key areas addressed in ISO 31000

Key Areas	**Objectives**
Establishing the context	This involves identifying the internal and external factors that can affect the achievement of objectives, defining the risk management scope and criteria and setting the risk management policy
Risk assessment	This involves identifying, analyzing and evaluating risks based on their likelihood and potential impact on objectives
Risk treatment	This involves selecting and implementing risk management options to modify risks, such as avoiding, transferring, mitigating or accepting them
Risk communication and consultation	This involves sharing information and consulting with stakeholders about risk management decisions and activities
Monitoring and review	This involves ongoing monitoring and review of the effectiveness of risk management activities, as well as the external and internal factors that can affect risk

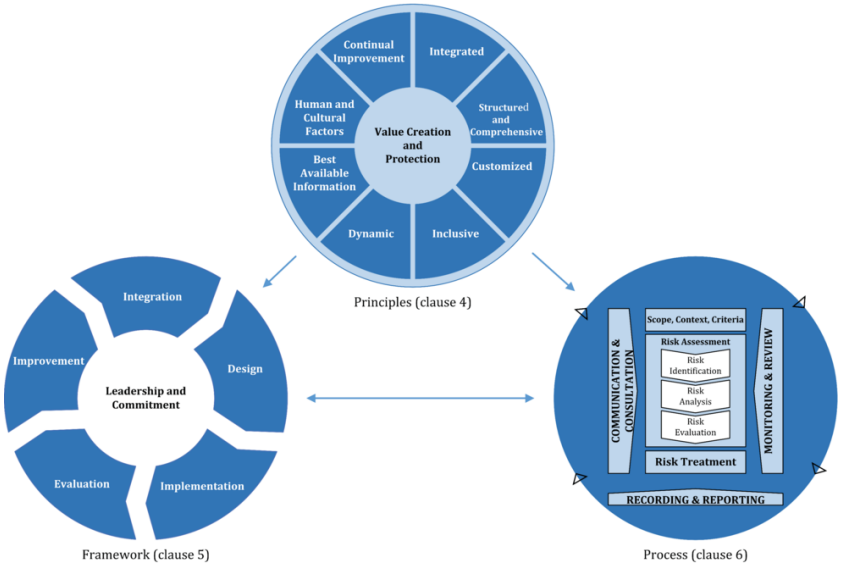


FIGURE 2.4: Structure of ISO 31000 - Risk Management Standard [46]

2.5.3 NIST RMF

NIST RMF stands for the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) [47]. It is a process that helps organizations manage risks associated with the operation and use of information systems and technology.

The NIST RMF is a comprehensive framework that provides guidelines, standards and best practices for managing cybersecurity risk. As shown in Figure 2.5, it includes 7 repeatable steps that organizations can use to implement and maintain effective risk management practices:

1. Prepare: This step involves the essential activities needed to prepare the organisation to counter security and privacy risks.
2. Categorize: This step involves identifying the information systems and assets that need protection and assigning a level of risk to each.
3. Select: This step involves selecting appropriate security controls that can help mitigate the identified risks.
4. Implement: This step involves implementing the selected security controls within the information system.
5. Assess: This step involves assessing the effectiveness of the security controls in reducing risks to an acceptable level.
6. Authorize: This step involves reviewing the risk assessment results and making a decision to authorize the system for operation.
7. Monitor: This step involves continuous monitoring of the system to ensure that the security controls remain effective and risks are managed appropriately.

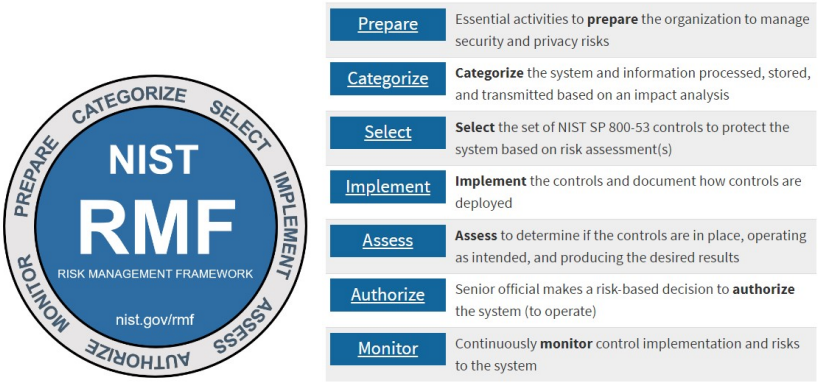


FIGURE 2.5: 7-step process of NIST Risk Management Framework [47]

The NIST RMF is widely used in the United States federal government, as well as in many other industries and organizations as a best practice for managing cybersecurity risks.

2.5.4 FAIR

The Factor Analysis of Information Risk (FAIR) is a risk management framework that provides a quantitative approach to analyzing and managing information security risks. It has emerged as the premier Value at Risk (VaR) model for cybersecurity and operational risk [48]. It is designed to help organizations understand the likelihood and potential impact of different types of security incidents, and to make informed decisions about how to allocate resources to mitigate those risks.

The FAIR framework has 3 stages in it's risk assessment methodology [48] (refer Figure 2.6):

1. Stage 1: Identify scenario components
    - Identify the asset at risk
    - Identify the threat community under consideration
2. Stage 2: Evaluate Loss Event Frequency
    - Estimate the probable Threat Event Frequency
    - Estimate the Threat Capability
    - Estimate Control Strength
    - Derive Vulnerability
    - Derive Loss Event Frequency
3. Stage 3: Evaluate Probable Loss Magnitude
    - Estimate worst-case loss
    - Estimate Probable Loss Magnitude
4. Stage 4: Derive and articulate risk
    - Derive and articulate risk
    - Identify the threat community under consideration

Therefore, the FAIR framework is a well-respected and widely used methodology for assessing and managing information security risks. Its focus on quantitative analysis

FIGURE 2.6: Model Controls in a FAIR Risk Analysis [48]

and transparency can help organizations make more informed decisions and prioritize their security investments more effectively.

Amongst the above three frameworks, i.e., ISO 31000, NIST RMF and FAIR, the most suitable one that fits best into Scamsweep's Risk Assessment Plan shall be adopted for implementation.

2.5.5 MITRE ATT&CK Framework

The MITRE ATT&CK framework [49], an extensive repository of adversary tactics, techniques and procedures that has gained widespread acceptance in both the cybersecurity sector and academic circles. Its diverse applications range from threat intelligence to incident response, extending beyond its original purpose. Despite its popularity, a systematic review of ATT&CK's applications and associated research is lacking. The paper "SoK: The MITRE ATT&CK Framework in Research and Practice" [50] aims to address this gap by introducing the inaugural taxonomic organization of ATT&CK-related literature. It assesses its utility in various applications, identifying gaps and inconsistencies and offering directions for future research. The findings offer valuable insights for scholars and practitioners, emphasizing the need for more research on ATT&CK's practical implementation and evaluation.

Leveraging the MITRE ATT&CK framework for risk assessment is a strategic approach that empowers organizations to comprehensively analyze potential threats. By mapping known adversary tactics and techniques to existing security controls, vulnerabilities are highlighted, guiding resource allocation and countermeasure planning. This framework's versatility lies in its ability to provide insights into attacker behavior, enabling tailored defense strategies. As a result, risk assessment becomes proactive, enabling organizations to adapt and fortify their cybersecurity posture against a dynamic array of cyber threats. This approach maximizes the efficacy of limited resources while fostering a

resilient defense against emerging attack vectors. Therefore, we shall incorporate the Enterprise Model of the MITRE ATT&CK Framework (refer Figure 2.7) along with other 3 frameworks discussed above to create a customised brand risk assessment framework for Scamsweep.

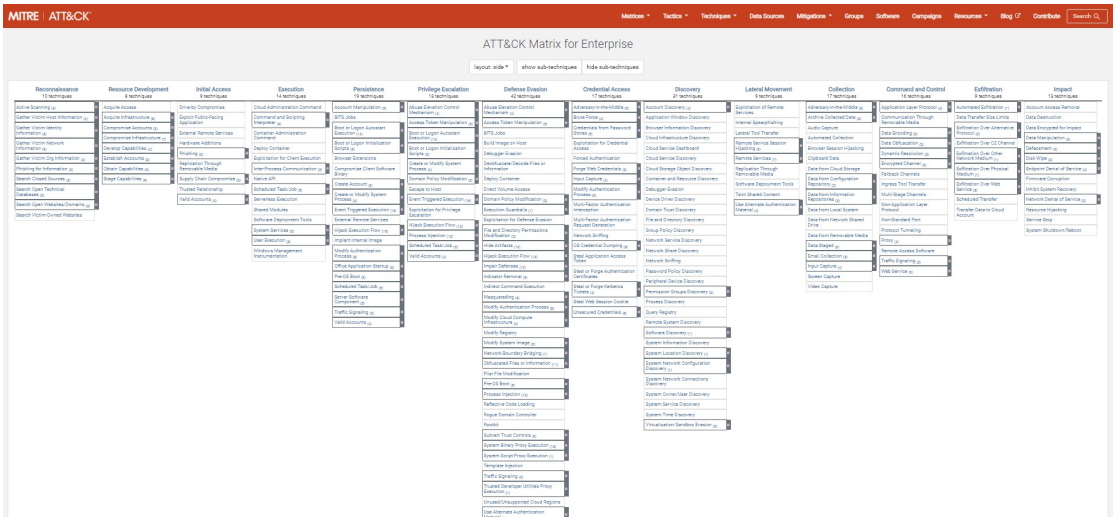


FIGURE 2.7: MITRE ATT&CK framework - Entreprise Model [49]

2.5.6 Risk Assessment Plan

Risk rating and risk registers are important components of any kind of risk management in an organization and this includes brand risk management. While risk rating is the process of assessing the likelihood and impact of each identified risk, the risk register serves as a tool to track the identifies risks alongside their corresponding ratings. This helps to prioritize risks based on their potential impact on the organization and to allocate resources to manage the risks appropriately. Risk rating can be done using various methods, such as probability and impact matrix, risk scoring or qualitative analysis.

This section explores two methods used for brand risk analysis, i.e., Bayesian Decision Model and "Risk = Impact x Likelihood" Formula to quantify the severity of a risk.

2.5.6.1 Bayesian Decision Model

The paper "Bayesian decision models: A primer" by Wei Ji Ma [51] of New York University provides an explanation of the Bayesian model of decision making under any kind of uncertainty. The authors explain how this model uses Bayes' theorem to update prior probabilities with new information or data, to arrive at a posterior probability that reflects the updated likelihood of an event occurring.

2.5.6.2 "Risk = Impact x Likelihood" Formula

The paper "The two-dimensionality of project risk" [52] by T M Williams discusses the importance of considering the likelihood and impact of risks when managing project risk. When allocating a threat score or rating to a project risk, it requires consideration of two factors, i.e., impact of the risk and likelihood of its occurrence. The idea of multiplying impact with likelihood to calculate the probability of a risk in a project is a common practice in project management, finance and safety engineering [52] that expresses the relationship between the impact and likelihood of a risk event. The paper argues that traditional approaches to project risk management have focused primarily on the likelihood of risks occurring, without sufficient consideration of their potential impact. The formula "Risk = Impact x Likelihood" suggests that the severity or level of risk associated with a particular event can be determined by considering both the potential impact of the event and the likelihood of it occurring. For example, if the impact of a risk is 3 and the likelihood of its occurrence is 4, then the risk score would be: 2x4=8.

While both the Bayesian model and the "Risk = Impact x Likelihood" formula can be used to assess and manage risks, they are distinct approaches with different underlying assumptions and calculations. The Bayesian model can be used in decision making, but it involves prior information on the sample data as a parameter for calculation, which can be challenging to obtain during the course of this project. Hence, the second method, i.e., "Risk = Impact x Likelihood" formula that involves only a simple multiplication of the two estimable parameters is more suitable for conducting a risk analysis on online brand management project.

2.6 Current Existing Solutions in the Market

There are already many brand protection products available in the industry. Some of the leading players in this field or technology are: ZeroFOX, RiskIQ, Redpoints, InSights, Brandshield, MarkMonitor and others.

In this section we shall compare the solutions offered by the security product of 3 companies, i.e., ZeroFOX, RiskIQ and Brandshield.

2.6.1 ZeroFOX

The ZeroFOX Platform offers thorough visibility and security with a comprehensive global coverage across the attack surface of an enterprise. It also goes beyond to search deep in the dark web [53]. It is always-on, providing full-spectrum external threat intelligence, protection and response solution. ZeroFOX offers businesses defense, intelligence and disruption to neutralize external threats to their brands, people, assets and data, all under one holistic platform [53]. The ZeroFOX Platform is capable of detecting and resolving targeted phishing attacks, credential compromise, data exfiltration, ransomware, brand hijacking, executive and location threats [53]. Its artificial intelligence-based analysis engine is supported by Intel [53]. Millions of posts, messages and accounts are processed everyday using ZeroFOX technology throughout the social and digital environment, including LinkedIn, Facebook, Slack, Instagram, Pastebin, YouTube and mobile app stores, domains, cloud-based email and more.

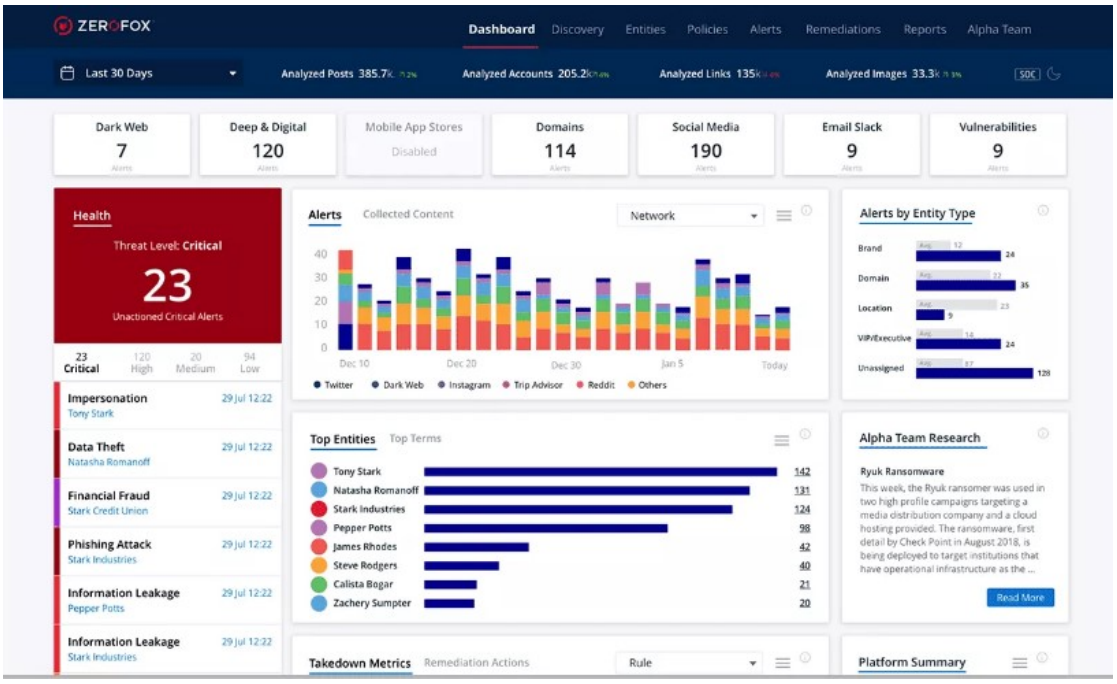


FIGURE 2.8: ZeroFOX Tool Console: Dashboards on Homepage [53]

2.6.2 RiskIQ

RiskIQ offers a range of features to help organizations protect their brand reputation online. One of its key capabilities is brand monitoring, which scans the internet for unauthorized use of trademarks, logos and other intellectual property associated with a particular brand [54]. RiskIQ's threat intelligence platform provides real-time insights

into potential threats, such as malware or social media scams, while its automated take-down feature allows companies to quickly remove infringing content (refer Figure 2.9) [54].

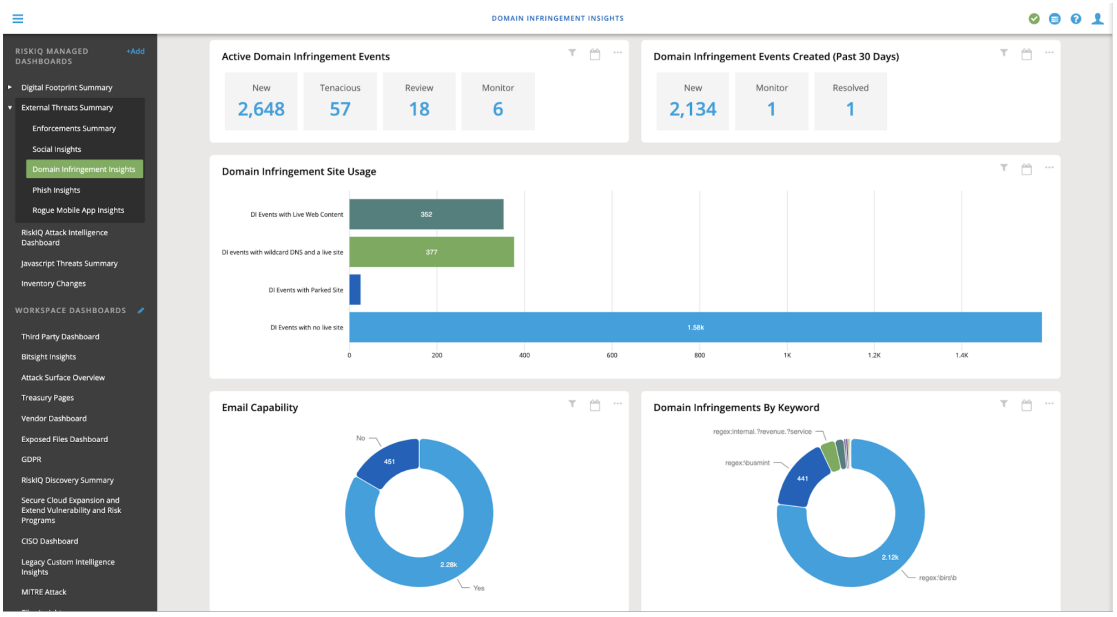


FIGURE 2.9: RiskIQ Tool Console: Dashboards on Homepage [54]

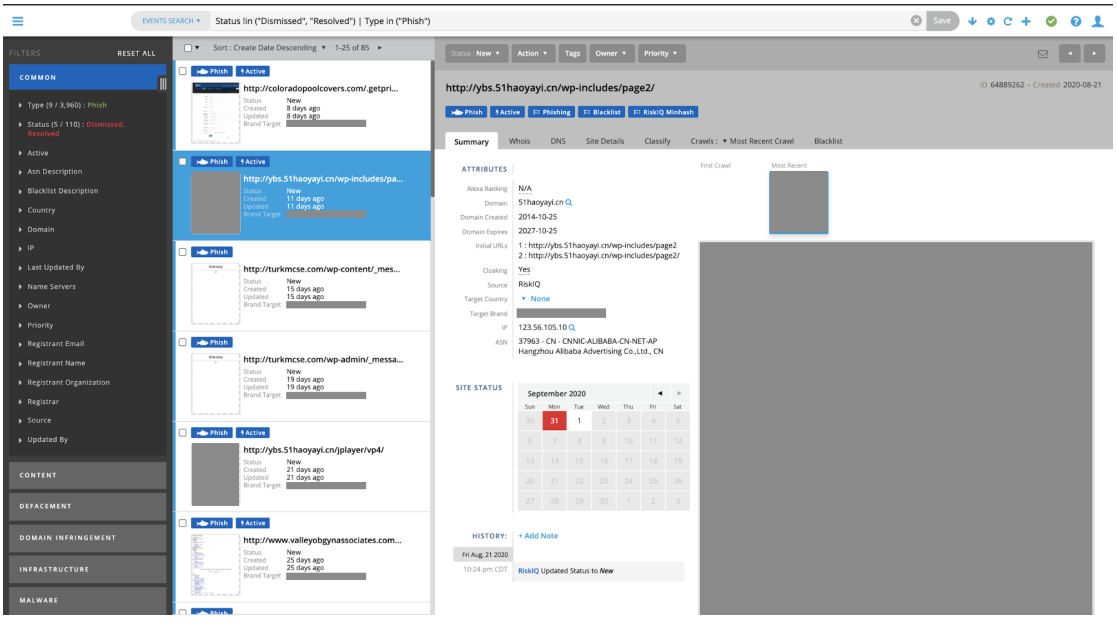


FIGURE 2.10: RiskIQ Tool Console: Domain Infringement Detections [54]

As shown in Figure 2.10, the tool also offers domain and website monitoring, allowing businesses to detect phishing sites or other fraudulent web pages that may harm their brand.

Additionally, RiskIQ offers a range of customizable reports and analytics to help businesses understand the scope and impact of brand abuse and track the effectiveness of their brand protection efforts over time [54].

2.6.3 BrandShield

BrandShield is an AI-powered Israeli product that provides brand protection service using a combination of machine learning and artificial intelligence. BrandShield tracks the Internet, social media, phishing websites, identity thefts and online frauds using its anti-phishing algorithm. As shown in Figure 2.11, it creates comprehensive dashboards to further produce a digital risk map of the external threats pertaining to the concerned brand name [15]. The other capabilities include a Website Duplication Detector, automatic takedown notifications, blacklists and many others [15]. BrandShield operates on cloud and does not need on-premise integration [15]. However, if needed, it also has the capability to integrate its API with SIEM to generate alerts [15]. All of these use cases are accomplished by the robust technology developed by BrandShield to track and protect the business's trademarks and visual assets.

FIGURE 2.11: Brandshield Tool Console: Dashboards on Homepage [15]

2.6.4 Comparitive Analysis: ZeroFOX vs RiskIQ vs BrandShield

This sub-section presents a comparative analysis of the key features of 3 commercial tools in the market of online brand protection. The tools considered for this comparative study are: ZeroFOX, RiskIQ, BrandShield. Table 1 showcases the features present in each of these tools.

TABLE 2.2: Comparison of 3 Pre-existing Brand Protection Solutions

Features	**ZeroFOX**	**RiskIQ**	**BrandShield**
Domain Monitoring	Yes	Yes	Yes
Trademark Infringement	Yes	Yes	Yes
Counterfeit Detection	Yes	Yes	Yes
Unauthorized Seller Detection	Yes	Yes	Yes
Social Media Account Protection	Yes	Yes	Yes
Customizable Reports and Analytics	Yes	Yes	Yes
Dark Web Monitoring	Yes	No	No
Automated Takedown	Yes	No	Yes
Pricing	Custom	Custom	Custom

2.7 Conclusion

In conclusion, to sum up, a literature review is an important and crucial part of any research effort. It entails locating, analyzing, and synthesizing the literature that already exists on a certain subject and serves as the basis for the research question, hypothesis, and approach. A thorough literature evaluation makes that the research is pertinent, significant and advances our understanding of the subject.

The literature presented in this chapter has significantly influenced the formulation of Scamsweep's design and architecture presented in the next chapter. It also influenced the implementation strategy of the project. First key takeaway from this chapter was discovering the success of open-source tools while conducting reconnaissance, which paved the way for using OSINT to gather network artifacts pertaining to the chosen brand or company. Second key takeaway was finding out about generating color histograms and calculating the Chi-square distance for image processing, which contributed in developing a script written in Python to differentiate between real and fake logos.

Chapter 3

Design

This chapter's primary subject of discussion will be a strategy to achieve the Literature Review provided in the previous chapter. This chapter is divided into five sections: problem definition, objectives, requirements and design. The problem definition provides a technical description of the primary issue that the suggested solution aims to solve. An outline of the goals this project seeks to accomplish is provided in the chapter titled "Objectives". The requirements section concludes with a list of the technical requirements that the project must meet.

Designing a solution for online brand protection is the key to establishing a robust defense mechanism against brand misuse and unauthorized activities. It is crucial to take into account a number of vital components while designing an efficient open-source online brand protection toolkit, such as the architecture diagram, requirements capture, data flow, risk assessment plan, alert creation process and reporting abuse. By carefully addressing these aspects, Scamsweep can assist in undertaking thorough proof-of-concepts linked to an organization's online brand protection while retaining efficiency and accuracy.

There are numerous modules or use cases to examine, design around and execute for the project solution based on the information in the preceding chapter. For example, the reconnaissance module is used to gather open-source intelligence and perform initial investigations to identify potential threats or brand misuse. The social media monitoring module captures hashtags, mentions and user interactions to identify brand impersonators or instances of customer dissatisfaction on social media platforms. The image processing module is utilized to differentiate between real and counterfeit brand logos. The risk assessment module helps in identifying and assessing the severity and impact of various threats, allowing organizations to allocate resources effectively and focus on

the most critical risks. It is necessary to look at how each of these modules function individually and in relation to the overall functioning while designing the solution.

3.1 Problem Definition

The problem of brand abuse in cyberspace pertains to the rampant misuse and exploitation of established brands by malicious actors. This includes unauthorized use of logos, trademarks and domain names for fraudulent activities, such as phishing, counterfeit sales and online scams. Brand abuse erodes consumer trust, tarnishes brand reputation and imposes financial losses on businesses. It necessitates robust strategies for early detection, prevention and mitigation to safeguard brands from cyber threats. Addressing this problem requires comprehensive solutions that combine technological tools, legal frameworks and proactive brand monitoring to counteract the proliferation of brand abuse across the digital landscape.

For this project, the problem at hand revolves around online brand protection, particularly the significant challenge posed by the high cost of commercial brand protection solutions. These solutions often come with hefty price tags that render them financially inaccessible for small businesses. As a result, these businesses remain vulnerable to various brand-related threats, including counterfeiting, trademark infringement and online impersonation. Therefore, there is a pressing need for an open-source brand protection solution that offers cost-effective alternatives to safeguard the interests of small businesses, ensuring their ability to maintain brand integrity in a competitive digital landscape.

3.2 Objectives

1. **Case Study:** Conduct a case study to highlight detailed market research on the selected brand for testing of features implemented within Scamsweep. Backup the choice made with reliable facts and quantifiable data. The outcome of the case study shall influence the choice of brand to be picked for conducting a Proof-of-Concept (PoC) for Scamsweep in Chapter 5.

2. **Data Collection:** Build a database containing a list of legitimate digital assets of a brand such as: designs, logos, trademarks, copyrights, domain names, IP addresses, social media accounts, applications available on App-store, authorised resellers on online marketplaces, marketing keywords, descriptors and others details. Reach out to company employees or explore other sources such as: Google

Dataset Search, Pastebin and Kaggle to download publicly available datasets for research purposes.

3. **Reconnaissance:** Experiment with various open-source tools and technologies such as: Maltego, Recon-ng, OTX Alienvault and Microsoft Defender Threat Intelligence in a reasonable and efficient manner to conduct reconnaissance and gather threat intelligence associated to the brand being investigated.

4. **Domain Infringement Detection:** Verify the reputation of the suspicious Indicators of Compromise (IOC) detected during the reconnaissance phase, especially URLs, domains and IP addresses by analysing it on well-known open-source sandboxes and threat intelligence platforms like URLScan.io [55], Cisco Talos Intelligence [56], Sucuri [57], VirusTotal [58] and more. Additionally, take a live snapshot of the phished website and analyse the content posted in real-time.

5. **Trademark Infringement Detection:** Research and develop a Python script that checks if the copyrights, trademarked words, marketing keywords or descriptors associated with the concerned brand is being abused by counterfeiters.

6. **Counterfeit Logo Detection:** Research and develop a Python script leveraging NumPy and OpenCV libraries that uses image processing techniques to distinguish between real and counterfeit logos being used by brand abusers. One such method involves using the Chi-square distance to measure similarity between image features by comparing two histograms ($x = [x_1, .., x_n]$ and $y = [y_1, ..., y_n]$) having n bins both. Equation to calculate the Chi-square distance (X^2) is given below [59]:

$$X^2 = \frac{1}{2} \sum_{i=1}^{n} \frac{(x_i - y_i)^2}{(x_i + y_i)} \tag{3.1}$$

   This approach circumvents the challenges associated with training machine learning models while still offering a viable solution.

7. **Social Media Monitoring:** Process the search results derived on entering the trademarked marketing keywords to identify potential impersonated social media accounts on multiple platforms like Instagram, Facebook, YouTube, Twitter, LinkedIn and more. Additionally, set up Google Alerts to stay updated on posts or announcements or any kind of user engagements made by the brand on their official account that would help determine if the identified suspicious accounts are legit or fake.

8. **Risk Assessment:** Conduct a thorough risk assessment of the identified threats pertaining to a brand. Assign a threat score (Range: 0-16) and a risk rating (High, Medium, Tolerable, Low) from a 4x4 risk matrix to understand the severity

of impact of these identified threats. This helps in prioritising enforcements in case the volume of brand abuse incidents for the concerned organization is significantly high.

9. **Alert Creation:** Create a prototype of generating automatic alerts by writing Snort rules with appropriate messages on identifying a threat and its severity based on the risk rating of the event.

10. **Reporting and Documentation:** Analyse and document the investigation results obtained from these open-source tools included in Scamsweep's toolkit to arrive at a conclusion whether the concerned brand has been infringed or not.

3.3 Requirements

The necessary functional requirements and non-functional requirements for Scamsweep are listed below. These specifications outline the implementation pre-requisites and what is anticipated of the toolkit itself in terms of key deliverables.

3.3.1 Functional Requirements

The functional requirements for the toolkit can be further divided into 3 categories, i.e., hardware requirements, software requirements and framework requirements.

1. Hardware Requirements:

   - Servers with CPU cores (for example, quad-core or higher) or a cloud instance with at least 2-4 GB of RAM should be sufficient for basic functionality and handling the expected workload.
   - Adequate storage capacity (minimum 15GB of storage on cloud or on-premise infrastructure) to store brand assets, collected data and analysis results of small-scale projects or proof-of-concept deployments.
   - High-speed and reliable internet connectivity with at least 10 Mbps download speed is required to ensure seamless processing of data, remote access and collaboration from different locations.
   - Redundancy and backup mechanisms to ensure data availability and disaster recovery.

2. Software Requirements:

   - Download and import datasets from Kaggle (Link: `https://www.kaggle.com/`) datasets or Pastebin (Link: `https://haveibeenpwned.com/DomainSearch`) into the project environment. The dataset should support common data formats (for example, CSV, JSON) or image formats (for example, JPEG, PNG) to ensure seamless integration with the project's data processing pipeline.
   - Download and install the latest stable version of Maltego from the official website (Link: `https://www.maltego.com/downloads/`) with proper configuration of network settings on the target operating system. It is to be noted that Maltego is platform independent and supports multiple operating systems such as: Windows, macOS and Linux. One can obtain either a commercial license or a free community edition, based on the intended usage and requirements.
   - Obtain a valid subscription or license for the community version of Microsoft Defender Threat Intelligence (Link: `https://ti.defender.microsoft.com/`), previously known as RiskIQ PassiveTotal (Link: `https://community.riskiq.com/`) depending on user requirements. User needs to create an account and adhere to the terms and conditions set by Microsoft for using the community version.
   - Access to open-source sandboxes like: urlscan.io (Link: `https://urlscan.io/`), virustotal.com (Link: `https://www.virustotal.com/gui/home/upload`), phlanx.com (Link: `https://phlanx.com/`) and others for real-time analysis of potential threats detected.
   - Download and install the latest version of Python from the official Python website (Link: `https://www.python.org/`) and then run the following to commands to install NumPy and OpenCV libraries and its dependencies:
     pip install numpy
     pip install opencv-python
     Alternatively, one can also use the pre-configured environments in Google Colab that uses Jupyter notebooks (.ipynb) for Python scripting. It supports both Python 2 and Python 3, and most commonly used Python libraries are already installed. The scripts can be downloaded in various formats, including .ipynb, .py, or .html.
   - Download and install HashCalc version 2.02 (Link: `https://hashcalc.en.softonic.com/`) for analysing hash values and PEStudio version 9.45 (Link: `https://pestudio.en.uptodown.com/windows/download/85128621`) to reverse engineer suspicious applications or programs (.exe files).

- Microsoft Office subscription to access tools like MS Powerpoint (to be used for developing architecture diagrams) and MS Excel (to be used for developing a Risk Assessment Framework for Online Brand Protection).
- Download and install Snort version 3.0 on the VM from their official website or package repository (Link: `https://github.com/snort3/snort3/`) specific to target operating system. User should have administrator or root privileges to access and edit the Snort configuration file (snort.conf) to write new rules or generate alerts.

3. Framework Requirements:

   - Incorporate industry-acknowledged Risk Management Frameworks (RMF), standards and best practices to evaluate brand risks based on severity, such as: NIST RMF, ISO 27001 or FAIR model.
   - Incorporate an industry-acknowledged threat models like the MITRE ATT&CK Framework to evaluate the counterfeiting tactics, techniques and procedures (TTPs) being used by brand abusers.

3.3.2 Non-functional Requirements

1. Scalability: Ability to handle a large volume of brand assets, data and user accounts, while maintaining performance and responsiveness.
2. Security: Ability to protect sensitive brand information and user data from unauthorized access, data breaches and cyber attacks through robust security measures.
3. Reliability: Ability to be reliable, with minimal downtime and a backup system to ensure data integrity and availability.
4. Cross-Platform Compatibility: Ability to accommodate users across different platforms, various operating systems and devices.
5. Performance: Ability to optimize for fast data processing, quick search capabilities, and efficient performance to provide timely brand protection insights.
6. Documentation: Ability to procure comprehensive documentation, including user manuals and guides to assist users in understanding and effectively using the platform.
7. Open Source Compatibility: Ability to adhere to open-source standards and be compatible with relevant tools, libraries and frameworks.

8. Extensibility: Ability to allow future enhancements, integration with third-party services, and the addition of new features to adapt to evolving brand protection needs.

9. Community Support: Ability to foster a supportive and active community to encourage collaboration, contributions and continuous improvement of the project.

3.4 Architecture Diagram of Scamsweep

The architecture of Scamsweep has been designed to incorporate information from various data sources, such as company websites, social media accounts, e-commerce websites and online marketplaces. This enables continuous monitoring of brand mentions and activities across multiple platforms. The workflow includes processes like data collection, web-reconnaissance, URL analysis, text analyis, logo detection, etc.

The functionality of Scamsweep may be divided into two distinct architectures, one for the front-end GUI and one for the back-end functionality. Although GUI development of the toolkit is a work currently scheduled for the future, but still a prototype has been proposed to outline the envisioned look and feel of Scamsweep's user interface.

The back-end workflow diagram in Figure 3.1, illustrates the sequence of operations, logical processing and interactions between different components that occur in the back-end architecture of toolkit, which is usually the server-side of an application or system, whereas the GUI workflow diagram in Figure 3.2 illustrates the sequence of user interactions, system responses and the overall navigation within the user interface of toolkit to be implemented in future.

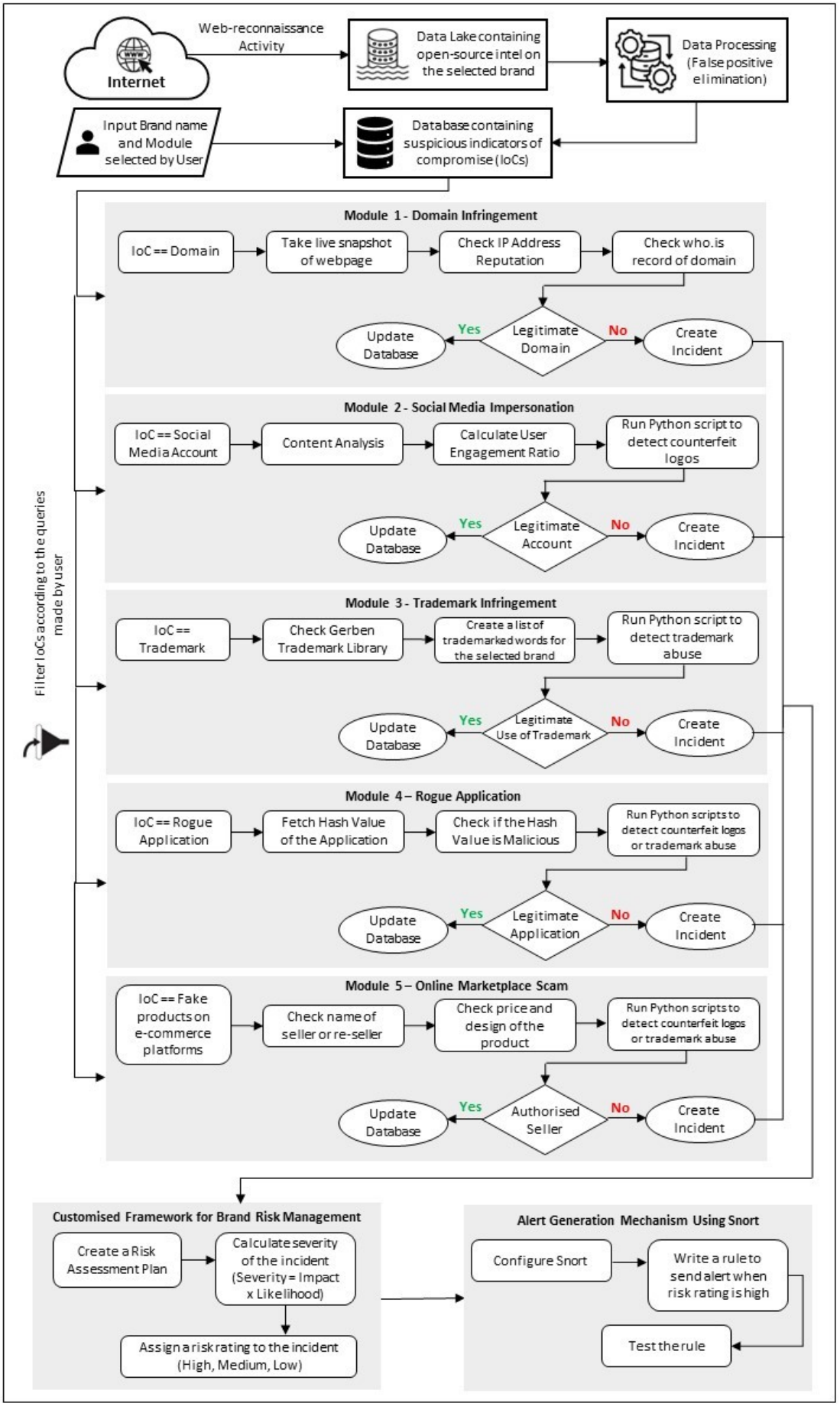


FIGURE 3.1: Workflow Diagram of Scamsweep's Backend Architecture

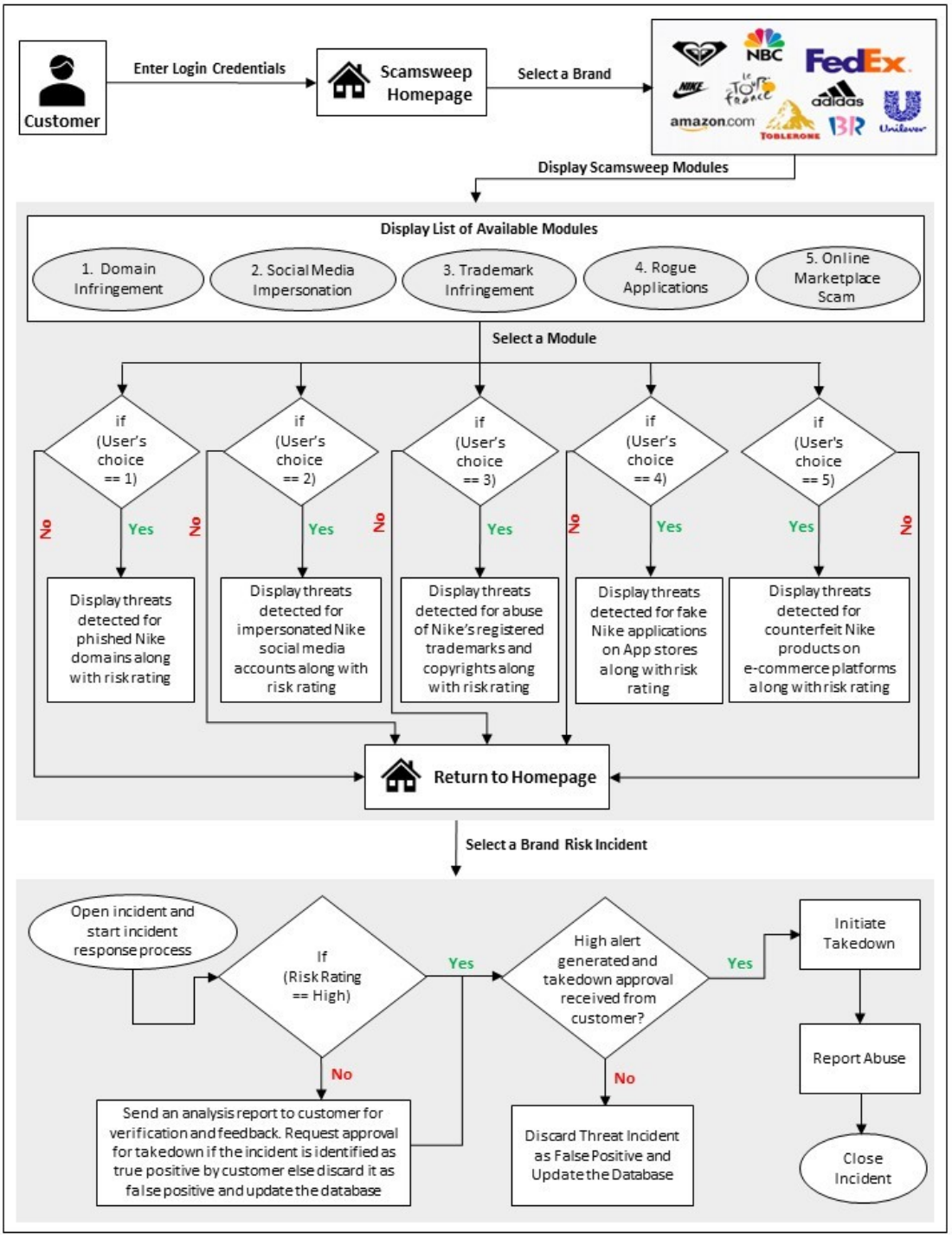


FIGURE 3.2: GUI Workflow Diagram of Scamsweep's Front-end Architecture (to be implemented in future)

Chapter 4

Implementation

This chapter covers the key elements in the implementation of Scamsweep. The goal here is to discuss the interesting features and relevant implementation components of the project, which requires an in-depth examination of a number of key characteristics present in an open-source brand protection solution.

4.1 Important Features: Executing the Vision

This section consists of implementation cycle of all the features present in the toolkit. Given below is the outline followed for each feature:

1. **Challenges in Implementation:** Brief description of any problems that were discovered during the implementation of this component. A description of issues created or fixed by this feature.
2. **Impact on Original Project Design:** Indicate how this difficulty affected:
   (a) Architecture of Scamsweep
   (b) Risks to the overall project
   (c) Methodology to develop the project. Any changes made in the original design
   (d) Changes in implementation schedule and original project plan
   (e) Changes in the testing or evaluation strategy
3. **Implementation Details:** Data collection methods, operational logic behind each code generated, steps for threat detection and incident response, development of a customised framework for brand risk management, installation and configuration details of open-source tools used during implementation are all to be referenced here.

4.1.1 Data Collection: Gathering Intellectual Property Assets of a Company

1. **Challenges in Implementation:** Collecting data for an open-source project to create an online brand protection toolkit was challenging. The original sources proposed for data collection plan of this project were Google Dorks and Pastebin. However, one of the key challenges associated with this approach was that Pastebin datasets were mostly outdated or incomplete, thereby making it unreliable for successful implementation. It was also difficult to mine data using Google Dorks, as relevant sources of information were hidden behind passwords or other security measures.

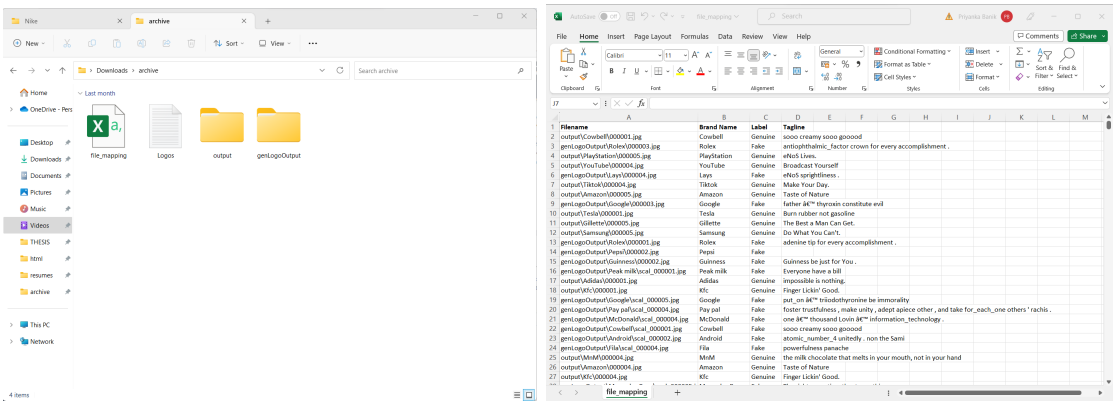
   To overcome these challenges associated with accuracy, company employees were approached for data. One of the major roadblocks faced in this method was that employees were hesitant to share their company's intellectual property assets with an external entity (which as a security best practice, they rightly should be). After a clear communication of project goals and a submission of project proposal draft highlighting the importance of the project, the concerned stakeholder at first expressed genuine interest to help. However, later on there was a lack of cooperation in getting official approvals from other key stakeholders from the higher management due to company's data sharing policies. This was mainly due to an understandable fear, i.e., possible misuse of shared data, further leading to violation of data protection regulations or internal compliance policies. Following up with these corporate employees yielded no fruitful results, thereby impacting the project timeline by causing a delay of 2 weeks.

2. **Impact on Original Project Design:** As a result of the challenges stated above, the original data collection strategy had to be modified slightly. These challenges paved the way for a more thorough research on data mining activities through open-source intelligence and publicly available datasets that foster community projects and learning initiatives. Due to these challenges, we learnt about Kaggle, which is the world's largest data science and machine learning community that allowed users to find enriched datasets, build AI models with powerful tools and resources, all under one platform. Kaggle was extremely helpful in building a database of fake and real logos pertaining to a particular brand.

   Another source of gathering intellectual property assets for this project was the Gerben Trademark Library [60]. Gerben Law Firm is acknowledged by the World Trade Organisation (WTO) for maintaining a regularly updated database of trademarks, copyrights, logos, product designs, brand marketing keywords and descriptors [35].

Although the new data collection strategy delayed the implementation of a centralised data repository for Scamsweep by two weeks, the research conducted during this shift in plan made up for the initial delay. The cumulative information obtained from these two new sources, i.e., Kaggle and Gerben Trademark Library were highly instrumental in achieving the data collection goals laid out for this project. Therefore, the overall impact of this change was a positive one.

3. **Implementation Details:** Scamsweep's central database containing intellectual property assets of various brands can be found here: `https://www.kaggle.com/datasets/prosperchuks/fakereal-logo-detection-dataset` and `https://www.gerbenlaw.com/trademarks/`. The downloded zipped folder "archive" has two sub-folders, i.e., "output" folder for real logo images and and "genLogoOutput" folder for fake logo images in .jpg format (refer Figure refer Figure 4.1(a)). The text file name "Logos" contains a list of brands or organisations whose logos have been captured (refer Figure 4.1(a)). The Excel sheet named "file_mapping" is a data classification spreadsheet that tags each image to a particular brand name and then labels the image as "Genuine" or "Fake" logo (refer Figure 4.1(b)).



(a) Folder name: archive.zip (b) Data Classification Spreadsheet: file_mapping.xls

FIGURE 4.1: Contents of .zip file downloaded from Kaggle

Figure 4.2 is a dated screenshot of the Gerben's IP repository of registered trademarks that are categorised according to the working sector of the industry or brand name. This database of filings is the primary source of information to implement the trademark infringement module designed for Scamsweep.

Additionally, some amount of manual scraping methods were also utilised to gather intelligence pertaining to fraudulent social media accounts, counterfeit products on sale on e-commerce platforms and others. We shall discuss this method in details in the upcoming sub-sections.

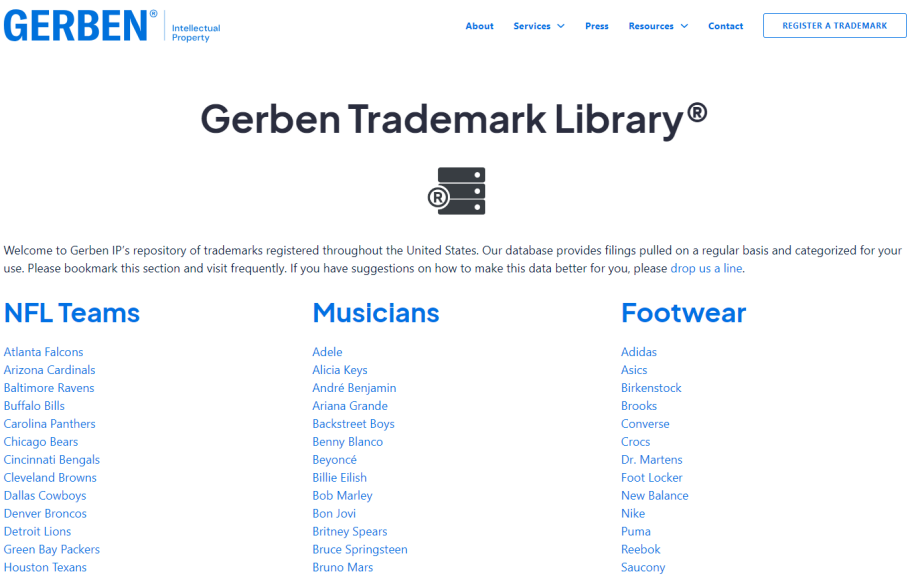


FIGURE 4.2: Screenshot of Gerben Trademark Library as of 11/07/2023

4.1.2 Web-reconnaissance: Scanning the Internet for Domain Names

1. **Challenges in Implementation:** Scamsweep's original design proposed the use of only 2 tools, i.e., Maltego (GUI based tool for Windows users) and Recon-ng (CLI based tool for Linux users) to conduct web-reconnaissance activity. While well-known open-source tools like Maltego can be helpful, there are several difficulties and restrictions that Windows-based users may run into if solely dependent on this one tool. Key challenges associated with community edition of Maltego are:

    - Maltego Community Edition 4.3.1 had limited functionality. The advanced capabilities and features available in the commercial or paid editions remains absent in the free community versions. It offers less access to data sources and APIs compared to the paid editions because it is completely dependant on community contributions. Thus, the outdated database restricts the scope of investigations and limits the amount of information that should be processed and analysed.
    - Maltego Community Edition 4.3.1 has a significantly high rate of false positives, making it unsuitable for commercial setup of any scale. The tool was unsuccessful in detecting a single phished domain that was active or live on the internet, which violated the original evaluation methodology proposed, i.e., if the tool is able to identify even one fake domain, then the proposed reconnaissance methodology would be deemed effective.

Due to the reasons highlighted above, despite adding Maltego to the toolkit, it was essential to find a suitable user-friendly tool that would substitute Maltego Community Edition 4.3.1 while implementing Scamsweep in a GUI-based operating system.

2. **Impact on Project Design:** To make it a more flexible open-source solution, Scamsweep was originally designed to be platform independent, keeping in mind that there is a large number of users in the market who are more comfortable with Windows based platforms, finding it difficult to operate tools in a Linux environment and vice-versa. Therefore, to tackle the challenges created by Maltego, it was necessary to explore other GUI-based reconnaissance tools and add them to Scamsweep's toolkit. These additional tools were mainly implemented to avoid the high false positive rate, thereby making Scamsweep a more competent open-source solution in the market.

   On exploring few popular cloud-native open-source threat intelligence platforms in the information security community, we found 2 feature-rich and user-friendly Software-as-a-Service (SaaS) applications that could potentially replace Maltego and help in conducting a seamless GUI-based reconnaissance activity. The additional GUI-based tools added to the toolkit were:

   - Alienvault - Open Threat Exchange (OTX)
   - Microsoft Defender Threat Intelligence (previously known as RiskIQ Passive Total)

   The introduction of these two new tools not only kept the overall design intact, but also made Scamsweep more efficient and easily accessible.

3. **Implementation Details:**

   A. Implementation of GUI-based Reconnaissance Tools:
   Three tools with a GUI-based interface were added to Scamsweep's toolkit, i.e., Maltego, OTX AlienVault and Microsoft Defender Threat Intelligence for a user to conduct web-reconnaissance on machines having Microsoft Windows or Apple macOS or Google Android as operating systems. Below is a summary of implementation steps followed for these 3 tools:

   • *Maltego*: Go to `https://www.maltego.com/maltego-community/` and download Maltego Community Edition 4.3.1. On successful installation and accepting the terms of service, the tool gets ready to be used. The implementation begins by creating a "New Graph" and finding a relevant top-level domain (TLD) pertaining to the target brand or organization. For example, the ".com" in the domain "maltego.com" is called top-level domain. The tool has a feature to extract all

the publicly available data (domain names, DNS records, email addresses, contact numbers, files uploaded on web, etc.) pertaining to the target domain, which is accomplished by running "All Transforms" as shown in Figure 4.3.

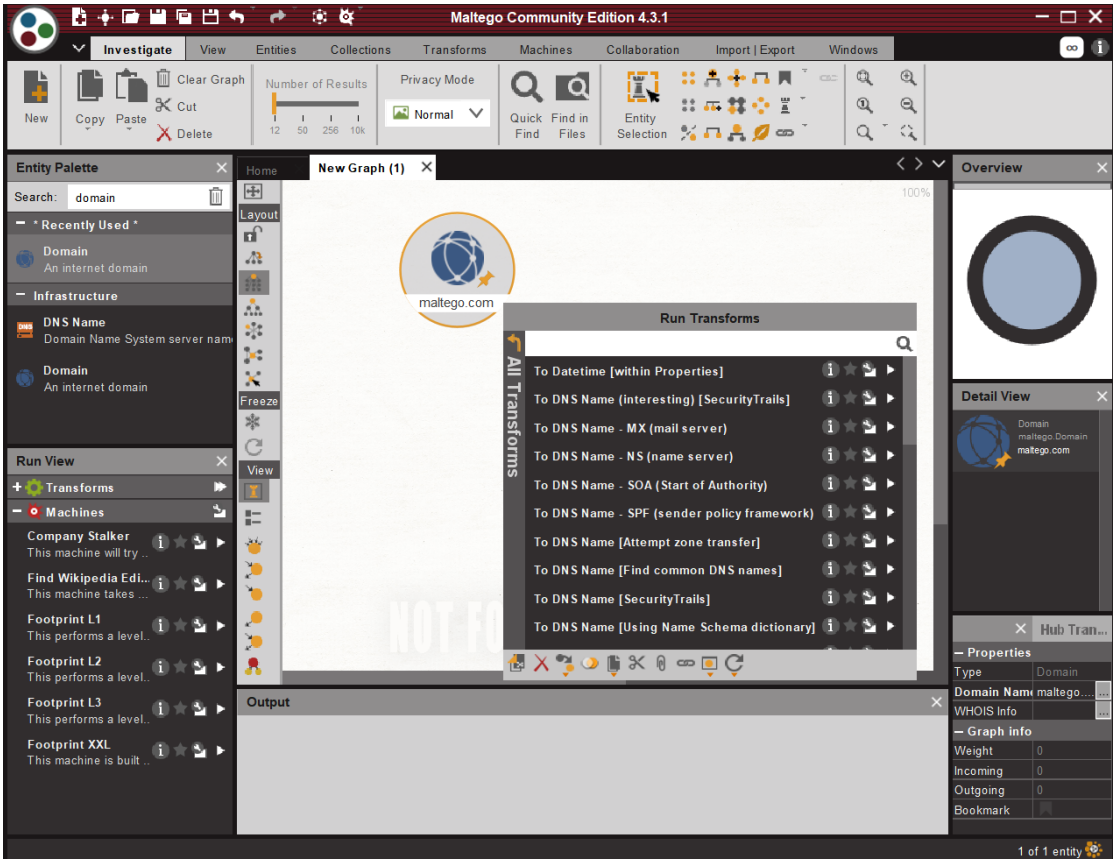


FIGURE 4.3: List of transforms that can be run on maltego.com

• *OTX AlienVault*: Go to `https://otx.alienvault.com/`, and enter the TLD or the brand name to be searched. Signing up and creating a user account is an optional source to gather intelligence from this tool.

• *Microsoft Defender Threat Intelligence*: Go to `https://ti.defender.microsoft.com/`. For accessing the community edition of this tool, it is mandatory to create an account. On a successful login, enter the TLD of the brand to be searched.

Both OTX AlienVault and Microsoft Defender Threat Intelligence provided additional information such as: details of the domain owner, domain registrar, IP geo-location, organization name and others.

B. Implementation of a CLI-based Reconnaissance Tool:

• *Recon-ng*: Recon-ng being a Linux native tool has distinct resource allocation processes, file system structures, which essentially required the installation of a Kali Linux virtual machine to run its modules. This OSINT tool can be installed

by using *sudo apt install recon-ng* and then can be opened on another Kali Linux terminal by running the command *$recon-ng* as seen in Figure 4.4.

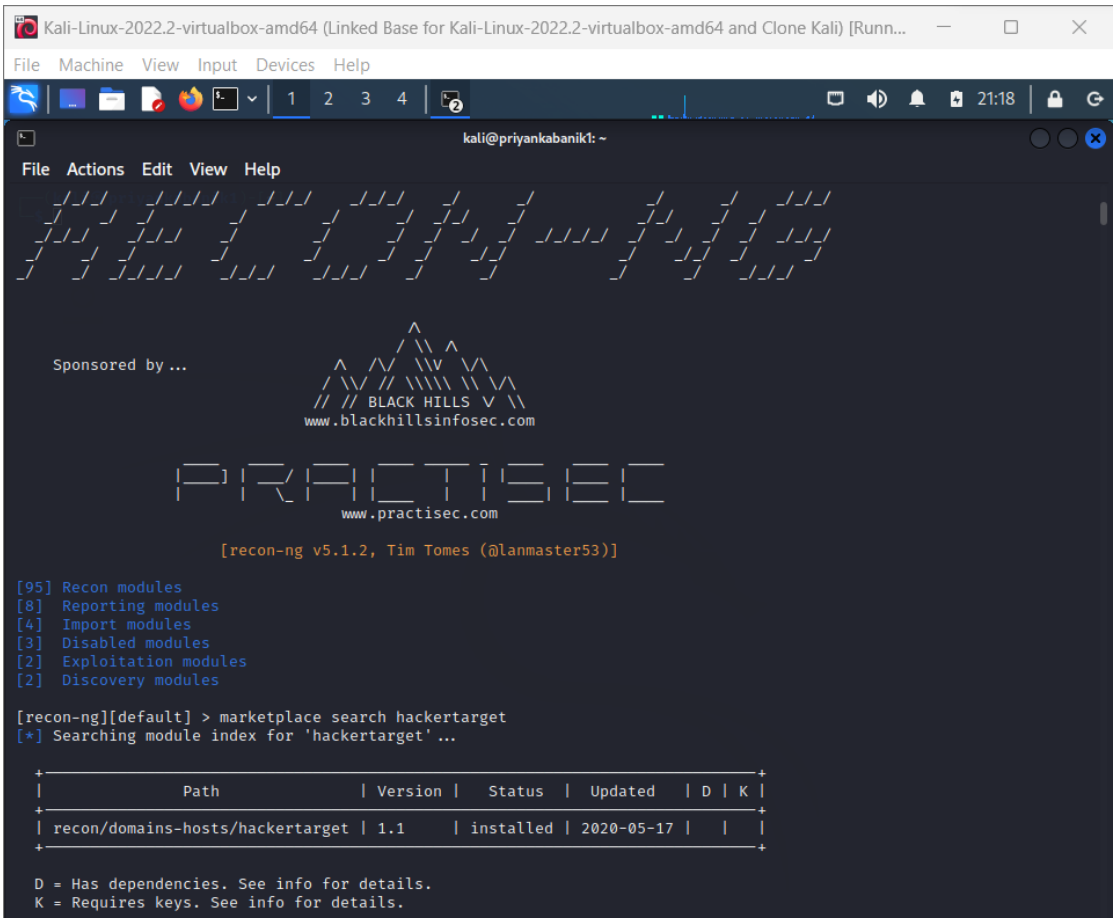


FIGURE 4.4: Successful installation of Recon-ng and HackerTarget module

Recon-ng also has an in-built marketplace that contains several modules depending on the type of information being gathered. The HackerTarget module was ingested to perform web-reconnaissance activity (refer Figure 4.4). The source of scan can be changed from default to target domain name (such as: example.com) as per user's choice. Once the target domain has been set, the HackerTarget module is run to get a list of associated domains, sub-domains, IP addresses, geo-location, organization details, etc.

Here is a list of commands to initiate the scan:

- *help*: To view the key features of this tool.
- *show*:To see the names of tables stored in Recon-ng database.
- *marketplace install all*: To install all modules stored in the marketplace. It is a good practice to refresh once using the *marketplace refresh* command prior to installation.

- *marketplace search hackertarget*: To search for the HackerTarget module on Recon-ng's in-built marketplace (refer Figure 4.4).
- *modules load recon/domains-hosts/hackertarget*:To load the domains-hosts entity present within the module (refer Figure 4.5).
- *info*: To view version details of the ingested module (refer Figure 4.5).
- *options set SOURCE example.com*: To change the source domain from default to example.com (refer Figure 4.5).
- *run*: To run the ingested module and generate output (refer Figure 4.5).

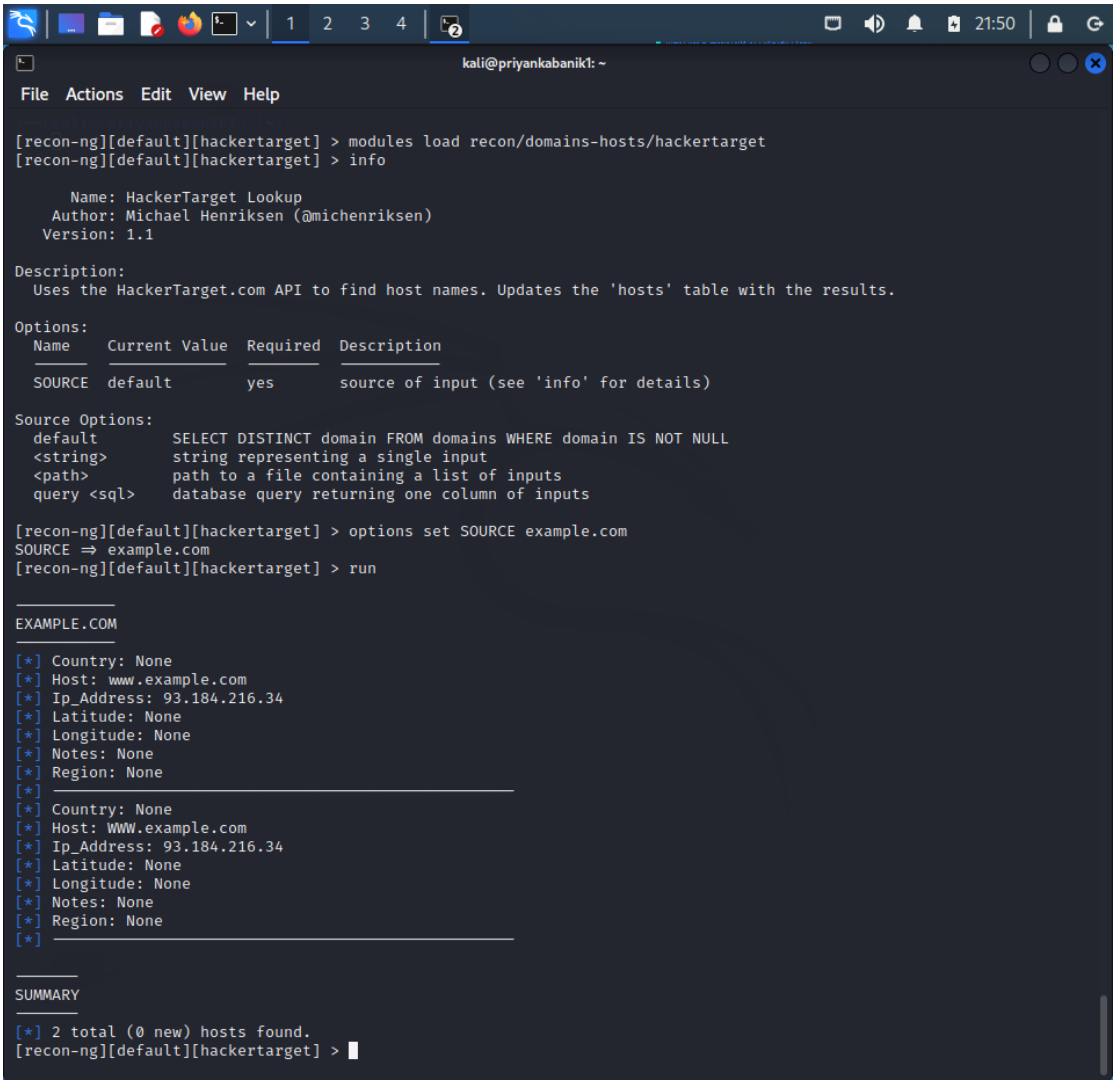


FIGURE 4.5: Recon-ng's output on scanning for example.com

The end goal of using these tools is to gather as many domain names or websites possible to implement the Domain Infringement module. All the intelligence collected from multiple sources are to be organised, processed (filtering out empty cells, duplicates removal) and finally consolidated into a spreadsheet, which shall

act as a threat library or database while implementing the use case to detect phished domains.

It is to be noted that the primary difference between the Data Collection phase and Web-reconnaissance phase is that during "Data Collection" we only gathered already simulated data or pre-built data-sets of intellectual property from sources like Kaggle and Gerber Trademark Library. However, during "Web-reconnaissance" we ran multiple tools to fetch information and then created a data-set of actionable intelligence from scratch.

4.1.3 URL Analysis: Checking Reputation of a Domain or IP Address

1. **Challenges in Implementation:** The original plan for conducting URL analysis was to develop an anti-phishing model by integrating the User Media API that allows access to the user's camera and microphone for capturing live snapshots of the webpage. While modern browsers including Chrome, Firefox and Safari do have support for the User Media API, however, requesting access to user's camera and microphone can be intrusive and raise privacy concerns, especially when visiting a phishy or malicious URL. Therefore, as a security best practice it was essential to necessitate an alternative sustainable approach.

2. **Impact on Original Project Design:** The limitation did not significantly impact the initial design of the anti-phishing model. Instead, it provided an opportunity for improvement, resulting in a simplified version of the previous model. For capturing the live snapshot of a webpage, we found an open-source online sandbox named UrlScan.io that helps analyze and scan URLs for potential security threats and risks. It is commonly used by security researchers, web developers and organizations to gain insights into the safety and reputation of specific web addresses. When a URL is submitted to URLScan.io, it initiates a scan to perform various security checks and provide a detailed report on potential threats and vulnerabilities associated with the website or webpage.

3. **Implementation Details:** Scamsweep's algorithm for conducting URL analysis consists of 5 crucial steps:

    - Select a suspicious looking domain from the dataset created post web reconnaissance activity.
    - Enter the domain on `https://urlscan.io/` and hit the "Public Scan" button. The tool examines the behavior of the URL in a controlled environment,

analyzing requests, responses and potential interactions with malicious entities to detect and alert on potential dangers. It also resolves the domain name into its corresponding IP address and generates a live snapshot of the webpage.

- Analyse the snapshot manually. Look for suspicious indicators like: counterfeit logos, trademarks, keywords, exposed email addresses, contact numbers and others.
- Check the geo-location, sender IP reputation (Trusted, Neutral, Poor or Unknown), block lists of the resolved IP address on Cisco Talos Intelligence (`https://www.talosintelligence.com/`)
- Conclude whether the threat detected is true-positive or false-positive incident, i.e., the suspicious domain identified is malicious or not based on the above investigation steps.

4.1.4 Text Analysis: Different Methods of Comparing Strings

1. **Challenges in Implementation:** Scamsweep's original implementation strategy to deploy the text analysis feature was a manual approach, which made it a labour intensive and challenging task. It was time-consuming and impractical to manually examine large volumes of text. As the volume of the text data-set increased, it was getting difficult to maintain precision and uniformity. It was observed human analysts introduced their own subjectivity and biases while interpreting text data. Different analysts interpreted the same text differently, leading to inconsistent results. Also, human error is inevitable when conducting manual analysis of texts. Errors like: overlooking typos, special characters or misinterpretations, could introduce inaccuracies in the analysis results. So, it was important to establish clear guidelines to minimize these issues that would make Scamsweep a more reliable toolkit in the market.

2. **Impact on Original Project Design:** The original project design was to manually scrape the internet and create a list containing potential abuse of trademarks and then compare this with a list of authentic trademarks (fetched from Gerben Trademark Library) using the VLOOKUP function in Microsoft Excel. However, VLOOKUP function had several limitations as follows:

   - Exact match lookups conducted by VLOOKUP led to false-positive errors if exact matches were not found.
   - Case-insensitivity of VLOOKUP caused unintended matches or mismatches.

- Structural changes in the lookup range, like inserting or deleting columns broke VLOOKUP formulas, yielding incorrect results.
- #N/A error in VLOOKUP lacked specific details for troubleshooting.
- Volatility of VLOOKUP caused frequent recalculations with any changes made in the spreadsheet, impacting performance, especially with large datasets or complex formulas.

Due to the above reasons, the original design became a tedious and time consuming method for conducting text analysis of brand keywords, making it unsuitable to be added as an implementation feature in the toolkit. Therefore, it was essential to automate the original design by putting together the human logic or way of thinking while analysing a text into a Python script. This automated method was a more concrete way to tackle any business use case pertaining to violation of registered trademarks, marketing keywords or descriptors of a particular brand.

3. **Implementation Details:** The feature for detecting trademark infringement was implemented through an automated method to conduct text analysis. A code was developed on Google Colab platform by leveraging the difflib and re libraries available in Python. All the fundamental elements that a user can think about when manually comparing strings were taken into account by this code.

   The code aims to check for trademark infringement in a user's input text by comparing it against a predefined list of trademarked words associated with a specific brand or company. It begins by defining the list of trademarked words obtained from the Gerben Trademark Library. To facilitate accurate comparison, a preprocessing function is created, which ensures that the user input contains only alphanumeric characters and whitespace. The main trademark infringement checking function then iterates over each trademarked word and pre-processes them for consistency. It also handles typographical errors and phonetically similar alphabets into consideration by utilizing the "SequenceMatcher" class from the "difflib" library while calculating the similarity ratio. The code compares the strings character by character and looks for matching sub-string. It considers the possibility that a character in one sequence may correspond to a different character due to a typographical error. By identifying the longest matching sub-string, it can capture and account for minor differences caused by typos or misspellings. The "SequenceMatcher" class treats each character as an atomic element and does not inherently have built-in support for phonetic similarity. However, if two phonetically similar alphabets are represented by the same character in the strings being compared, it would be considered as matching characters. For example, if "k" and "c" have the

same phonetic representation in the context of the comparison, they would be considered a match if they appear in the corresponding positions of the sequences.The "ratio()" method of the "SequenceMatcher" class calculates a similarity ratio between the two texts. The similarity ratio threshold (local variable "x" set at 0.5 or 50%) determines if there is a potential trademark infringement. The threshold (x) is set to an unbiased metric of 0.5, leaving a fair room for benefit of doubts in case of different interpretations by users for different brand names. The value of x can be adjusted as customer's requirement. If the user input exceeds the threshold with any trademarked word, it indicates trademark infringement and the code prints the similarity ratio and returns "True". Otherwise, it prints the similarity ratio and returns "False", indicating no infringement. The code prompts the user to enter a text, invokes the trademark infringement check function and displays the result, indicating whether the input shows trademark infringement or not. Figure 4.6 is a snippet of how the code "trademark_infringement.py" analyses texts by iterating through the list of trademarked words and calculates the similarity ratio after pre-processing the user input. See Appendix **B.1** to view the full code.

trademark_infringement.ipynb ☆

File Edit View Insert Runtime Tools Help All changes saved

+ Code + Text

```
[9] # Function to preprocess the text by removing special characters
    def preprocess_text(text):
        # Remove special characters using regular expression
        processed_text = re.sub(r"[^\w\s]", "", text)
        return processed_text

    # Function to check for trademark infringement
    def check_trademark_infringement(user_input):
        # Preprocess the user input and convert it to uppercase for comparison
        user_input_processed = preprocess_text(user_input).upper()

        # Iterate over each trademark word
        for word in trademarked_words:
            # Preprocess the trademark word and convert it to uppercase for comparison
            trademark_word_processed = preprocess_text(word).upper()

            # Compare the user input with the trademark word, accounting for typographical errors
            similarity_ratio = difflib.SequenceMatcher(None, user_input_processed, trademark_word_processed).ratio()
            x=0.5 # The value of x can be changed and the threshold value is variable
            # Check if the similarity ratio is above a threshold (adjust as needed)
            if similarity_ratio >= x:
                print(f"The similarity ratio: {similarity_ratio:.2f}")
                return True
                break

        print(f"The similarity ratio: {similarity_ratio:.2f}")
        return False

    # Get input from user
    user_input = input("Enter a text: ")

    # Check for trademark infringement
    if check_trademark_infringement(user_input):
        print("Trademark infringement observed.")
    else:
        print("Not a trademark infringement.")
```

FIGURE 4.6: Code Snippet: trademark_infringement.py

4.1.5 Image Processing: Differentiating between Real and Fake Logos

1. **Challenges in Implementation:** The original design of the code was to use the OpenCV library was to read two logo images, i.e., image1.jpg and image2.jpg, of which image1.jpg is real logo and image2.jpg is fake. The code checked if the shapes of the two images are equal. The "shape" attribute in OpenCV represents the dimensions of the image as a tuple (height, width, channels), where height is the number of rows, width is the number of columns, and channels is the number of color channels in the image (for example, channel value is 3 for RGB images). If the dimensions of the two images were an exact match, then the code returned "True", indicating that the two images are similar. The challenge here was that this code only verified the dimensions of the image and was unable to extract the contents within the image. Therefore, this logic failed while comparing two visually similar images, which required more advanced image processing technique.

2. **Impact on Original Project Design:** To start writing a script that is capable of recognizing objects within an image, it was essential to first gain a high-level understanding of visual data and learn some basic techniques used in computer vision processing, which was outside the scope of cyber security. This impacted the original project timeline and caused a delay in finishing the implementation of this feature particularly.

3. **Implementation Details:** To counter the limitations of "shape" attribute, several new attributes were implemented to enhance the efficiency of the code. Table 4.1 enlists the functions and modules added from OpenCV library in Python:

Table 4.1: New features added to the Logo Detection capability

Attributes	**Description**
cv2.resize()	This function resizes the input images to a uniform scale
cv2.cvtColor()	This function converts the input images from one color space to another
cv2.COLOR_BGR2GRAY()	This function converts an RGB (Red-Green-Blue) image to grayscale to maintain a uniform resolution
cv2.calcHist()	This function creates histograms of input images with a typical range of 0-255 for grayscale images
cv2.flatten()	This function converts the multi-dimensional array into a one-dimensional array of feature vectors extracted from the input images
cv2.compareHist()	This function compares two histograms
cv2.HISTCMP_CHISQR()	This function computes the Chi-square distance between two histograms, which measures the dissimilarity between the histograms

It is to kept in mind that this code has limitations and it may not be an exhaustive or full-proof way to detect fake logos. Limitations of the code and its overall impact on performance of the toolkit has been discussed in details in Chapter 6. See Appendix **B.2** to view the full code.

4.1.6 Social Media Analysis: Calculating User Engagement Ratio on Social Media Platforms

1. **Challenges in Implementation:** The original design was to monitor the social media traffic of a particular brand by setting up Google Alerts. While Google Alerts is a useful tool for monitoring online content, it is primarily designed for sources like websites, blogs, books, videos and news articles. It does not have any option to customise the alert for filtering content from social media platforms like Facebook, Instagram and Twitter in particular. As shown in Figure 4.7, we set up a trial alert for Ryanair flights with a frequency of one alert per day to receive updates on their digital footprints. However, this gave no alerts or leads which could be utilised in automating the process of gathering relevant social media search results, i.e., account or profile names, hashtags, insights, etc. when a keyword related to a brand is entered. Also, the scheduled frequency of the trial Google Alerts overwhelmed our inbox with false positive alerts. Therefore, this strategy of gathering automated social media analytics was a failed experiment.

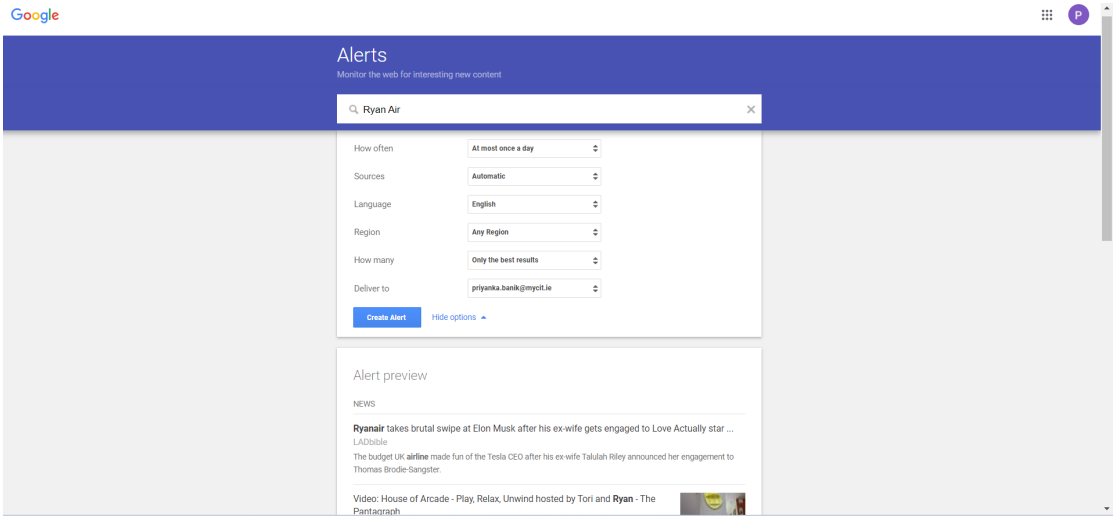
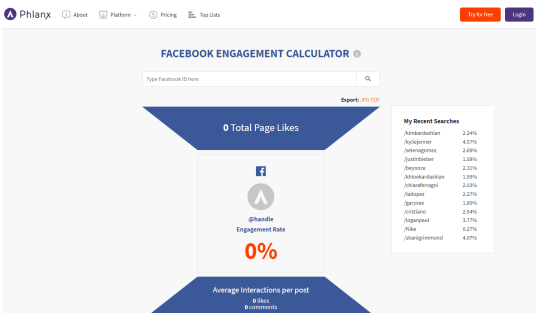


FIGURE 4.7: Setting up a trial Google Alert for Ryanair

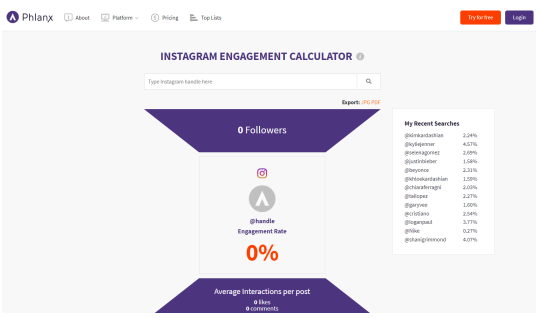
2. **Impact on Original Project Design:** The immediate impact of the challenges discussed above were that we had to shift from an automated method to a manual method of processing the social media search results. The marketing keywords in the search boxes of various social media platforms were entered and the search

results were filtered manually. We created a list of Facebook pages, Instagram accounts and Twitter handles that looked remotely suspicious. We also used a tool named Phlanx to analyse the social media activity of the target brand that had an embedded algorithm for calculating the user engagement ratio (based on the number of followers, posts, likes, comments and shares pertaining to that user profile). This ratio was helpful in determining whether the rate of activity was high or low. So, if a fake account has high rate of activity then it poses a greater threat on the target brand as compared to a dormant fake account.

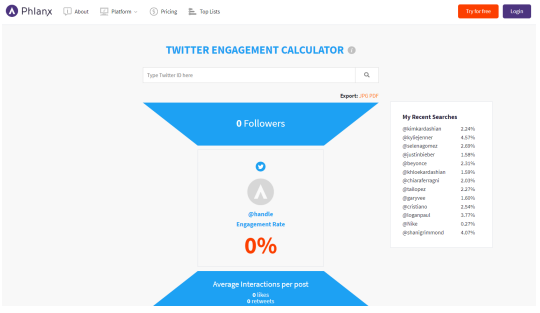
3. **Implementation Details:** To implement this feature, the first step involved was the conducting of comprehensive searches on various social media platforms such as Facebook, Instagram, Twitter or YouTube by entering relevant marketing keywords (in the search box) associated with the target company or brand. In the second step, a carefully curated list of potentially suspicious social media accounts was compiled, taking into account a thorough analysis of their content posted online. The content analysis phase included identification of any instances of illegal usage of registered logos or trademarks related to the subject brand on social media. For the identification of fake logos or trademark infringements, Python scripts discussed in previous sections were utilized.



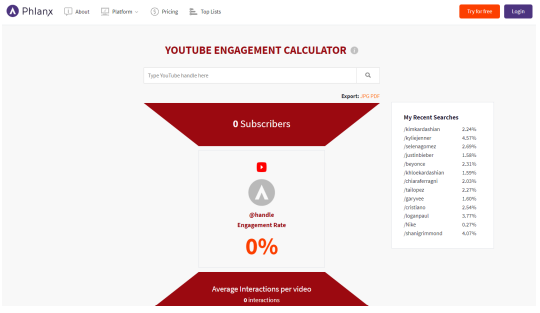
(a) Phlanx's Facebook Engagement Calculator



(b) Phlanx's Instagram Engagement Calculator



(c) Phlanx's Twitter Engagement Calculator



(d) Phlanx's YouTube Engagement Calculator

FIGURE 4.8: Phlanx's customized calculators developed for different social networking platforms like Facebook, Instagram, Twitter and YouTube

Once the list of suspicious accounts was prepared, the final step involved using Phlanx's specialized calculators tailored for different social media platforms as shown in Figure 4.8. By inputting the obtained profile names into their respective calculators on `https://phlanx.com/`, the user engagement ratio was determined. Additionally, Phlanx offers the option to generate a comprehensive social media audit report, accessible through a 30-day trial premium version upon registration. The detailed audit report aids in obtaining valuable insights and metrics for further analysis and decision-making regarding the investigated brand's social media presence and engagement. This step has been kept optional as the registration process involved providing financial information like credit card details. Therefore, level of insights desired has been left to user's discretion.

4.1.7 Malware Analysis: Reverse Engineering of Rogue Applications

1. **Challenges in Implementation:** Detecting malicious applications without being provided an authorised list of whitelisted applications by customer is difficult. It is quite challenging to find malicious applications on Android or Apple app-store because these platforms already check the hash value as a screening test before uploading any new application.

2. **Impact on Original Project Design:** The original design served to verify the authenticity of mobile applications only. So, due to the above challenge, we were unable to download any sample malicious application directly from the app-store. This impacted the scope of the design, which had to expanded from suspicious mobile applications to any suspicious programs, processes or executables (.exe files) detected.

3. **Implementation Details:** Two tools were downloaded and installed to perform blackboxing techniques on the malicious application, i.e., HashCalc and PEStudio. The purpose of HashCalc was to fetch the hash value of the suspicious application and PEStudio was to gather a wealth of information on the IOCs, libraries imported, embedded strings and other resources residing in the source code of the application being investigated. Additionally, PEStudio also integrated VirusTotal results and MSDN searches to identify the behaviour of the malware sample.

   For running a trial on the proposed investigation methodogy, a malware sample was downloaded from GitHub (Link: `https://github.com/Anila-Mjeda/MalwareInvestigations/blob/main/Malware_Investigations_Assignment_1.7z`). The file was first uploaded on HashCalc to determine the SHA256 hash value (refer Figure 4.9).

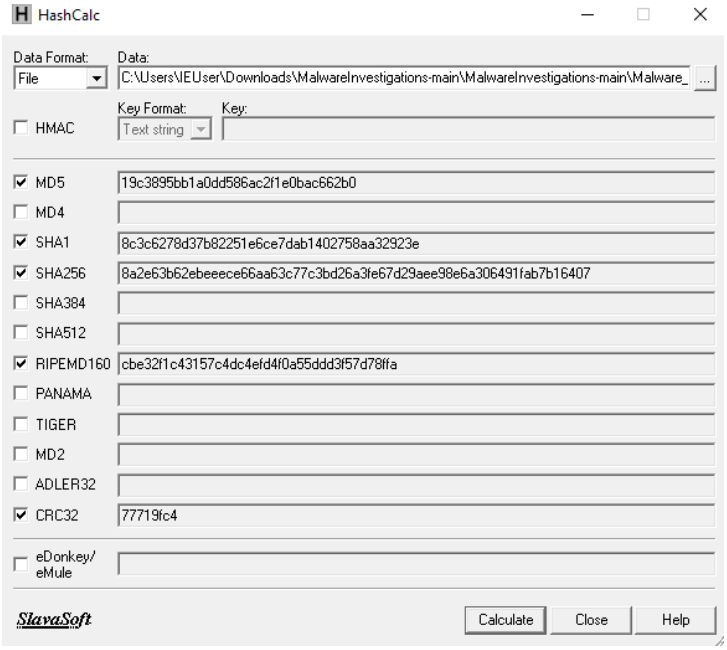


FIGURE 4.9: HashCalc tool for calculating the hash values of malware sample in MD5, SHA1 and SHA256 algorithms

The SHA256 hash value was then fed into PEStudio to verify whether it successfully detects it to be malicious or not. The tool found 55 IOCs, 83 imports, 7173 strings, 25 resources and 7 libraries embedded in the malware (refer Figure 4.10).

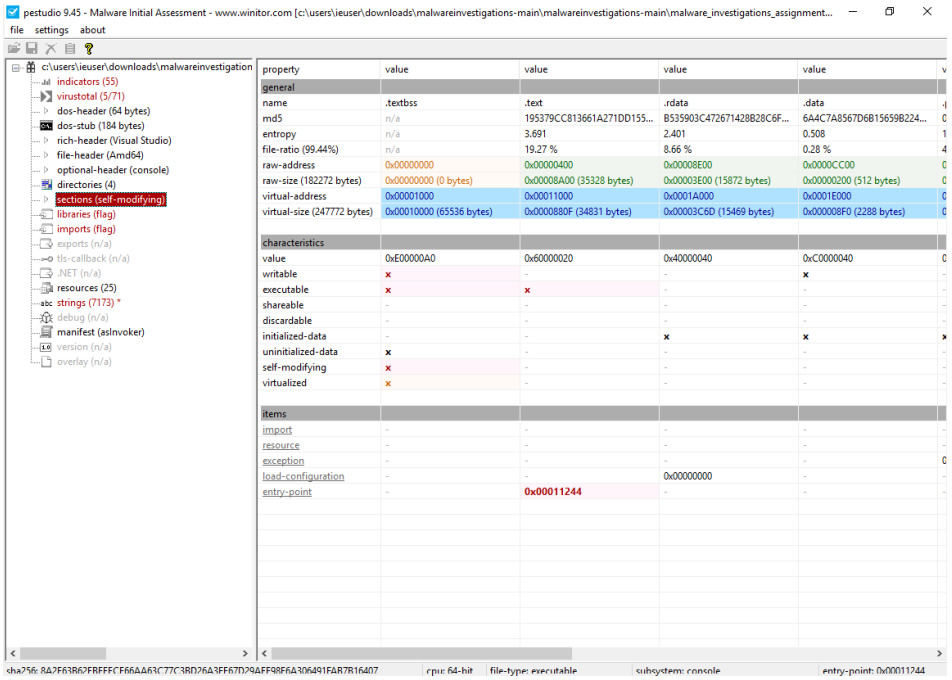


FIGURE 4.10: PEStudio tool for understanding the characteristics of malware sample

The libraries detected were: kernel32.dll, advapi32.dll, shell32.dll, ucrtbased.dll, urlmon.dll, user32.dll and vcruntime140d.dll, of which PEStudio flagged urlmon.dll

as suspicious. The tool also identified the characteristics and behaviour of malware sample, i.e., writable, executable, shareable, discardable, initialized-data, uninitialized-data, self-modifying and virtualized. Additionally, PEStudio also gave a VirusTotal rating of 5/71, meaning 5 out 71 security vendors rated this file to be malicious. As a result, it was verified that the 2 implemented tools effectively offered ample insights to draw reasonable conclusions when examining any given sample.

4.1.8 Risk Assessment: Developing a Framework for Analysing Risks Critical to Brands

1. **Challenges in Implementation:** Choosing the correct risk assessment framework for online brand protection can be a complex task, given the unique challenges and dynamics of the digital landscape. To assess risks effectively, the frameworks such as: NIST CSF, ISO 27001 and FAIR may require access to client-sensitive data, which was difficult to obtain during the data collection phase. So, if we decide to implement any one of these frameworks in its entirety, then we should have access to accurate data and tag or classify them into correct categories. Depending on these categories, we should also implement all the associated controls and sub-controls defined in the framework and keep it open for a quarterly or annual audit as per security best practices. Performing these activities were a clear-cut deviation from online brand protection as these tasks streamlined more into the GRC (Governance, Risk and Compliance) side of information security. Another problem with implementing an industry acknowledged framework is that it should also consider the local laws and data protection regulations, which changes with geographical locations (as threats can originate from any part of the world).

   Our primary motive behind implementing a risk assessment framework was to quantify the threats identified by assigning it a risk rating post investigation on the target brand. Somehow, this objective was not being fulfilled if we chose to implement any one particular industry acknowledged framework. Therefore, it was essential to come up with a simple customised framework, which focuses only on calculating the risk rating, i.e., high, medium or low (depending on defined thresholds) for the identified attack vectors.

2. **Impact on Original Project Design:** These challenges made it inevitable to reconsider the original plan of choosing any one particular framework from NIST CSF, ISO 27001 or FAIR. However, this change in design had a positive impact on the project timeline and conveniently made up for the time lost earlier in choosing the most suitable framework. The implementation process became less

complex when we opted for a tailored approach by leveraging the strengths of each framework. This hybrid approach allowed us to combine elements from multiple frameworks and create our own customised risk assessment and brand protection strategy that aligned closely with Scamsweep's unique features and capabilities. Additionally, we also mapped the tactics and techniques used by the brand abusers to a whole new framework, i.e., the MITRE ATT&CK Framework.

3. **Implementation Details:** Figure 4.11 is a tabular representation of the customised risk assessment framework that has been designed on Microsoft Excel to assess and rate the risk level for different use cases related to potential threats affecting a brand's reputation in the digital space. The framework consists of several use cases, each representing a specific threat scenario and each use case is associated with various indicators, conditions and observations. The goal is to evaluate the likelihood and potential impact of the threats based on these indicators and conditions.

   The structure of the framework is as follows:

   - *Use Cases*: Each serial number represents a different use case, such as Domain Infringement, Trademark or Copyright Infringement, Social Media Impersonation, Rogue Applications and Online Marketplace Scam. These use cases are potential scenarios where brand risks may occur.
   - *MITRE ATT&CK Mapping*: The "Tactic" and "Technique" columns are left empty in the provided table, but in practice, these columns would map specific threat tactics and techniques from the MITRE ATT&CK framework to each use case.
   - *Source of Indicator*:This column mentions various sources where indicators related to the specific use case can be found. For example, it includes tools like Maltego, Recon-ng, OTX Alienvault, and Microsoft Threat Defender Intelligence. It also includes social media and e-commerce platforms like, Facebook, Instagram, Amazon, Flipkart, etc.
   - *Threat Indicator*: This column indicates the specific element being assessed in each use case, such as Domain Name, Text Detected, Account Name, Application Name or Product Name.
   - *Conditions and Observations*: The framework lists several conditions that need to be checked for each threat indicator. There is also an observations column corresponding to each condition. If the condition is satisfied, then the observation would be "Yes" and if the condition is not satisfied, then the observation would be "No".

- *Impact, Likelihood, Risk Rating and Total Score*: For each condition, there are corresponding columns to rate the impact (say x) and likelihood (say y) of each threat occurring. If the condition is satisfied, then impact is negative and point allocated for negative impact is 1 point (as negative impact is directly proportional to potential threat or risk, hence score is 1). Similarly, if a condition is not satisfied, then impact is positive or no impact and points allocated for positive impact is 0 points. We also quantify the likelihood of occurrence of the use case being examined, i.e., 1 point if the condition is very likely to occur again, 0 points if the condition is rare and not likely to occur again in future. The sum of impact (say I) and the sum of likelihood (say L) are also calculated. As we already know, the formula for calculating the score of risk is: *Risk Score = Impact (I)* x *Likelihood (L)*
  Therefore, on calculating the product of I and L for each use case, the risk score for that use case is determined.

Sl. No.	Brand Risks	MITRE ATT&CK Mapping	Source of Indicator	Threat Indicator	Conditions	Observations	Impact (x)	Likelihood (y)	Risk Rating
1	Domain Infringement	Tactic: Technique:	• Maltego • Recon-ng • OTX Alienvault • Microsoft Threat Defender Intelligence	Domain Name:	Is the target brand name present in URL or domain name, whose resolved IP reputation is poor?	Yes / No	0 or 1	0 or 1	High / Medium / Low
					Does the website contain trademarked words of the target brand?	Yes / No	0 or 1	0 or 1	
					Does the website contain logos similar to target brand?	Yes / No	0 or 1	0 or 1	
					Is the website selling items that look similar to products of the target brand?	Yes / No	0 or 1	0 or 1	
Total Score							I=Σx	L=Σy	I * L
2	Trademark or Copyright Infringement	Tactic: Technique:	• Platform where the text was observed in use	Text Detected:	Found text similar to the registered trademarks of the target brand?	Yes / No	0 or 1	0 or 1	High / Medium / Low
Total Score							I=Σx	L=Σy	I * L
3	Social Media Impersonation	Tactic: Technique:	• Instagram • Facebook • Twitter • LinkedIn	Account Name:	Found text similar to the registered trademarks of the target brand?	Yes / No	0 or 1	0 or 1	High / Medium / Low
					Found logos similar to the registered logos of the target brand?	Yes / No	0 or 1	0 or 1	
					Found items on sale that look similar to products of the target brand?	Yes / No	0 or 1	0 or 1	
					Is the user engagement ratio low?	Yes / No	0 or 1	0 or 1	
Total Score							I=Σx	L=Σy	I * L
4	Rogue Applications	Tactic: Technique:	• Android Playstore • Apple Playstore	Application Name:	Is the hash value of the application malicious?	Yes / No	0 or 1	0 or 1	High / Medium / Low
Total Score							I=Σx	L=Σy	I * L
5	Online Marketplace Scam	Tactic: Technique:	• Amazon • Flipkart • eBay • Etsy • Alibaba • Shopify	Product Name:	Found text similar to the registered trademarks of the target brand?	Yes / No	1	0 or 1	High / Medium / Low
					Found logos similar to the registered logos of the target brand?	Yes / No	1	0 or 1	
					Found items on sale that look similar to products of the target brand?	Yes / No	1	0 or 1	
Total Score							I=Σx	L=Σy	I * L

FIGURE 4.11: Scamsweep's Customised Risk Assessment Framework

Now based on the risk score, we created a 4x4 risk matrix (refer Figure 4.12), also known as heat map that assigns a risk rating, i.e., high, medium or low, to the use case being assessed. Thresholds for each risk rating have been defined as follows:

- If risk score is 0-3, then risk rating is Low
- If risk score is 4-7, then risk rating is Tolerable
- If risk score is 8-11, then risk rating is Medium
- If risk score is 12-16, then risk rating is High

It is to be noted that we have allocated a set of 4 numeric values per risk rating, i.e., Low = 0,1,2,3, Tolerable = 4,5,6,7 and so on. But practically, in a 4x4 matrix

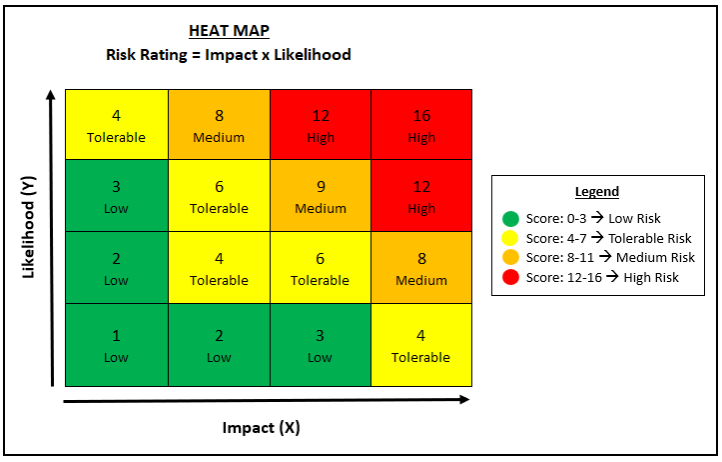


FIGURE 4.12: Heat Map or 4x4 Risk Matrix for Brand Risk Assessment

the product or the risk score can never be 5, 7, 10, 11, 13, 14 or 15 because the maximum number conditions per use case in our framework is only 4, which means that the maximum value on either x-axis (for impact) and y-axis (for likelihood) can only be 4. For example, achieving a risk score of 10 would require an impact rating of 2 and a likelihood rating of 5 or vice-versa, which is beyond maximum rating scale, i.e., 4. Similarly, achieving a risk score of 11 would require an impact rating of 3 and a likelihood rating of 4 or vice-versa, which is within rating scale but does not result in 11, i.e., $3 * 4 = 12$.

4.1.9 Alert Generation: Deploying Snort Rules

1. **Challenges in Implementation:** Implementing Snort rules to generate automated email alerts can be a powerful way to enhance the security posture of a network belonging to the victim organisation. The original plan was to write Snort rules that would deliver automated email alerts if the risk rating for a threat vector is High or Medium. The email would have a pre-defined template and would contain a brand risk analysis report as attachment. However, to execute this plan, it was essential to have a well-configured email delivery system that had access to an SMTP (Simple Mail Transfer Protocol) server for sending the automated email alerts. Configuring and setting up an SMTP server was a complex task because first, it required sufficient powered resources (CPU, memory, disk space) to handle the email traffic. Second, it required deployment of anti-spam measures like SPF, DKIM, DMARC and third, it required proper security measures and authentication mechanisms like SSL/TLS encryption and IP restrictions to prevent relays of spam emails. The lack of infrastructure was the biggest roadblock but it was genuinely difficult to proceed further with the original design without any certified

training or prior work experience in such implementations. Hence, it was essential to revise the originally proposed alert generation mechanism for Scamsweep.

2. **Impact on Original Project Design:** As an impact of the challenges discussed above, the original alert generation mechanism by divided it into two parts:
   i. Write a Snort rule to generate only log messages, that could be treated as an alert or threat notification depending on the risk ratings, i.e., high, medium, tolerable or low. These alerts could be later integrated with an SIEM solution
   ii. Send an email to the target recipient manually, only when the risk rating is high or medium. The email would have a pre-defined template to be included in the body of the message, along with an attached risk analysis report.

3. **Implementation Details:** We first installed Snort using the command *sudo apt install snort* and then created a backup of */etc/snort/snort.conf* file. The purpose of creating this backup was to save the default snort configuration file (*snort.conf*). We used the *cp* command to create a copy of *snort.conf* file stored in path */etc/snort/snort.conf* and *.bakup* extension was used to create a backup file. This was essentially done as a preventive mechanism to handle fatal errors. Here are the commands that were used to first create a backup and then open *snort.conf* file (refer Figure 4.13):
   sudo cp /etc/snort/snort.conf /etc/snort/snort.conf.bakup
   sudo less -N /etc/snort/snort.conf

FIGURE 4.13: Commands to open and create a backup of snort.conf

As shown in Figure 4.14, the total number of commented lines (starting with #) present in *snort.conf* was 607 and to define a local rule on Snort, line number 571 was uncommented (removed #), i.e., *include $RULE_PATH/exploit.rules*.

The *nano* editor was leveraged (Command: *sudo nano /etc/snort/rules/local.rules*) to write the Snort rules. Several issues were encountered before arriving at the correct rule.

Here are some rules that were developed during the implementation phase:

Rule 1: ***alert tcp any any → any any (msg:"Send an email alert to user for High or Medium Risk Rating"; content:"risk_rating: high"; nocase; content:"risk_rating: medium"; nocase; sid:100001; rev:1;)***

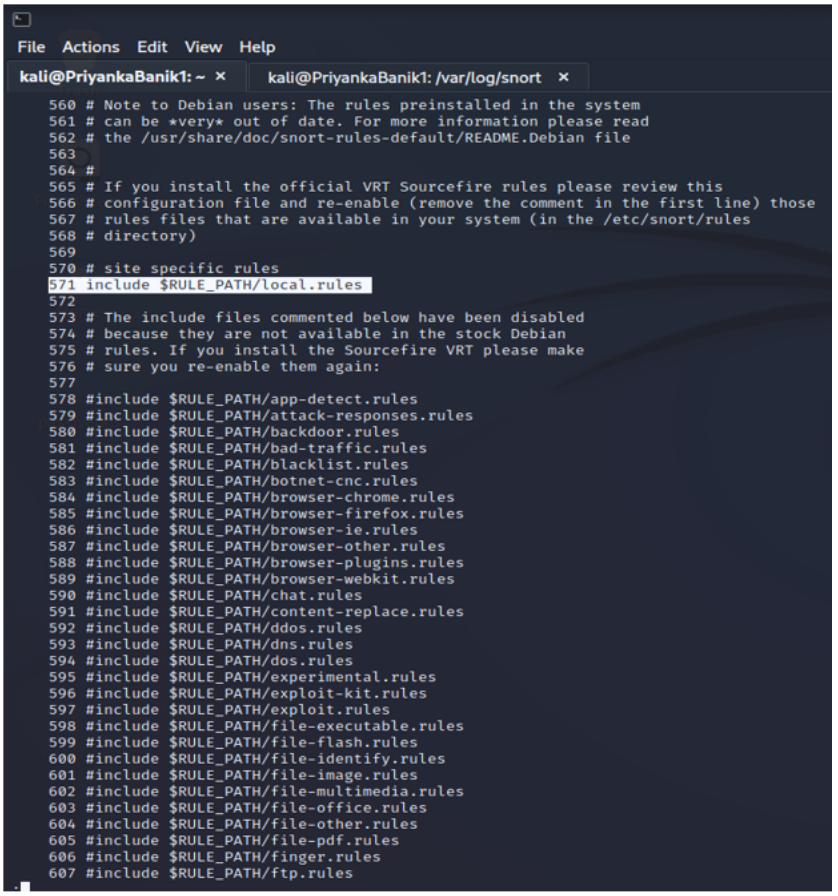


FIGURE 4.14: Screenshot of Snort configuration file as of 25/07/2023

Status: *Not Implemented*

Explanation of the rule:

• *alert*: This keyword tells Snort to generate an alert when the conditions are met.

• *tcp any any → any any*: This specifies the traffic direction, which, in this case, is TCP traffic in any direction (from any source port to any destination port).

• *(msg:"Send an email alert to user if the risk rating is High or Medium";)*: This is the message that will be generated when the rule matches the condition.

• *content:"risk_rating: high"; nocase;*: This checks for the string "risk_rating: high" case-insensitively in the packet payload.

• *content:"risk_rating: medium"; nocase;*: This checks for the string "risk_rating: medium" case-insensitively in the packet payload.

• *sid:100001;*: This is the unique identifier for the rule.

• *rev:1;*: This indicates the revision number of the rule, which can be updated if the rule is modified in future.

It is to be noted that this rule relied on a "risk_rating" field is in the packet payload, which was not present in the actual HTTP header. We tried adding it with Burpsuite to test the rule (refer Figure 4.15) but faced difficulties integrating Snort with Burpsuite within tight timelines. Hence, this rule was discarded.

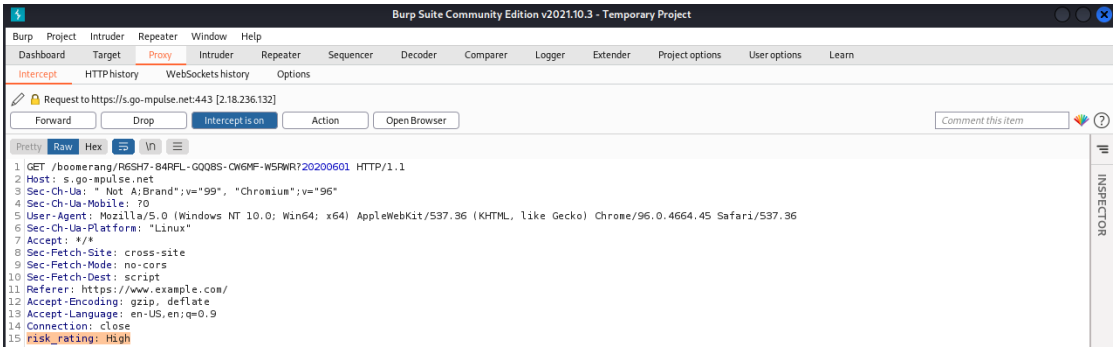


FIGURE 4.15: Added a new HTTP header, i.e., risk_rating

Rule 2: ***alert tcp any any → any any (msg:"Send an email alert to user if the risk rating is High or Medium"; sid:100002; rev:1;)***

Status: ***Not Implemented***

Explanation of the rule:

In response to the difficulties encountered with Rule 1, we decided to eliminate the "risk_rating" field entirely and instead logged a generic text message without any specific conditions. While this implementation was straightforward, it proved highly impractical and lacked logical significance, as there were no predefined conditions to trigger the alert message. Integrating this rule with commercial detection mechanisms such as firewalls, intrusion detection systems (IDS), or Security Information and Event Management (SIEM) tools would result in an excessive number of false positives, rendering it ineffective for practical use in a professional setting.

Rule 3: ***alert tcp any any → any any (msg:"Send an Email Alert to User when the Risk is High"; content:"200"; http_stat_code; flags:AS; classtype:High; priority:1; sid:100003; rev:1;)***

Status: ***Implemented***

Explanation of the rule:

After recognizing the need for an improved implementation of Rule 1, we conducted thorough research for open-source platforms that could facilitate the creation of more proficient Snort rules. Our discovery of Snorpy, a web-based Snort rule creator (`http://snorpy.cyb3rs3c.net/`), proved to be highly valuable. Utilizing Snorpy's pre-defined fields, such as Class and Priority, significantly streamlined rule customization. We set priorities ranging from 1 for High risk to 4 for Low

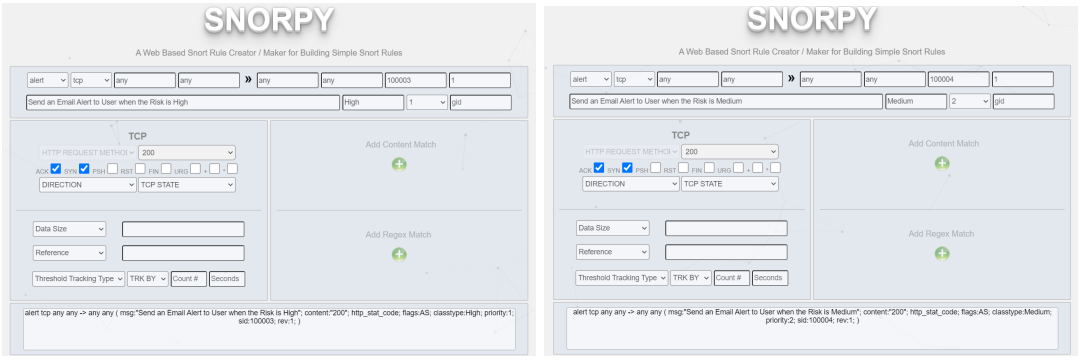
risk. Additionally, we incorporated a condition to verify the HTTP status code as 200, ensuring a successful connection when visiting the target webpage. Integration of TCP flags (SYN and ACK) was also implemented to signify user domain requests and acknowledgments. Ultimately, with Snorpy's assistance, we successfully crafted the rule (see Figure 4.16(a)).

Rule 4: ***alert tcp any any → any any (msg:"Send an Email Alert to User when the Risk is Medium"; content:"200"; http_stat_code; flags:AS; classtype:High; priority:1; sid:100004; rev:1;)***

Status: ***Implemented***

Explanation of the rule:

This rule closely resembles Rule 3, with the only difference being the modification of the priority to level 2 and the class to "Medium" (see Figure 4.16(b)).



(a) Rule created for "High" alerts on Snorpy (b) Rule created for "Medium" alerts on Snorpy

FIGURE 4.16: Rules created on Snorpy

These 2 implemented Snort rules shall be tested in the next chapter, i.e., Chapter 5 to verify whether the rules were triggered and the alerts were generated by Snort.

The next step in implementing the alert generation feature within Scamsweep involves initiating a manual email dispatch to the designated recipient..

See Appendix **D.1** for the email template to initiate the takedown at client side as a part of the incident management procedure.

Chapter 5

Testing and Evaluation

This chapter presents an objective and quantitative evaluation of the features integrated into Scamsweep's final system model. As this project revolves around analysis of intellectual property assets and data, we shall evaluate the Scamsweep model through a Proof-of-Concept (PoC) by subjecting its implemented features to testing on a prominent commercial brand that requires online brand protection for running a business smoothly.

To conduct our evaluations efficiently, we have adopted JIRA's test case template, a widely used test case management platform employed by software developers and testers to monitor progress in agile projects [61]. The test case template used for this project consists of 8 headings, i.e., test ID, tool being tested, testing platform, purpose of testing, testing steps, expected result, actual result and test status. Additionally, to enhance the credibility of our findings, we shall compare the results obtained from manual analysis leveraging Scamsweep's open-source tools with results derived from a commercial tool. This comparison aims to verify the PoC outcomes and ensure the reliability and effectiveness of both approaches in the context of online brand protection.

After careful consideration, the brand selected for the PoC of Scamsweep's model is Nike. The selection of Nike was based on a comprehensive market research and case study, as documented in Appendix **A.1**. The case study played a crucial role in making an informed choice for the testing phase.

5.1 Use Case 1: Data Collection

In Use Case 1, titled "Data Collection" we focus on the process of gathering essential information for Nike's brand protection. The two test cases, Test Case 1.0 and Test Case

1.1, respectively aims to evaluate the effectiveness of using Kaggle for collecting Nike's logos and the Gerben Trademark Library for acquiring Nike's registered trademarks, ensuring a comprehensive approach to data gathering.

5.1.1 Test Case 1.0: Testing Kaggle for Collecting Nike's Logos

In Test Case 1.0, we evaluate the use of Kaggle to collect Nike's logos. The purpose of this test is to assess the effectiveness of utilizing Kaggle as a platform for gathering relevant logo data for Nike. The steps involve accessing Kaggle, searching for the appropriate dataset, downloading the dataset, and verifying its contents.

Test ID:	1.0
Tool:	Kaggle
Platform:	Web-based
Purpose:	To gather Nike's logos using Kaggle.
Steps:	1. Open web browser and go to the Kaggle website (www.kaggle.com). 2. Use the search bar at the top of the Kaggle website to search for "fakereal-logo-detection-dataset" or click on the following link to directly access the dataset page: `https://www.kaggle.com/datasets/prosperchuks/fakereal-logo-detection-dataset` 3. On the dataset page, there is information about the dataset, such as its description, size and number of files. 4. To download the dataset, click on the "Download" button on the right-hand side of the screen. 5. The dataset will be downloaded as a compressed ZIP file. After the download is complete, locate the ZIP file and extract its contents to access the dataset files.
Expected Result:	The dataset downloaded from Kaggle should have at least 1 real Nike logo and 1 fake Nike logo.
Actual Result:	The dataset downloaded from Kaggle had 4 real Nike logos and 8 fake Nike logos
Status:	Pass

5.1.2 Test Case 1.1: Testing Gerben Trademark Library for Collecting Nike's Registered Trademarks

In Test Case 1.1, we assess the effectiveness of using the Gerben Trademark Library to gather Nike's registered trademarks. The purpose of this test is to verify the accuracy and comprehensiveness of the trademark search results provided by the Gerben Trademark Library for Nike's registered intellectual property.

Test ID:	1.1
Tool:	Gerben Trademark Library
Platform:	Web-based
Steps:	1. Open the web browser and navigate to the Gerben Trademark Library website (`https://www.gerbenlaw.com/trademarks/`). 2. Select the brand "Nike" from the "Footwear" section. 3. The search results should display a list of trademarks associated with the term "Nike". Copy these trademarked words in an Excel spreadsheet. 4. Download the logos presented in the Gerben Trademark Library by doing "Save Image As" in .jpg format. These images combined with Kaggle's real logo dataset shall form the final dataset for Nike's real logo collection. 5. Use MS Excel to filter the texts, i.e., marketing keywords or descriptors by removing duplicate trademarked words that belong to Nike. This shall be the final list of Nike's registered trademarked words.
Expected Result:	The Gerben Trademark Library search should provide a list of at least 5 Nike's registered trademarks in total (including both logos and words).
Actual Result:	The Gerben Trademark Library search provided a list of 258 registered trademarked words associated with Nike (`https://www.gerbenlaw.com/trademarks/footwear/nike/`).
Status:	Pass

It is to be noted that this use case is mostly downloading of data. But it has been included under testing because we are validating whether Kaggle and Gerben Trademark Library are good data sources to be included in the final toolkit of Scamsweep.

5.2 Use Case 2: Web-Reconnaissance

Use Case 2, "Web-Reconnaissance" involves conducting comprehensive web-based intelligence gathering for Nike's brand protection. The following test cases, Test Case 2.0, Test Case 2.1, Test Case 2.2 and Test Case 2.3, assess the performance of different tools, namely Maltego Community Edition 4.3.1, OTX Alienvault, Microsoft Defender Threat Intelligence and Recon-ng, respectively. The purpose is to evaluate the efficiency of these open-source tools in identifying potential suspicious domains that pose a threat to Nike's online presence.

5.2.1 Test Case 2.0: Testing Maltego Community Edition 4.3.1

Test Case 2.0 assesses the effectiveness of Maltego Community Edition 4.3.1 in gathering actionable intelligence for Nike's brand protection through web reconnaissance. The test

aims to evaluate Maltego's ability to identify potential suspicious domains and activities associated with Nike to enhance online security measures.

Test ID:	2.0
Tool:	Maltego Community Edition 4.3.1
Platform:	Windows
Purpose:	To gather actionable intelligence on Nike using Maltego
Steps:	1. Launch Maltego Community Edition 4.3.1. 2. Enter the entity name in the "Entity Search Palette", i.e., "Domain" 3. Enter an active top-level domain belonging to Nike, i.e., nike.com 4. Run "All Transforms" for complete graphical visualization on Nike (refer Figure 5.1) 5. Analyze the collected data for relevant information about Nike.
Expected Result:	Maltego should directly give a result of at least 1 active domain related to Nike that looks potentially suspicious.
Actual Result:	Maltego's search results did not directly yield any active suspicious domains associated with Nike. It gave us an indirect lead to a typo-squatting domain, i.e., nike.ink through its finding nike.link (refer Figure 5.1)
Status:	Fail

Observations: The majority of the domains discovered by Maltego were false-positives. The sites either redirected to the parent domain (nike.com) or could not be reached. The latter usually occurs when the server IP address could not be found. Few domains were observed to be outdated/parked, which is harmless or low threat at present but could be picked up by cybercriminals in future for domain squatting. Table 5.1 enlists the findings from Maltego tool as shown in Figure 5.1.

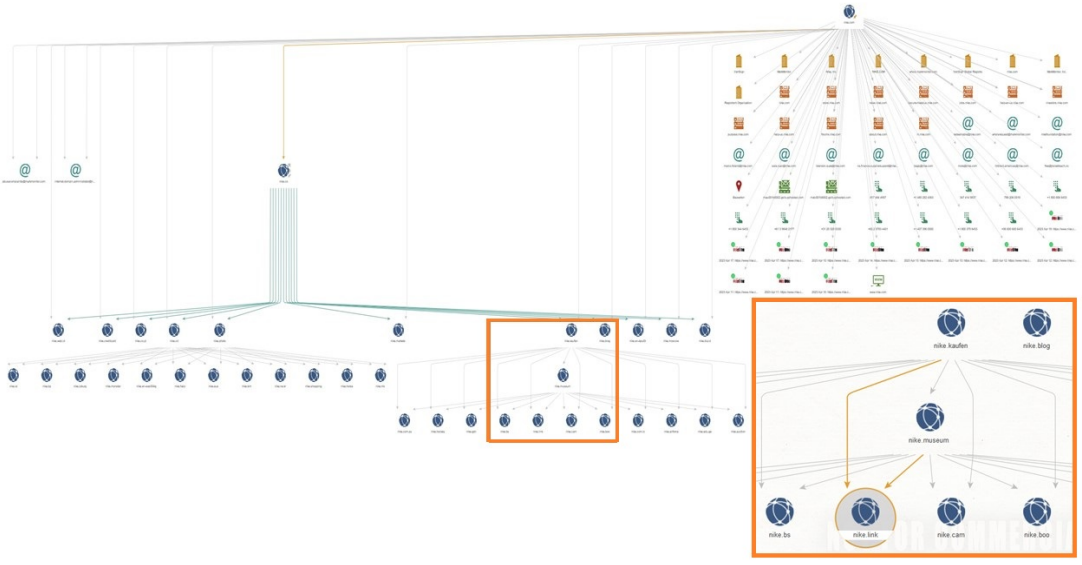


FIGURE 5.1: Maltego's findings on Nike domains with special focus on nike.link

TABLE 5.1: List of Domains and Sub-domains excavated from Maltego

Domain	Sub-domain	Sub-domain Web Status
nike.com	nike.co	Active and redirects to nike.com
nike.co	nike.markets	Active and redirects to nike.com
	nike.kaufen	Site cannot be reached
	nike.blog	Site cannot be reached
	nike.xn–kput3i	Site cannot be reached
	nike.moscow	Domain registration has expired
	nike.biz.id	Active and parked with irrelevant content
	nike.web.id	Site cannot be reached
	nike.creditcard	Active and redirects to nike.com
	nike.co.pl	Domain is blocked
	nike.cd	Site cannot be reached
	nike.photo	Active and redirects to nike.com
nike.cd	nike.vc	Site cannot be reached
	nike.bz	Active and redirects to nike.com
	nike.joburg	Site cannot be reached
	nike.monster	Inactive and parked under Namecheap
	nike.xn–ses554g	Site cannot be reached
	nike.help	Active and redirects to nike.com
	nike.eus	Site cannot be reached
	nike.kim	Site cannot be reached
	nike.ne.kr	Site cannot be reached
	nike.shopping	Active and redirects to nike.com
	nike.horse	Site cannot be reached
	nike.mk	Domain for sale on GoDaddy
nike.kaufen	nike.museum	Site cannot be reached
nike.museum	nike.com.py	Active and redirects to nike.com
	nike.hockey	Active and redirects to nike.com
	nike.gdn	Site cannot be reached
	nike.bs	Active and redirects to nike.com
	nike.link	Potential threat detected (typo-squatting domain)
	nike.cam	Active and redirects to nike.com
	nike.boo	Site cannot be reached
	nike.com.lc	Site cannot be reached
	nike.airforce	Site cannot be reached
	nike.edu.ge	Active with unknown web reputation
	nike.auction	Active and redirects to nike.com

Despite having a large volume of false-positives, it is worth mentioning that Maltego did provide a valuable lead to a typo-squatting domain nike.ink indirectly through its finding nike.link. On visiting nike.link, the result was "This site cannot be reached. Check if there is a typo in nike.link". So on investigating further by purposefully making a spelling error (entering "ink" instead of "link"), we found a fraudulent domain (nike.ink) which hosted a phishy website. The site had typographical errors (the word "team" was misspelled as "tearm") with poor quality web-design which is highly unlikely for a reputed brand like Nike. The site also used Nike's logo and mentioned a suspicious

email china@nike.ink along with a contact number of sales team, which is a confidential detail and is highly unlikely to be revealed by Nike (refer Figure 5.2 for a live snapshot of `http://www.nike.ink/`). Therefore, as per our analysis, nike.ink is a phished domain imposing a threat on Nike's online brand integrity.

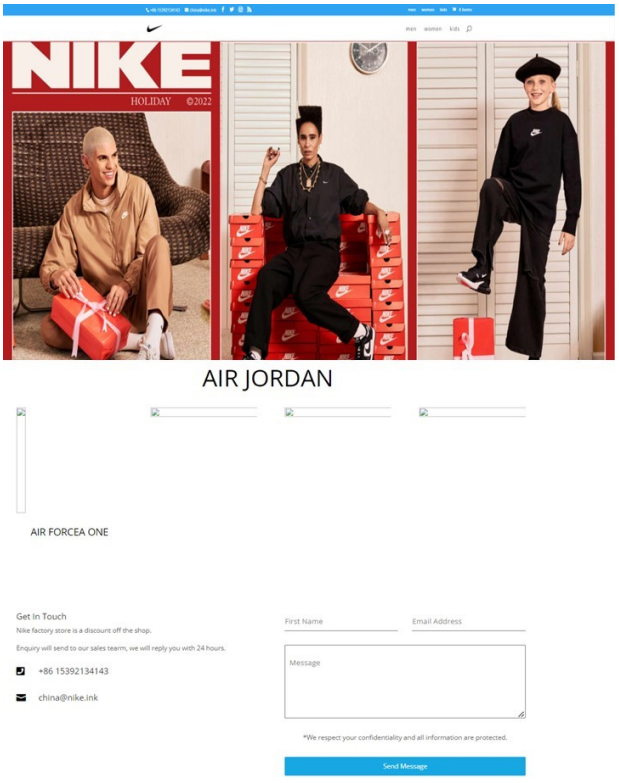


FIGURE 5.2: Live snapshot of nike.ink dated as of 13/07/2023

Comparative Analysis of Scamsweep vs. Commercial Solution: To validate the manual analysis conducted using Scamsweep's toolkit, we examined the domain "nike.ink" on Iris Investigate, an enterprise-grade domain and IP intelligence tool. According to Iris Investigate's findings, "nike.ink" was identified as a malicious domain with a phishing threat profile. The tool also assigned risk scores for various threat categories related to this deceptive domain, such as 20 for phishing, 8 for malware, 6 for spam and 14 for proximity (indicating close association with other malicious domains). Figure 5.3 illustrates the results obtained from Iris Investigate.

On comparing the outcomes of our manual analysis with those obtained from the commercial solution, we observed a strong alignment in the results. This alignment confirms that the indirect lead provided by Maltego due to a typographical error was a true positive event. As a result, Maltego has proven to be a valuable addition to Scamsweep's final toolkit, further enhancing its reconnaissance capabilities for online brand protection.

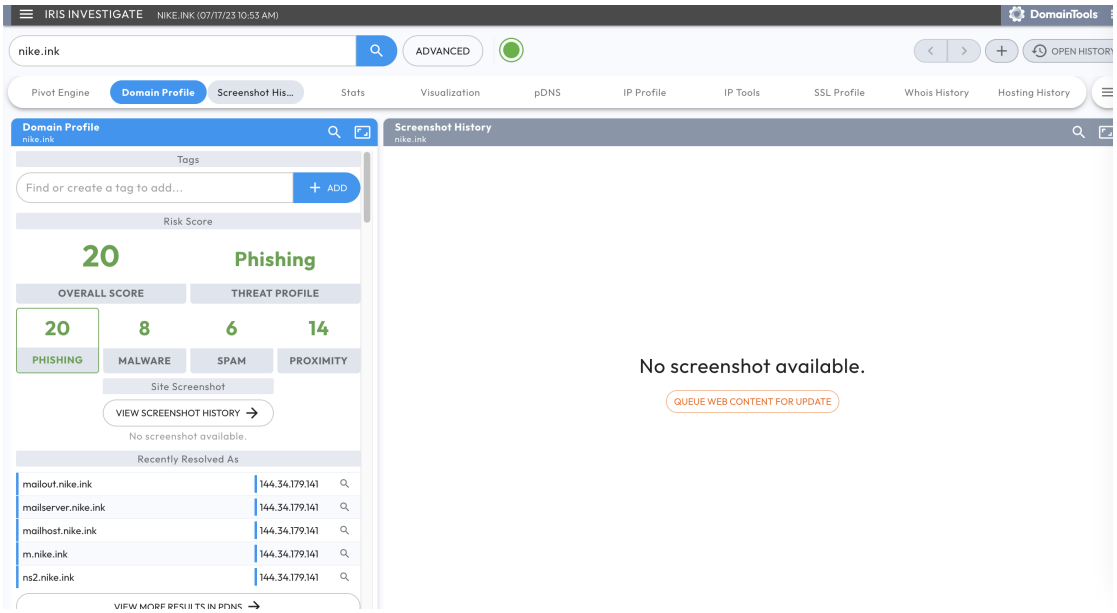


FIGURE 5.3: Screenshot of Iris Investigate's analysis on nike.ink dated as of 17/07/2023

5.2.2 Test Case 2.1: Testing OTX Alienvault

Test Case 2.1 evaluates the performance of OTX Alienvault, an intelligence platform, within the context of Use Case 2 - Web-Reconnaissance. The purpose is to assess the effectiveness of OTX Alienvault in gathering actionable threat intelligence for Nike's online brand protection.

Observations: Figure 5.4 showcases the domain "nikenflcheapjerseys.us", which raised suspicion due to its use of marketing terms like "cheap jerseys" alongside a reputable brand name like Nike in its domain. According to Alienvault's analysis, this domain is classified as a Domain Generation Algorithm (DGA) domain, indicating its association with a program that generates numerous domains automatically, often utilized by malware families to evade security measures [62]. Moreover, Alienvault detected that "nikenflcheapjerseys.us" has surpassed SPF (Sender Policy Framework) Record checks, suggesting its potential to circumvent blocking measures when used for sending spoofed emails or spam [63]. Notably, the SSL (Secure Socket Layer) Certificate used by the domain is "Let's Encrypt", a free certificate issued by the non-profit Internet Security Research Group (ISRG). Although legitimate entities may use this certificate, cybercriminals have exploited it in the past for malvertising campaigns, leading to numerous scam complaints on the Let's Encrypt Community Support portal [64]. Consequently, the usage of this free certificate by a genuine Nike domain is highly unlikely and raises suspicions as a potential threat indicator. Based on these findings, it is reasonable to

Test ID:	2.1
Tool:	OTX Alienvault
Platform:	Web-based
Purpose:	To gather actionable intelligence on Nike using Alienvault
Steps:	1. Go to the Alienvault website (`https://otx.alienvault.com/`). 2. Sign up for a free account to access the platform. 3. Login to the OTX account. 4. In the search bar at the top of the page, type "nike.com" or "Nike" (without quotes) and press "Enter" or click on the magnifying glass icon to initiate the search. 5. The search results will display any relevant threat intelligence related to "nike.com" or the keyword "Nike". 6. Review the search results to identify any potential threats, indicators of compromise or relevant information associated with the search query.
Expected Result:	Alienvault should give a result of at least 1 active domain related to Nike that looks potentially suspicious.
Actual Result:	Alienvault's search results gave 501 DNS records on searching for nike.com and result of 10,113 threat indicators on searching for the brand name "nike" only. From this list 4 domains appear to be suspicious, i.e., nikeshang.shop, nikeshoesplaza.us, nikenflcheapjerseys.us (refer Figure 5.4)
Status:	Pass

classify "nikenflcheapjerseys.us" as a malicious domain. For a complete analysis, refer to OTX Alienvault's report on `https://otx.alienvault.com/indicator/domain/nikenflcheapjerseys.us`.

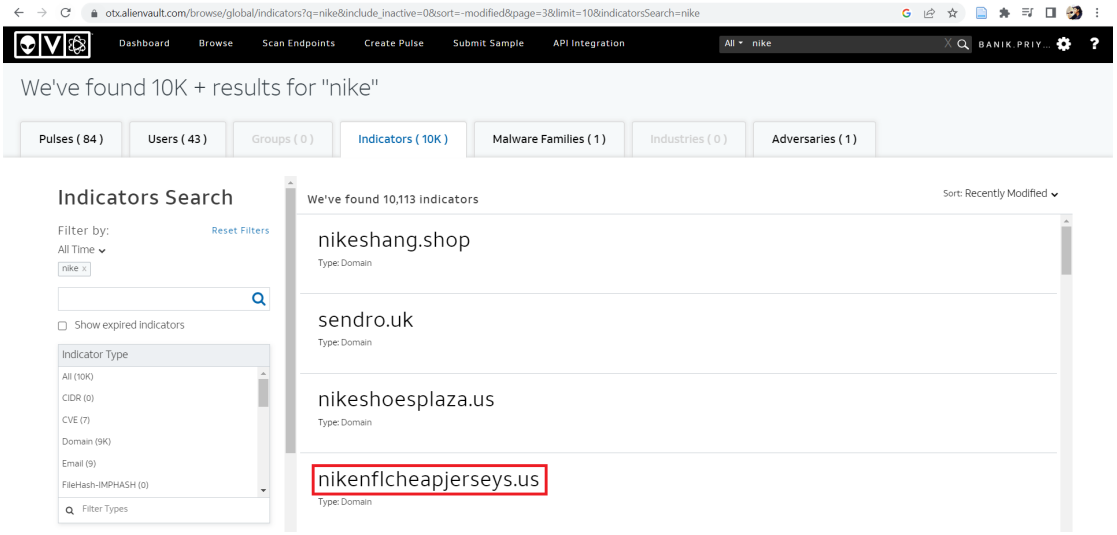


FIGURE 5.4: OTX AlienVault's output on searching for "nike" brand name

Comparative Analysis of Scamsweep vs. Commercial Solution: To validate our manual analysis, we conducted a domain search for "nikenflcheapjerseys.us" on Iris Investigate. The results obtained from Iris Investigate, as depicted in Figure 5.5,

aligned with our manual analysis, confirming that "nikenflcheapjerseys.us" is indeed a fraudulent domain. This commercial tool flags "nikenflcheapjerseys.us" as a phishing domain with a threat score of 15 under the category of phishing, 17 under the category of malware, 4 under the category of spam and 26 under the category of proximity threat. This consistency proves the effectiveness of OTX Alienvault in detecting a true positive event, making it a valuable addition to Scamsweep's final toolkit. By enhancing its reconnaissance capabilities for online brand protection, OTX Alienvault contributes significantly to the overall effectiveness of Scamsweep's efforts.

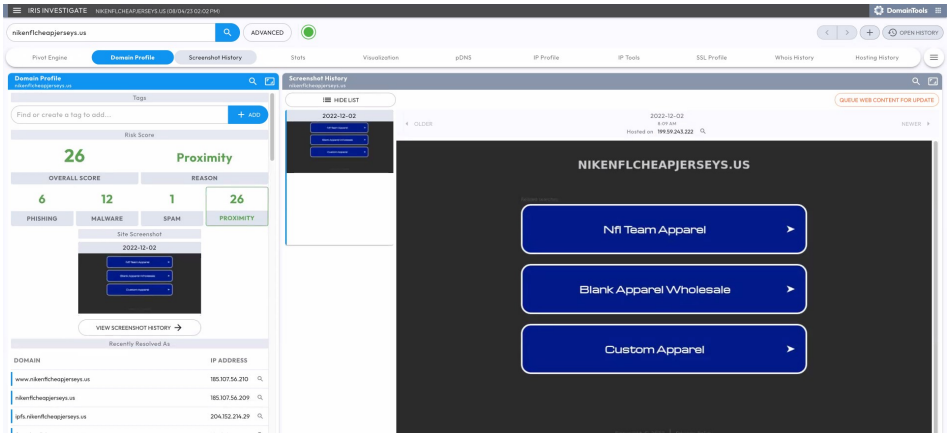


FIGURE 5.5: Screenshot of Iris Investigate's analysis on "nikenflcheapjerseys.us" on Iris Investigate dated as of 05/08/2023

5.2.3 Test Case 2.2: Testing Microsoft Defender Threat Intelligence

Test Case 2.2 evaluates the performance of Microsoft Defender Threat Intelligence, an advanced threat protection tool, within the context of Use Case 2 - Web-Reconnaissance. The purpose is to assess the tool's capability in gathering actionable intelligence for Nike's online brand protection by searching for potential threats or suspicious activities related to the domain "nike.com" and the brand name "Nike".

Observations: During the analysis of Microsoft Defender Threat Intelligence results, we encountered the domain "nikeclearance.us" (refer Figure 5.6). Upon inspecting the Whois record for this domain, we observed that it is registered under Namecheap Inc, a company known for providing starightforward domain registration services that opens doors for online businesses easily [65]. However, the email address of the domain registrant, "humphries0514@hotmail.com", raises doubts as it is highly improbable for a reputable company like Nike to utilize Namecheap for domain registration and the use of a Hotmail ID is atypical. Although these observations are not conclusive evidence of the domain's malicious intent, they have prompted us to conduct further investigation in the subsequent test cases to ascertain its true nature. For a complete analysis, refer to

Test ID:	2.2
Tool:	Microsoft Defender Threat Intelligence
Platform:	Web-based
Purpose:	To gather actionable intelligence on Nike using Microsoft Defender Threat Intelligence
Steps:	1. Go to the Microsoft Defender Threat Intelligence website (`https://ti.defender.microsoft.com/`). 2. Sign in to your Microsoft account with appropriate permissions to access threat intelligence data. 3. In the search bar or query box, type "nike.com" or "Nike" (without quotes) and press Enter or click on the search button to initiate the search. 4. Microsoft Defender Threat Intelligence will now search its threat database for any relevant information related to "nike.com" or the keyword "Nike." 5. Review the search results (domains, IPs, hash values) to identify any potential threats or suspicious activities related to "nike.com" or "Nike".
Expected Result:	Microsoft Defender Threat Intelligence should give a result of at least 1 active domain related to Nike that is potentially suspicious.
Actual Result:	Microsoft Defender Threat Intelligence gave 1,686 search results on entering the TLD "nike.com" and 29,368 search results (refer Figure 5.5) on entering just the brand name "nike"
Status:	Pass

Microsoft Defender Threat Intelligence's report on `https://ti.defender.microsoft.com/search/data/whois/records?query=nikesclearance.us`.

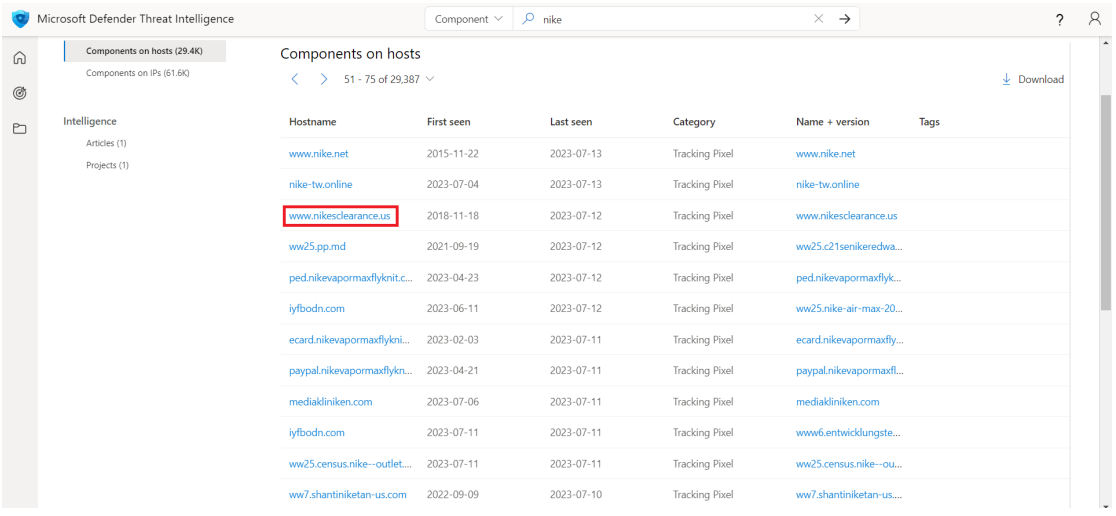


FIGURE 5.6: Microsoft Defender Threat Intelligence's output on searching for "nike" brand name

Comparative Analysis of Scamsweep vs. Commercial Solution: To conduct further investigation on the domain "nikeclearance.us", we attempted to access the URL within our test environment using a Windows Virtual Machine. Upon trying to open

the URL, we received a warning from McAfee Anti-virus [66], a commercial product installed on our test machine for security purposes. McAfee Anti-virus flagged "nike-clearance.us" as a suspicious website (refer Figure 5.7), providing a degree of validation to our initial suspicions. However, it is important to note that we have not yet utilized all the capabilities of Scamsweep to reach a conclusive determination on the malicious nature of this domain. In the upcoming test cases, we will continue the investigation to arrive at a firm conclusion regarding its status. For this specific test case, Microsoft Defender Threat Intelligence successfully provided a potentially suspicious domain that warranted further in-depth investigation, leading to a "Pass" status as a result.

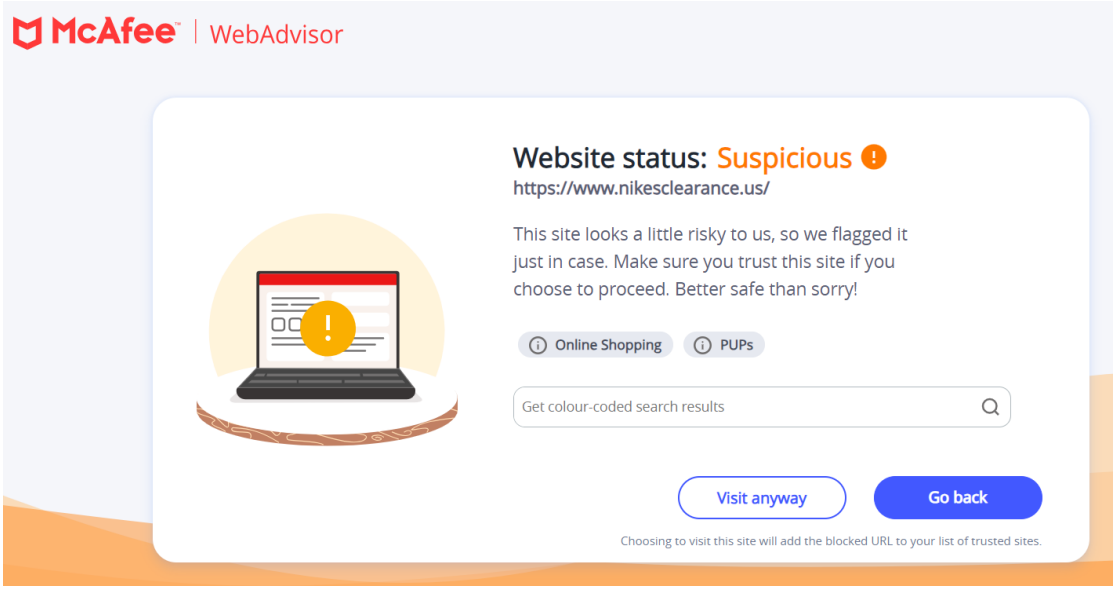


FIGURE 5.7: McAfee Anti-virus result on entering "nikeclearance.us"

5.2.4 Test Case 2.3: Testing Recon-ng

Test Case 2.3 evaluates the usage of Hackertarget module in Recon-ng, a reconnaissance framework for retrieving active hostnames associated with Nike.

Observations: An interesting observation here is the striking similarity in the output metrics of Recon-ng and OTX AlienVault, i.e., both the tools produced exactly 501 DNS records on searching for "nike.com" domain. This indicated some resemblance in the back-end engineering of how both these tools pull and process search requests. However, upon closer examination of results of both the tools, it became evident that while the number of detected domains was the same, the individual results were distinct. Since Recon-ng was useful in gathering a wealth of intelligence on a command line interface, we shall consider this tool to be a valuable addition to Scamsweep's final toolkit for web reconnaissance. See **Appendix C.1** for a complete list of commands used and the intelligence gathered on Nike using Recon-ng.

Test ID:	2.3
Tool:	Recon-ng
Platform:	Linux
Purpose:	To gather actionable intelligence on Nike using Recon-ng
Steps:	1. Launch Recon-ng in the Linux terminal. 2. Refresh the marketplace index by executing the command "marketplace refresh". 3. Install the "recon/domains-hosts/hackertarget" module by executing the command "marketplace install recon/domains-hosts/hackertarget". 4. Load the module "recon/domains-hosts/hackertarget" by executing the command "modules load recon/domains-hosts/hackertarget". 5. Set the source as "nike.com" using the command "options set SOURCE nike.com". 6. Execute the module by running the command "run". 7. Verify the results to ensure that relevant host names related to "nike.com" have been discovered and recorded in the "hosts" table.
Expected Result:	Recon-ng should execute the "recon/domains-hosts/hackertarget" module and gather host names associated with "nike.com".
Actual Result:	Recon-ng successfully retrieved 501 host names related to "nike.com" using the "recon/domains-hosts/hackertarget" module and recorded them in the "hosts" table.
Status:	Pass

5.3 Use Case 3: Domain Infringements

Use Case 3 focuses on Domain Infringements and involves testing the tools URLScan.io and Cisco Talos Intelligence to analyze and assess potential domain threats and reputations related to the brand Nike. These tests aim to identify any unauthorized use of Nike's trademarked assets and evaluate the reputation of IP addresses or domains associated with the brand.

5.3.1 Test Case 3.0: Testing URLScan.io for Analysis of Nike's URL

Test Case 3.0 involves the utilization of the web-based tool URLScan.io to conduct a comprehensive security evaluation of "nikeclearance.us". Within this analysis, potential threats or vulnerabilities inherent to the URL are sought to be uncovered, thereby shedding light on crucial aspects of its digital infrastructure. Through subjecting "nikeclearance.us" to URLScan.io's scrutiny, valuable insights are contributed towards fostering a well-rounded comprehension of its online security posture.

Observations: On analysing the live snapshot captured by URLScan.io, it was observed that this website uses the trademarked logos and trademarked words registered by Nike, for example, Air Jordan, Nike Dunk, Travis Scott and more. The primary IP address on

Test ID:	3.0
Tool:	URLScan.io
Platform:	Web-based
Purpose:	To analyze the URL "nikeclearance.us" using URLScan.io for potential threats and security vulnerabilities.
Steps:	1. Open a web browser and go to the URLScan.io website (`https://urlscan.io`). 2. In the search bar on the website's homepage, enter the URL "nikeclearance.us" and press Enter to initiate the analysis. 3. URLScan.io will process the URL and display a summary report of its findings, which may include information about HTTP requests, response data, domains accessed, JavaScript execution, live snapshot of the URL being investigated and potential threats or security issues. 4. Pay attention to elements such as blacklisted domains, JavaScript behavior, SSL certificate details and any other noteworthy findings. 5. Analyze the provided data to determine if "nikeclearance.us" poses any risks or is associated with malicious activities.
Expected Result:	URLScan.io should generate a report with detailed analysis of the URL "nikeclearance.us", highlighting at least 1 attack vector associated with the website.
Actual Result:	URLScan.io generates a report containing multiple attack vectors such as: 4 IP addresses, 4 domains, geo-location details, 1 live snapshot of web-page, 40 HTTP transactions, 4 Javascript cookies, 40 hash values, 10 proximity hits, DOM (Document Object Model) of the web-design characteristics and API request related to "nikeclearance.us" (refer Figure 5.8).
Status:	Pass

resolving this domain was observed to be 45.12.2.63, whose geo-location is Ukraine and web-reputation is unknown (`https://talosintelligence.com/reputation_center/lookup?search=45.12.2.63`). The website appears to be selling Nike products and using its copyrights without legal authorisation. URLScan.io also analysed the behaviour of the 4 Javascript cookies captured while visiting "nikeclearance.us" and detected that one 1 out of these 4 cookies is not secure. In view of these compelling indications, it is evident that this domain poses a significant potential threat. The combination of unauthorized usage of trademarked materials, questionable IP geolocation and insecure Javascript cookies underscores the need for immediate attention to mitigate the potential risks associated with "nikeclearance.us". Therefore, based on these evidences, we agree with the result given by McAfee Anti-virus earlier in Test Case 2.2 and conclude that this domain is an indicator of compromise.

To view the the full URL analysis report on "nikeclearance.us" generated by URLScan.io, go to `https://urlscan.io/result/1f4463bf-11af-4be6-ac2f-afcfce252e41/#summary`.

Comparative Analysis of Scamsweep vs. Commercial Solution: On entering "nikeclearance.us" on Iris Investigate, we see that the tool categorises it as a phishing

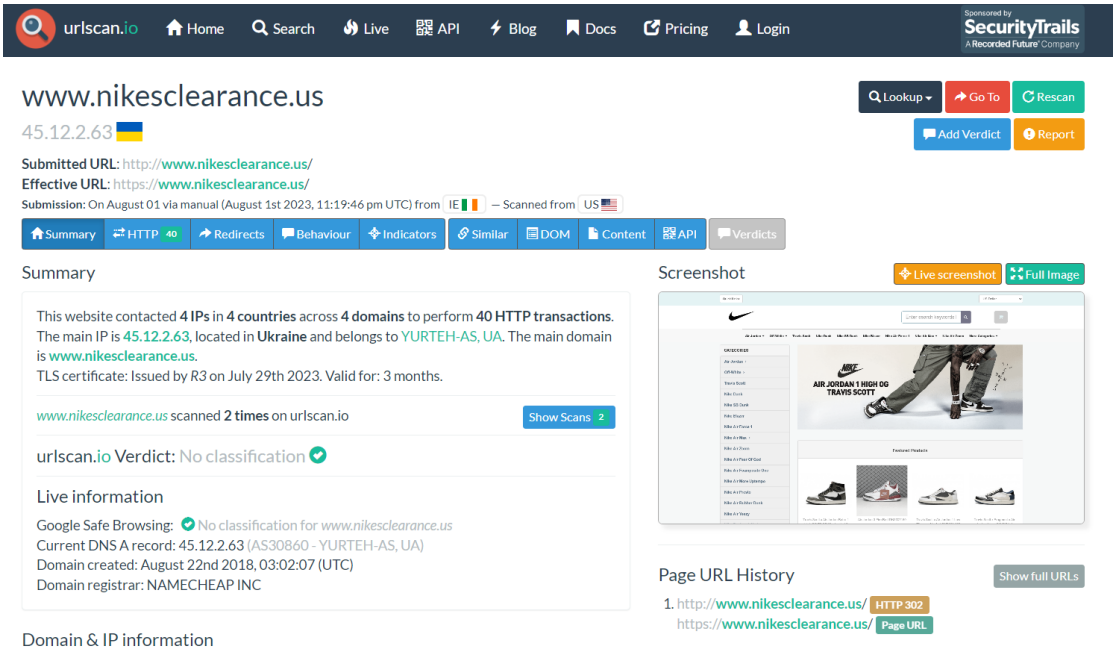


FIGURE 5.8: URL analysis of "nikeclearance.us" on urlscan.io

domain with a threat score of 15 in its analysis report (refer 5.9). This validates our analysis and proves that nikeclearance.us is indeed a malicious domain and urlscan.io is a good tool to be included in Scamsweep's final toolkit.

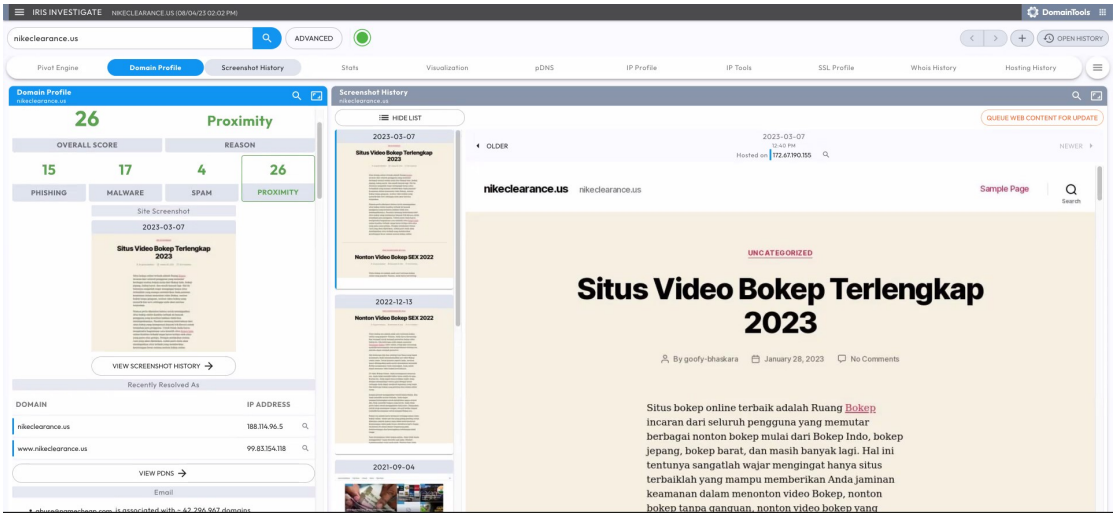


FIGURE 5.9: URL analysis of "nikeclearance.us" on Iris Investigate

5.3.2 Test Case 3.1: Testing Cisco Talos Intelligence for Checking Reputation of Nike's IP or Domain

In Test Case 3.1, we will utilize Cisco Talos Intelligence to assess the reputation of Nike's IP address or domain, aiming to identify any potential threats or malicious activities

associated with it. The expected outcome is to obtain a IP reputation report from Cisco Talos Intelligence, indicating the status of the IP or domain and any potential security concerns.

For this test case, we shall use the IP address fetched on the resolving the domain "nikeshang.shop", i.e., 47.92.32.206. This domain was detected earlier by OTX Alienvault as seen in Figure 5.4.

Test ID:	3.1
Tool:	Cisco Talos Intelligence
Platform:	Web-based
Purpose:	To check the reputation of the IP address 47.92.32.206 using Cisco Talos Intelligence for potential threats and malicious activities.
Steps:	1. Open a web browser and go to the Cisco Talos Intelligence website (`https://talosintelligence.com`). 2. In the search bar on the website's homepage, enter the IP address "47.92.32.206" and press Enter to initiate the search. 3. Cisco Talos Intelligence will perform a reputation check on the provided IP address and display the results. 4. Review the information provided by Cisco Talos Intelligence to identify any indicators of malicious behavior associated with the IP address. 5. Pay attention to elements such as geo-location data, network owner name, IP reputation, web reputation, email reputation, presence in any spam blocklists and other noteworthy findings. 6. Analyze the provided data to determine whether "47.92.32.206" is associated with any security risks or malicious activities.
Expected Result:	Cisco Talos Intelligence should provide a reputation report for the IP address "47.92.32.206", indicating a "Neutral" or "Poor" or "Unknown" sender IP reputation with potential security concerns associated with it.
Actual Result:	Cisco Talos Intelligence generates a reputation report for the IP address "47.92.32.206", indicating a "Poor" Sender IP reputation with potential security risks (such as: this IP address is blacklist as a spammer) and malicious activities associated with it (refer Figure 5.10).
Status:	Pass

Observations: In the report fetched from Cisco Talos Intelligence, it was observed that location for the IP address 47.92.32.206 is in Beijing, China and the network owner is "hangzhou alibaba advertising co., ltd." In terms of reputation, the sender IP reputation is marked as "Poor" and the web reputation is labeled as "Unknown." The email volume data shows no email activity in recent times. However, the spam level is categorized as "Critical". Regarding blocklists, the IP is listed in the PBL.SPAMHAUS.ORG block list, but it is not found in other major blocklists such as BL.SPAMCOP.NET, CBL.ABUSEAT.ORG or SBL.SPAMHAUS.ORG. Additionally, the resolved domain for 47.92.32.206, i.e., nikeshang.shop has been categorised as a phished domain by OTX

Alienvault related pulses. We also checked it on SucuriSitecheck (`https://sitecheck.sucuri.net/results/nikeshang.shop`), which rated it as a Medium Security Risk (refer Figure 5.11). So, based on these evidences it can be concluded that this IP is malicious and as a security recommendation, it is advisable that any inbound or outbound traffic from 47.92.32.206 should be blocked at the firewall, proxy or border-router placed at Nike's security perimeters.

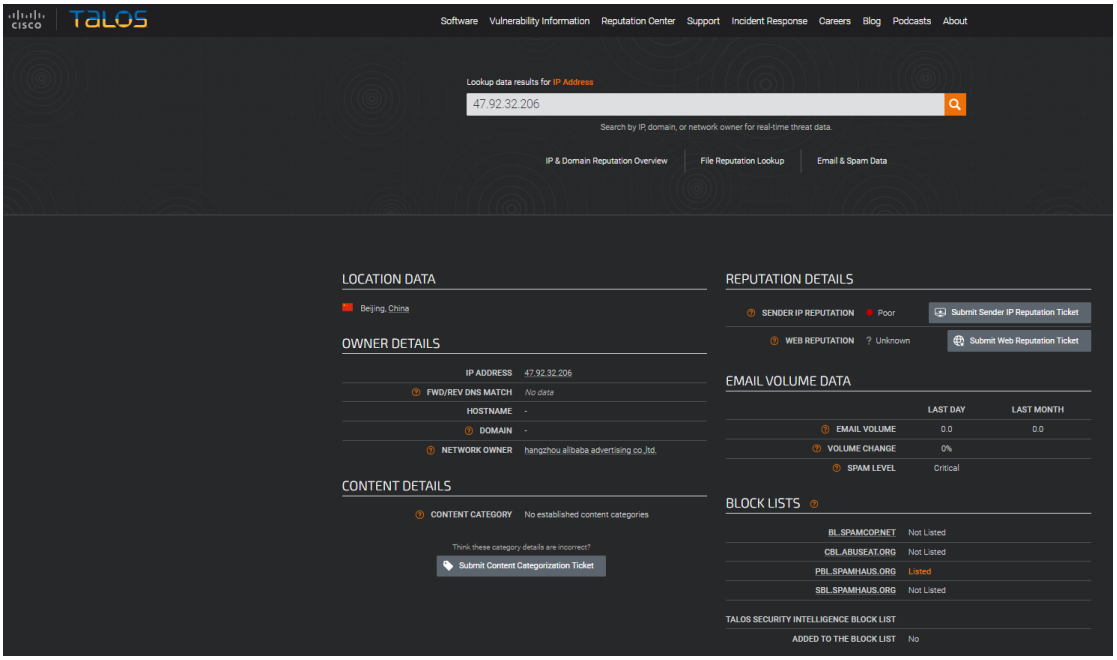


FIGURE 5.10: IP reputation analysis of "47.92.32.206" on Cisco Talos Intelligence

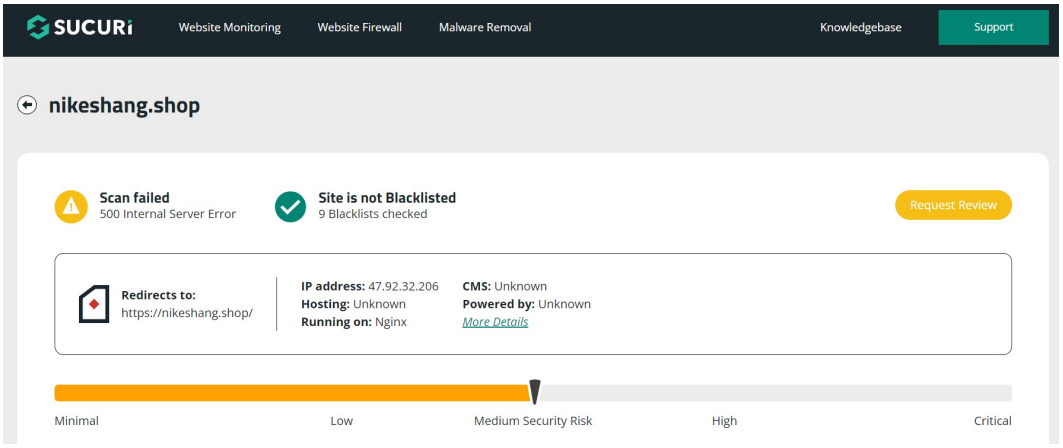


FIGURE 5.11: Domain analysis of "nikeshang.shop" on sitecheck.sucuri.net

Comparative Analysis of Scamsweep vs. Commercial Solution: On entering "nikeshang.shop" or its resolved IP address "47.92.32.206" on Iris Investigate, the results highlight that the domain is malicious (refer Figure 5.12).

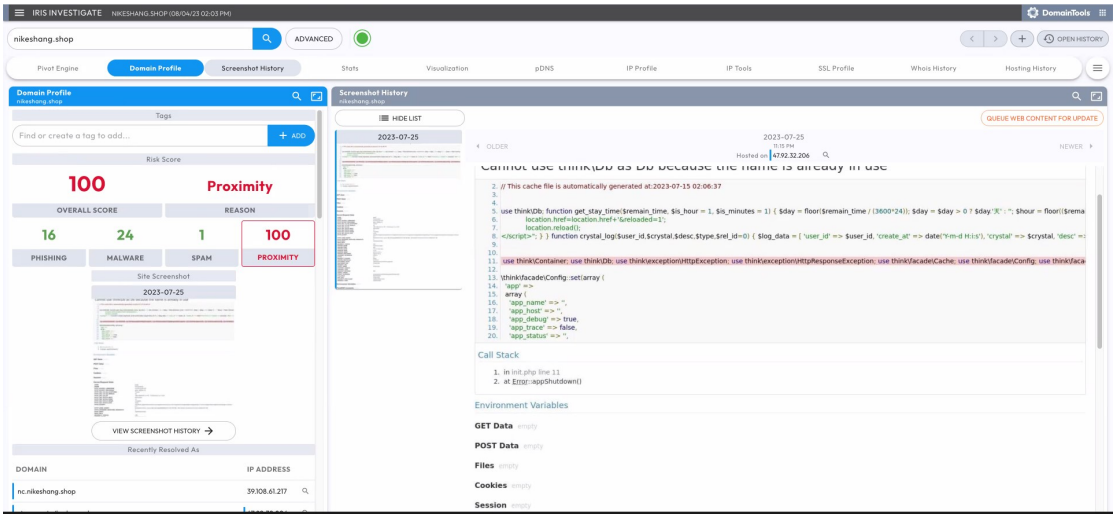


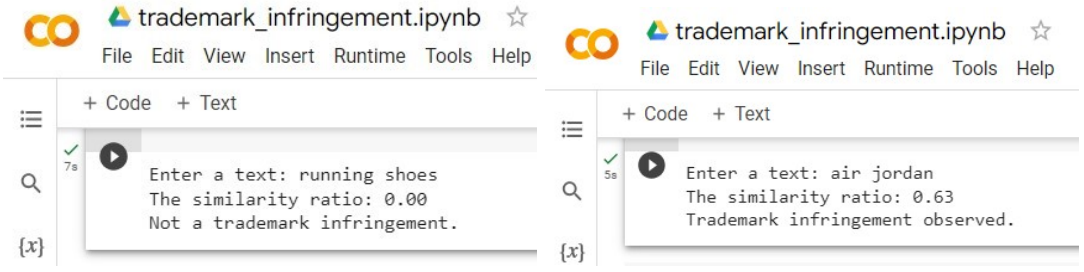
FIGURE 5.12: Screenshot of Iris Investigate's analysis on "nikeshang.shop" or "47.92.32.206" on Iris Investigate dated as of 05/08/2023

5.4 Use Case 4: Trademark Infringements

Use Case 4 delves into Trademark Infringements, centering on the evaluation of a Python script designed for conducting text analysis on Nike's trademarked terms. This use case aims to identify any instances of unauthorized usage or potential infringements of Nike's registered trademarks in textual content.

5.4.1 Test Case 4.0: Testing trademark_infringement.py Python Script on Google Colab

This test case verifies the functionality of the trademark_infringement.py script for analyzing Nike's trademarked words using text analysis. It involves running the script on Google Colab and providing two different user inputs ("running shoes" and "air jordan") to assess whether trademark infringement is correctly detected or not.



(a) Output for user input "running shoes" (b) Output for user input "air jordan"

FIGURE 5.13: Test output based on simulated user inputs to test the code functionality

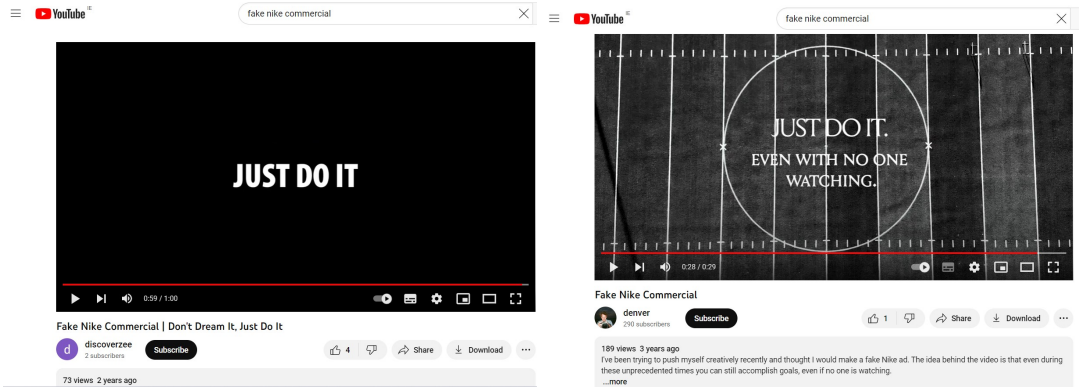
Test ID:	4.0
Tool:	Python 3.x
Platform:	Google Colab
Purpose:	To conduct text Analysis of Nike's Trademarked Words.
Steps:	1. Open Google Colab environment. 2. Create a new Python 3 notebook. 3. Copy and paste the provided Python script, i.e., trademark_infringement.py (`https://colab.research.google.com/drive/11iTtAquNWz6jM-UG_8sXfHE-oREpmhii`) into a code cell. 4. Run the code cell (Click the "play" button or press "Ctrl+Enter". 5. When prompted, enter the following user inputs: "running shoes" and "air jordan" (without quotes).
Expected Result:	The script should print "Not a trademark infringement" for first user input, i.e., "running shoes" and it should print "Trademark infringement observed" for second user input, i.e., "air jordan".
Actual Result:	The script prints "Not a trademark infringement" for first user input "running shoes" (with similarity ratio: 0.00) and it prints "Trademark infringement observed" (with similarity ratio: 0.63) for second user input, i.e., "air jordan". (refer Figure 5.13).
Status:	Pass

Based on outputs derived from Test ID 4.0, we can affirm the accurate functionality of our script. However, the data employed for Test ID 4.0 was simulated and possessed a certain bias. Therefore, let us now proceed to identify instances where Nike's trademarked words and copyrights have been potentially abused in real-time.

Observations: On going to YouTube and searching for "Fake Nike Commercials", two videos were found, where Nike's copyrights have been potentially infringed. These videos can be found at:
Video 1: `https://www.youtube.com/watch?v=KVH-yVHr3os`
Video 2: `https://www.youtube.com/watch?v=5LOuTkUJglM`

In Video 1, it was observed that the caption of the video was "Fake Nike Commercial — Don't Dream It, Just Do It". We observed the usage of Nike's tick mark logo and "Just Do It" slogan (refer Figure 5.14(a)). Therefore, the user input while testing indications of trademark infringement for this video shall be "Don't Dream It, Just Do It".

In Video 2, we observed that the caption of the video was "Fake Nike Commercial". We observed the usage of Nike's tick mark logo and "Just Do It" slogan. It is to be noted that here the video-maker has included a special character, i.e., a fullstop (".") after "JUST DO IT" and has modified the slogan to "JUST DO IT. EVEN WITH NO ONE WATCHING." (refer Figure 5.14(b)). Therefore, the user input while testing indications of trademark infringement for this video shall be "JUST DO IT. EVEN WITH NO ONE WATCHING.".



(a) Screenshot of Video 1 on YouTube as of 03/08/2023

(b) Screenshot of Video 2 on YouTube as of 03/08/2023

FIGURE 5.14: Cases of potential trademark violations observed in real-time on YouTube videos

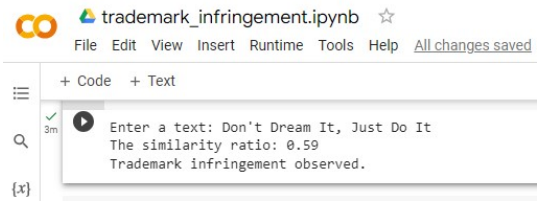
Based on our manual analysis, the anticipated outcomes for Video 1 and 2 involve the script printing "Trademark infringement observed" for the respective inputs. The existing similarity threshold, denoted as x, is currently set to 0.5. Initiating the evaluation, we entered the text "Don't Dream It, Just Do It," resulting in the output "Trademark infringement observed" (refer Figure 5.15(a)). This outcome validates the alignment between our manual and automated analyses.

Subsequently, we provided the next input, "JUST DO IT. EVEN WITH NO ONE WATCHING." and the output generated was "Not a trademark infringement" (refer Figure 5.15(b)). While this outcome does not align with our manual analysis, it is logically accurate. When the threshold is set at 0.5, the algorithm does not consider the additional words on input. Therefore, the second input is unlikely to yield a "Trademark infringement observed" output unless the threshold is adjusted. Furthermore, we examined the script with the input "JUST DO IT." (“.” included), resulting in the output "Trademark infringement observed", which was consistent with our manual analysis (refer Figure 5.15(c)).

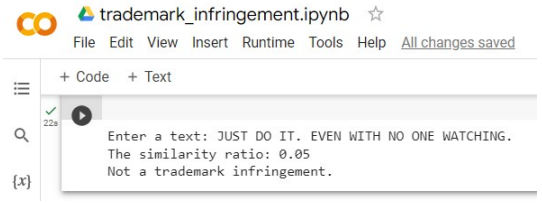
Comparative Analysis of Scamsweep vs. Commercial Solution: To validate the accuracy of the results fetched on running the script (devoid of any manual logic), we shall use the same user input texts on a trademark checker tool named "Marcaria".

As per Marcaria's analysis, the results were as follows:

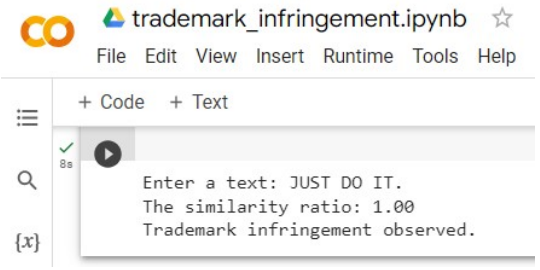
Input: Don't Dream It, Just Do It
Output: Found 0 Trademarks, i.e., not a trademark infringement (refer Figure 5.16(a))
Test Status: Fail (not aligned with script result)



(a) Script output for user input "Don't Dream It, Just Do It"



(b) Script output for user input "JUST DO IT. EVEN WITH NO ONE WATCHING."



(c) Script output for user input "JUST DO IT."

FIGURE 5.15: Test output for user inputs based on trademark infringements identified in real-time on YouTube

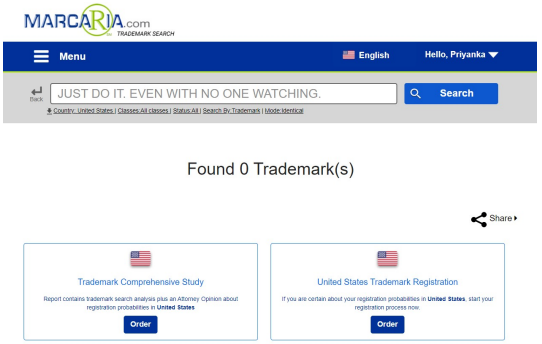
Input: JUST DO IT. EVEN WITH NO ONE WATCHING.
Output: Found 0 Trademarks, i.e., not a trademark infringement (refer Figure 5.16(b))
Test Status: Pass (aligned with script result)

Input: JUST DO IT.
Output: Found 2 Trademarks owned by Nike.Inc, i.e., trademark infringement observed (refer Figure 5.16(c))
Test Status: Pass (aligned with script result)

Hence, during live analysis, our script encountered a setback in the second scenario. This failure can be attributed primarily to the challenge of determining an optimal threshold value. The appropriateness of this threshold varies across diverse brands and requires a consultation with the customer for approval before implementing this script on any production environment.

A comprehensive exploration of the implications of this constraint and the prospective avenues for enhancing the script's efficiency shall be elaborated further in Chapter 6.

(a) Marcaria's output for user input "Don't Dream It, Just Do It"



(b) Marcaria's output for user input "JUST DO IT. EVEN WITH NO ONE WATCHING."

(c) Marcaria's output for user input "JUST DO IT."

FIGURE 5.16: Marcaria's output for user inputs based on trademark infringements identified in real-time on YouTube

5.5 Use Case 5: Image Processing

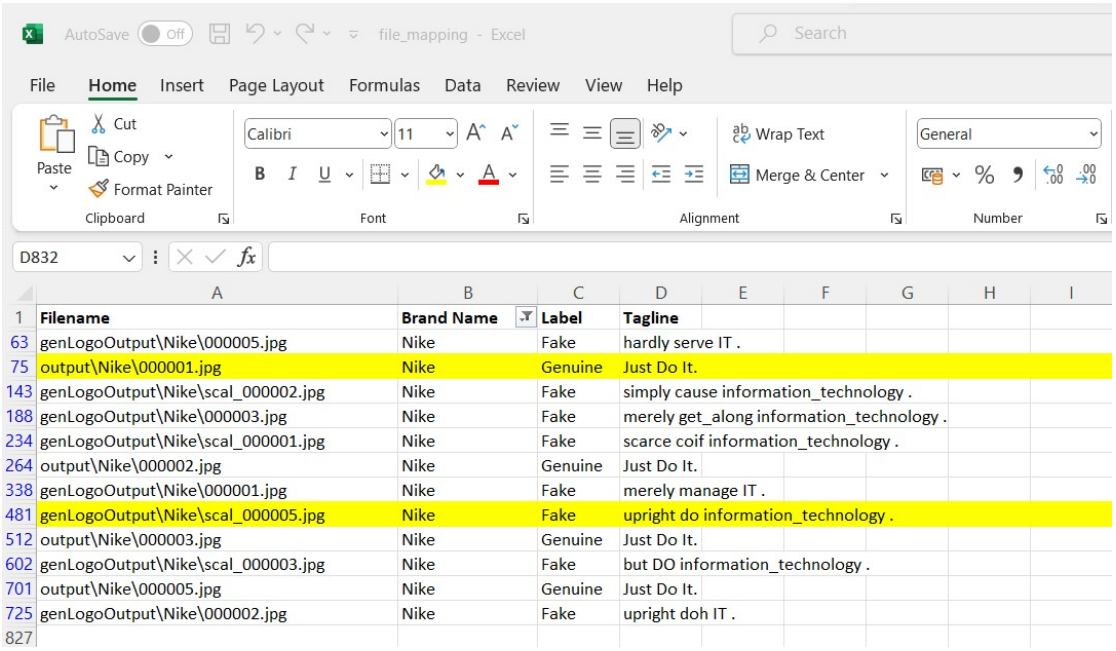
In Use Case 5, the focus lies on Image Processing, where we delve into the practical application of detecting image manipulation techniques used by brand abusers. A dataset of Nike logos were employed for testing and validation of the script developed to distinguish between real and fake brand logos.

5.5.1 Test Case 5.0: Testing counterfeit_logo_detection.py Python Script on Google Colab

Test Case 5.0 involves the evaluation of the counterfeit_logo_detection.py Python script within the Google Colab environment. This test utilizes a synthesized dataset of logos sourced from Kaggle, aiming to assess the script's ability to differentiate between real and counterfeit Nike logos.

Test ID:	5.0
Tool:	Python 3.x
Platform:	Google Colab
Purpose:	To differentiate between real and counterfeit Nike logos.
Steps:	1. Open Google Colab environment. 2. Create a new Python 3 notebook. 3. Copy and paste the provided Python script, i.e., counterfeit_logo_detection.py (`https://colab.research.google.com/drive/1AofT9B5gYmJFD4YUb4iEHiAlAcqSzU58#scrollTo=ZZc4vQU0wc6x`) into a code cell. 4. Create a repository of real Nike logos collected from Kaggle and Gerben Trademark Library in a folder named "RealNike" (Path: "/content/drive/My Drive/Scamsweep/Nike Logos/RealNike"). 5. Create a folder containing test logos (consisting of both real and fake Nike Logos) collected from Kaggle and Roboflow [67] in a folder named "TestNike" (Path: "/content/drive/My Drive/Scamsweep-/Nike Logos/TestNike"). 6. Open the file_mapping.xls spreadsheet which classifies the logo as fake or genuine. Apply filter to Column B (Brand Name) and select "Nike" to extract a list of images pertaining to Nike only (refer Figure 5.17). 7. Choose 2 images for testing, i.e., one real logo (000008.jpg) and one fake logo (scal_000005.jpg). 8. First test the code with a real Nike logo, i.e., "000008.jpg" taken from Kaggle (Path: "/content/drive/My Drive/Scamsweep/Nike Logos/TestNike/000008.jpg"). 9. Secondly, test with a fake Nike Logo i.e., "scal_000005.jpg" taken from Kaggle (Path: "/content/drive/My Drive/Scamsweep/Nike Logos/TestNike/scal_000005.jpg") 10. Run the code cell (Click the "play" button or press "Ctrl+Enter".
Expected Result:	The script should print "This test image appears to be a REAL brand logo." for first test logo, i.e., 000008.jpg. It should also highlight the image name with which it found a match. For the second test logo, the script should print "This test image appears to be a FAKE brand logo."
Actual Result:	The script prints "This test image appears to be a REAL brand logo." for first test logo (000008.jpg) and indicates that it found a match with "000003.jpg". For the second test logo (scal_000005.jpg), the script prints "This test image appears to be a FAKE brand logo."
Status:	Pass

Observations: The correct output was observed during testing using a simulated dataset downloaded from Kaggle, where the script successfully identified 000008.jpg as a genuine Nike logo (refer Figure 5.18) and scal_000005.jpg as a counterfeit version (refer Figure 5.19). However, an issue was observed as 000008.jpg, which is an exact duplicate of 000001.jpg from the RealNike folder, resulted in the script accurately generating the "This test image appears to be a REAL brand logo" output. To assess the script's performance and efficiency, additional genuine logos were obtained from Roboflow's dataset



	Filename	Brand Name	Label	Tagline
63	genLogoOutput\Nike\000005.jpg	Nike	Fake	hardly serve IT .
75	output\Nike\000001.jpg	Nike	Genuine	Just Do It.
143	genLogoOutput\Nike\scal_000002.jpg	Nike	Fake	simply cause information_technology .
188	genLogoOutput\Nike\000003.jpg	Nike	Fake	merely get_along information_technology .
234	genLogoOutput\Nike\scal_000001.jpg	Nike	Fake	scarce coif information_technology .
264	output\Nike\000002.jpg	Nike	Genuine	Just Do It.
338	genLogoOutput\Nike\000001.jpg	Nike	Fake	merely manage IT .
481	genLogoOutput\Nike\scal_000005.jpg	Nike	Fake	upright do information_technology .
512	output\Nike\000003.jpg	Nike	Genuine	Just Do It.
602	genLogoOutput\Nike\scal_000003.jpg	Nike	Fake	but DO information_technology .
701	output\Nike\000005.jpg	Nike	Genuine	Just Do It.
725	genLogoOutput\Nike\000002.jpg	Nike	Fake	upright doh IT .

FIGURE 5.17: Screenshot of file_mapping.xls with filtered list of Nike logo images only

[67]. In the subsequent evaluation, the script was tested with a real orange-colored Nike logo (nike–eps–vector-logo.jpg) sourced from Roboflow, residing at "/content/drive/My Drive/Scamsweep/Nike Logos/TestNike/nike–eps–vector-logo.jpg". It is to be noted that this orange-colored Nike logo from Roboflow is a real Nike logo but is not present in the RealNike folder. Despite its similarity to authentic logos from the Gerben Trademark Library, the script incorrectly classified this logo as fake (refer Figure 5.20). This highlights a limitation in the script's performance, which tends to classify images as fake unless they are precise duplicates of those in the RealNike folder, revealing its reliance on exact matches for accurate classification.

FIGURE 5.18: Script output for test image 000008.jpg

FIGURE 5.19: Script output for test image scal_000005.jpg

FIGURE 5.20: Script output for test image nike–eps–vector-logo.jpg

Comparative Analysis of Scamsweep vs. Commercial Solution: To evaluate the efficiency of the script, we shall upload the same test images on a commercial tool named "TinEye" [68]. This tool is a reverse image search engine, that identifies an uploaded image and gives search results pertaining to that image [68]. So, a real Nike logo should generate search results pertaining to Nike and fake logo should either generate no results or should give leads to suspicious websites hosting counterfeit Nike images.

As per TinEye's analysis, the results were as follows:

Test Image-1: 000008.jpg (real Nike logo)
Output: 93 results for this input, indicating that it is a real logo owned by Nike.Inc (refer Figure 5.21)
Test Status: Pass (aligned with script result)

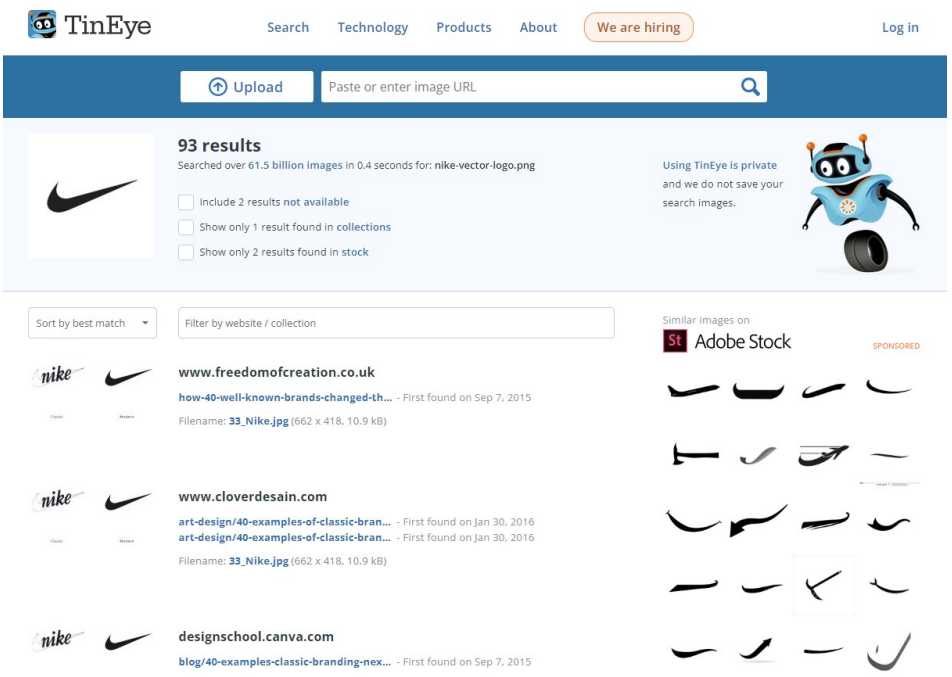


FIGURE 5.21: TinEye's output for test image 000008.jpg (real Nike logo)

Test Image-2: scal_000005.jpg (fake Nike logo)

Output: No results for this input, indicating that it is a fake logo not owned by Nike.Inc (refer Figure 5.22)

Test Status: Pass (aligned with script result)

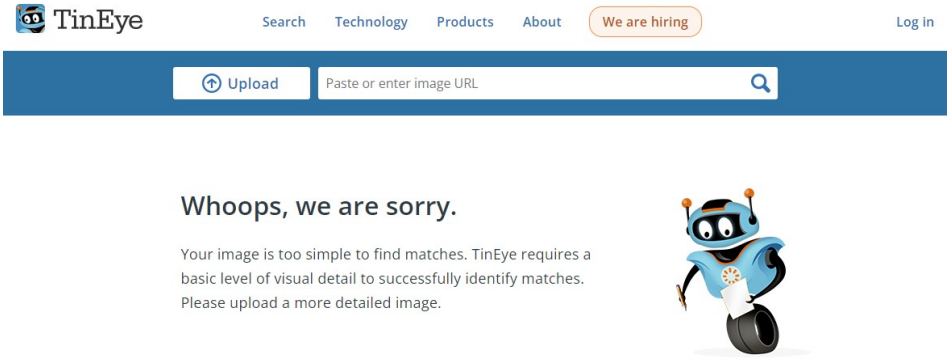


FIGURE 5.22: TinEye's output for test image scal_000005.jpg (fake Nike logo)

Test Image-3: nike–eps–vector-logo.jpg (real Nike logo)

Output: 23,525 results for this input, indicating that it is real logo owned by Nike.Inc (refer Figure 5.23)

Test Status: Fail (not aligned with script result)

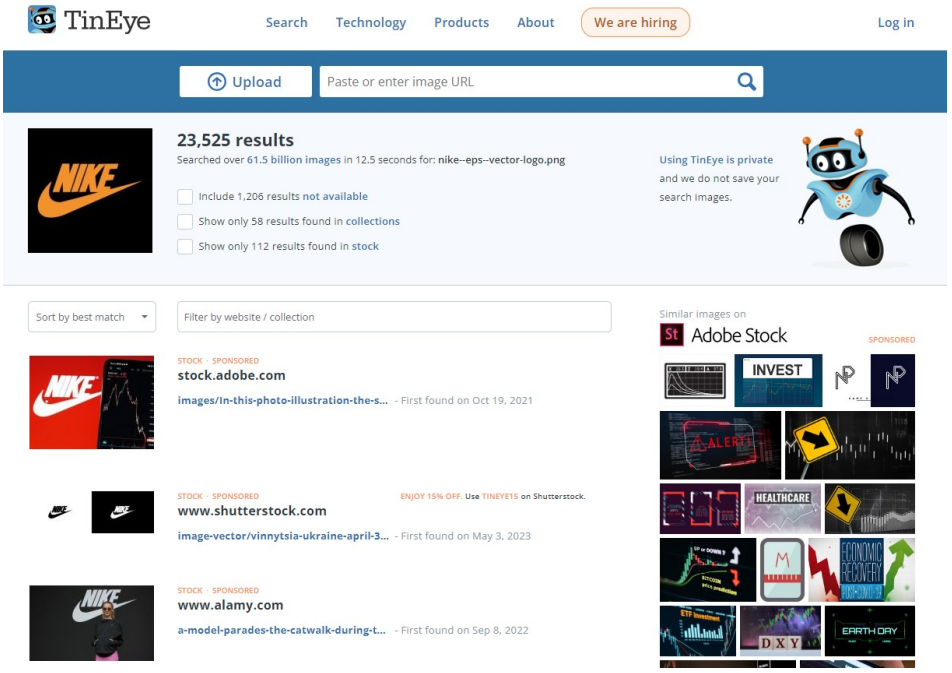


FIGURE 5.23: TinEye's output for test image nike–eps–vector-logo.jpg (real Nike logo)

Hence, upon contrasting the script's results with TinEye's analysis of the aforementioned three test images, it can be inferred that the script's accuracy is not absolute. Furthermore, the established threshold of 0.5 (50%) was maintained, pending consultation with the client. Therefore, constraints arise when utilizing the Chi-square distance as a measuring metric for image similarity. A comprehensive exploration of these constraints and strategies for enhancing the script's performance shall be elabarated upon in Chapter 6.

5.6 Use Case 6: Social Media Monitoring

Use Case 6 revolves around Social Media Monitoring, focusing on assessing and enhancing user engagement across various platforms. As a standard, the user engagement rates can be evaluated as shown in Table 5.2 [69].

TABLE 5.2: Thresholds of engagement rates and their corresponding scores

Engagement Rate	**Engagement Score**
less than 1%	Low
1% - 3.5%	Average
3.5% - 6%	High
greater than 6%	Exceptional

In this context, Test Case 6.0 involves evaluating the performance of Phlanx's User Engagement Calculator specifically designed for Instagram accounts, ensuring its effectiveness in measuring user engagement metrics by comparing it with the thresholds described in Table 5.2.

5.6.1 Test Case 6.0: Testing Phlanx's User Engagement Calculator for Instagram Accounts

In Test Case 6.0, we will be conducting comprehensive testing of Phlanx's User Engagement Calculator develop ed for Instagram accounts. This testing aims to evaluate the functionality, accuracy and reliability of the calculator in assessing user engagement on Instagram.

Test ID:	6.0
Tool:	Phlanx
Platform:	Web-based
Purpose:	To calculate the user engagement ratios of potential fake Instagram accounts impersonating Nike
Steps:	1. Go to Instagram (`https://instagram.com`) or download the mobile application from Playstore. 2. Sign up to create an account on Instagram. 3. Enter Nike's marketing keywords on the search box. 4. Make a list of account that have characteristics like: username contains the word "nike", uses Nike logos, seems to sell unauthorised or fake Nike products, accounts have less number followers, likes, comments and posts. Some examples of suspicious Instagram account usernames impersonating Nike are: nike__colombia__, coles__nike_slippers, fake_nikesneakerscommunity and unbox.nike 6. Open the browser and go to Phlanx (`https://phlanx.com`) 7. Select the user engagement calculator for the concerned social media platform. In this case, it is Instagram Engagement Calculator. 8. Type the profile name in the search box of Phlanx and hit enter (say, nike__colombia__).
Expected Result:	Phlanx should generate a percentage value for user engagement rate that lies between 3.5% to 6%, indicating a high engagement score for the account nike__colombia__.
Actual Result:	Phlanx calculates the user engagement rate and yields a value of 0.02% for nike__colombia__, which is less than 1%. Therefore, indicating a low engagement rate for nike__colombia__
Status:	Fail

Observations: On visiting nike__colombia__ (one of the Instagram search results), we observed that the account uses Nike's trademarked logo as its profile picture. There were posts containing pictures of Nike products on sale. The account uses WhatsApp (contact number provided) as a medium to sell these products, which is a revenue leakage for Nike.

The posts also includes a disclaimer message stating "NO COPYRIGHT INFRINGEMENT INTENDED", which makes it more suspicious (refer Figure 5.24). The number of likes per post is as low as 0 likes despite having a base of 3235 followers, indicating that these are not real followers and are likely to be bots. After thorough manual analysis of the content posted on this account, we concluded that nike__colombia__ should have a high engagement rate as it possesses all the characteristics of a fake account selling Nike's goods without any authorisation.

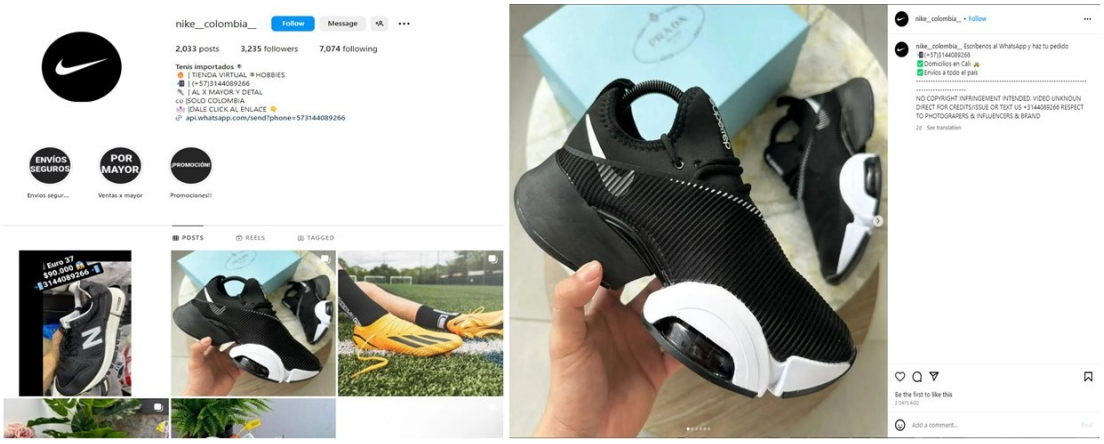


FIGURE 5.24: Content posted on nike__colombia__ as of 11/08/2023

To validate our analysis, we entered this account name on Phlanx's Instagram Engagement Calculator and it determined the engagement rate to be 0.02%, with an average interaction of 1 like and 0 comments per post (refer Figure 5.25) which is a low engagement rate as per the thresholds defined in Table 5.2, thereby contradicting our manual analysis. To cross-verify, we also compared this with the engagement rate of officially verified Nike account, i.e., nike, which has also has a low engagement rate of 0.03% but the average interactions per post is as high as 95,823 likes and 540 comments. It was interesting to observe that after normalising the number of likes, comments and followers, the engagement rates of both the accounts were very close marginally, thereby making it difficult to verify statistically that nike__colombia__ is a fake account and poses a high risk to Nike's brand value.

It is to be noted that Phlanx computes the engagement rate by dividing the combined count of likes and comments on a post by the total number of followers an account has. [40], [41]. Equation to calculate the user engagement rate (say R) using Phlanx's Instagram Engagement Calculator is given below [40], [41]:

$$Engagement\ Rate\ (R) = ((Likes + Comments)/Followers) * 100 \tag{5.1}$$

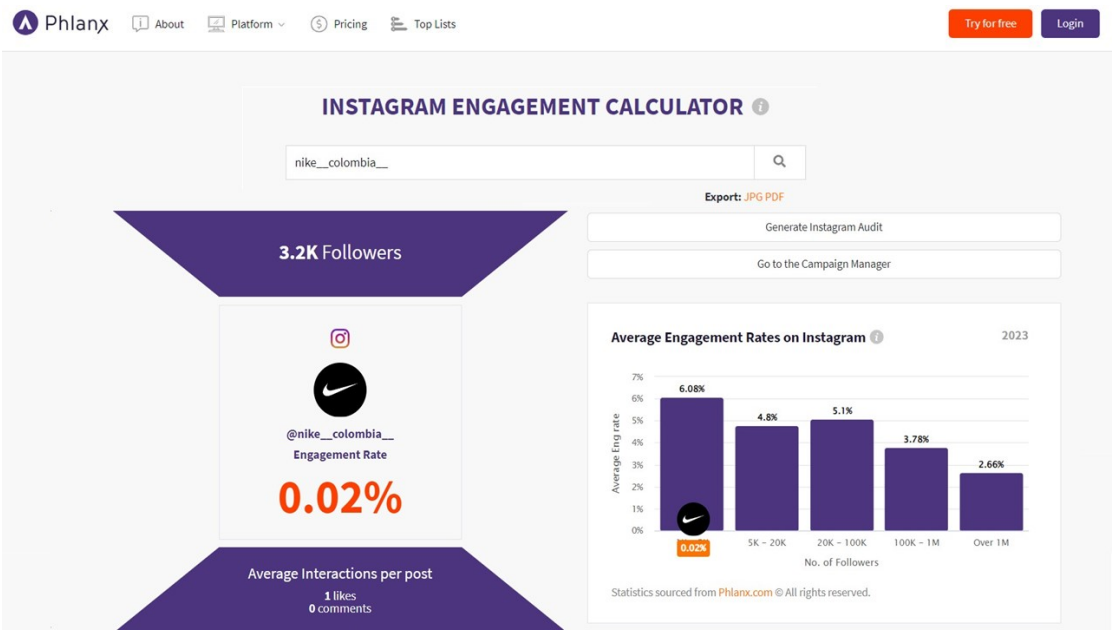


FIGURE 5.25: Output of Phlanx's Instagram Engagement Calculator for nike__colombia__ as of 11/08/2023

Additionally, we also looked into other suspicious accounts such as: coles__nike_slippers, fake_nikesneakerscommunity and unbox.nike. Table 5.3 is an assessment of the metrics generated by Phlanx (on August 11, 2023) for the suspicious accounts by comparing them with the thresholds defined earlier in Table 5.2.

TABLE 5.3: Comparison of metrics generated by Phlanx and the thresholds defined in Table 5.2

Username	**Phlanx's Output**	**Engagement Rate Range**	**Engagement Score**
nike__colombia__	0.02%	less than 1%	Low
coles__nike_slippers	11.95%	greater than 6%	Exceptional
fake_nikesneakerscommunity	10.42%	greater than 6%	Exceptional
unbox.nike	2.58%	1% - 3.5%	Average

After evaluating the metrics during the assessment and analysing the formula running behind Phlanx's engagement calculator, it was concluded that user engagement ratio is not the best metric for social media monitoring because it is volatile in nature (changes with increase or decrease in number of likes, comments and followers) and it normalises all the involved factors, i.e., number of likes, comments, followers to generate a certain percentage, whereas in practicality all these factors are individual contributors while monitoring social media activity for a brand. For example, account like fake_nikesneakerscommunity has only 2 posts with 8 likes, 5 comments on average and 96 followers but engagement rate is exceptionally high at 10.42% due to normalisation of involved numbers. Although in reality, the activity of that account is very low compared to a real Nike account.

5.7 Use Case 7: Rogue Applications

To test this use case, we searched for Android APK files for the Nike app hosted on Google or Apple Playstore. While browsing, we came across an app store named "MEmuPlay" which claimed to host the APK file for the legitimate Nike App (Nike logos were used as seen in Figure 5.26). This looked like a suspicious activity because developers of Nike would never release the APK file on a public forum. We downloaded the MemuPlay application, i.e., MEmu-setup-abroad-sdk.exe (`https://www.memuplay.com/download-com.nike.omega-on-pc.html`) on our sandboxed environment, i.e., Windows Virtual Machine to take a deeper look into the .exe file and investigate it with HashCalc and PEStudio.

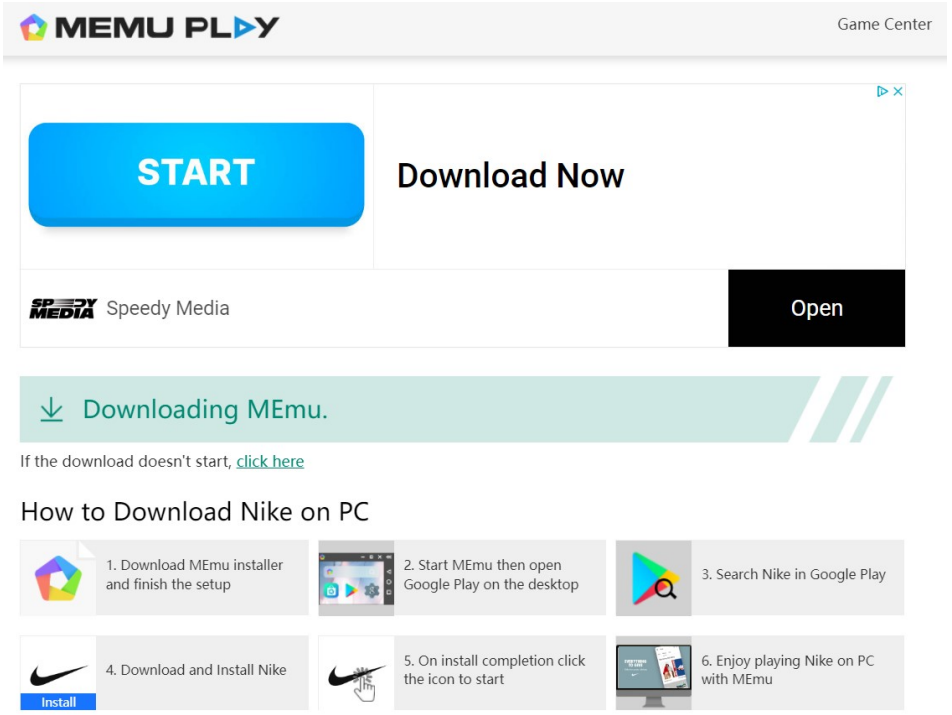


FIGURE 5.26: Screenshot of MEmuplay hosting the Nike App dated as 11/08/2023

5.7.1 Test Case 7.0: Testing HashCalc

In Test Case 7.0, we will be conducting testing for HashCalc, a software tool designed to calculate and verify hash values of files. This testing aims to validate the accuracy, reliability and functionality of HashCalc in generating hash values for data integrity and security purposes.

Test ID:	7.0
Tool:	HashCalc
Platform:	Windows
Purpose:	To calculate the hash value of MEmu-setup-abroad-sdk.exe
Steps:	1. Open HashCalc 2. Upload the file MEmu-setup-abroad-sdk.exe 3. Select SHA256 to generate the checksum using SHA256 algorithm (most secure) 4. Click "Calculate"
Expected Result:	HashCalc should generate a hash value in SHA256 format
Actual Result:	HashCalc generates a hash value in SHA256 format, i.e., *8fb453bf498acb05af9e0a442f26029cd6c5a3d68431fdff7fc385faf1541b96* (refer Figure 5.27)
Status:	Pass

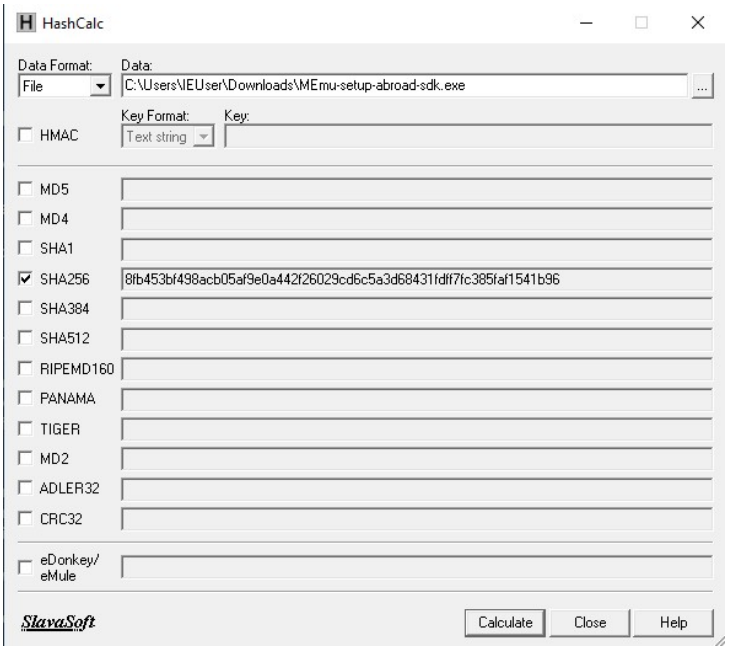


FIGURE 5.27: Hash value of MEmu-setup-abroad-sdk.exe calculated using SHA256 algorithm

5.7.2 Test Case 7.1: Testing PEStudio

Test Case 7.1 involves the comprehensive testing of PEStudio, a specialized software designed for analyzing and auditing Windows executable files. This testing aims to assess PEStudio's effectiveness in detecting potential security vulnerabilities, identifying suspicious components and providing insights into the structure of executable files, enhancing overall system security.

Test ID:	7.1
Tool:	PEStudio
Platform:	Windows
Purpose:	To analyse the characteristics and behaviour of MEmu-setup-abroad-sdk.exe
Steps:	1. Open PEStudio 2. Enter the hash value obtained from HashCalc on PEStudio, i.e., *8fb453bf498acb05af9e0a442f26029cd6c5a3d68431fdff7fc385faf1541b96* 3. PEStudio conducts a static analysis of MEmu-setup-abroad-sdk.exe 4. Report generated with findings
Expected Result:	PEStudio should generate report that contains a list of IOCs indicating that this application is malicious
Actual Result:	PEStudio generated a report containing malicious IOCs (refer Figure 5.28, which clearly indicated that MEmu-setup-abroad-sdk.exe is a malicious executable
Status:	Pass

Observations: On analysing the MEmu-setup-abroad-sdk.exe file downloaded in our sandbox, it was observed that the VirusTotal score was 25/71, meaning 25 out of 71 security vendors flagged this file as a riskware, Trojan, Artemis and all in all unsafe. The libraries exported were all malicious and requested for administrator level permissions to execute, indicating privilege escalation malicious tactic commonly used by malwares (refer Figure 5.28 and Figure 5.29). From these indicators of compromise, we can conclude that MEmuPlay is not only malicious, but also illegally hosting Nike's Android APK file and abusing its brand reputation.

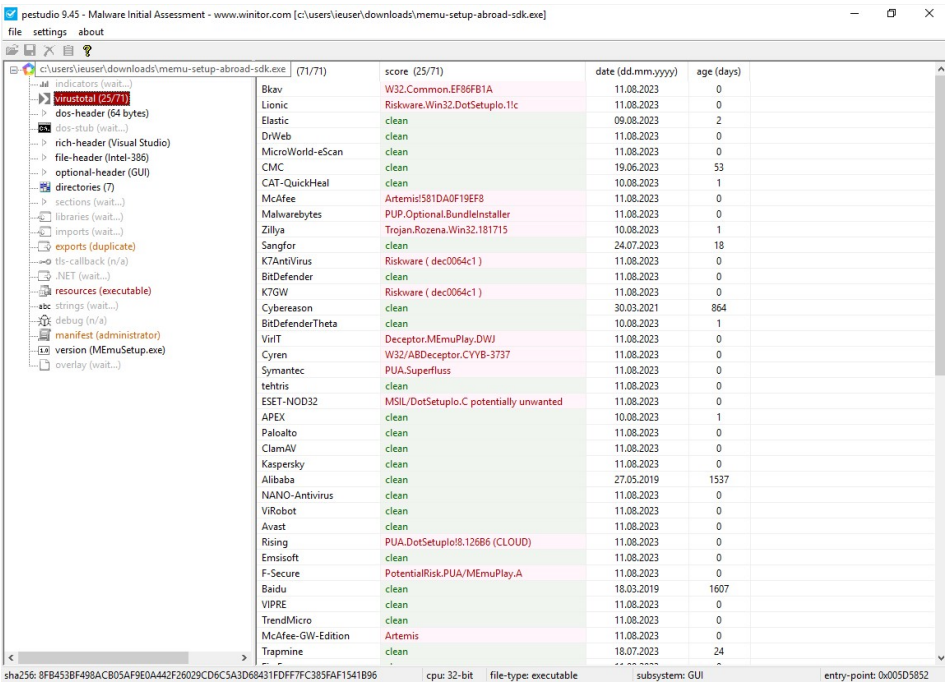


FIGURE 5.28: PEStudio's analysis of MEmu-setup-abroad-sdk.exe

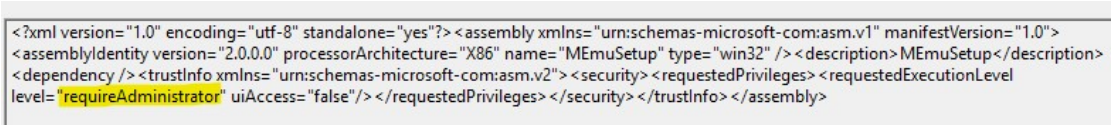


FIGURE 5.29: MEmu-setup-abroad-sdk.exe requesting for Admin privileges

Comparative Analysis of Scamsweep vs. Commercial Solution: To validate our findings from HashCalc and PEStudio, we tried to install MEmu-setup-abroad-sdk.exe in a sandboxed environment. McAfee Anti-Virus [66] generated an alert and tried to block this installation as a preventive measure. It described the file to be suspicious with high security risk. Since a commercial anti-virus software like McAfee also flagged this installation as a security risk, we can say that the results derived from HashCalc and PEStudio are accurate and these tools add immense value for conducting malware analysis and reverse engineering when included in the final toolkit of Scamsweep.

It is to be noted that McAfee Anti-Virus is not a part of Scamsweep's final toolkit. It is only being used as a commercial solution for validation of our results while testing HashCalc and PEStudio on Nike's intellectual properties.

5.8 Use Case 8: Brand Risk Assessment

Use Case 8 involves conducting a Brand Risk Assessment using a customised risk assessment framework to evaluate and categorize potential risks to a brand's reputation, such as Nike, based on identified threat indicators and their corresponding impact and likelihood scores.

5.8.1 Test Case 8.0: Testing the Risk Assessment Framework

Test Case 8.0 assesses the effectiveness of the developed risk assessment framework by evaluating identified threat indicators' impact-likelihood scores and aligning them with the MITRE ATT&CK Framework for brand risk assessment of Nike Inc.

Observations: The conducted brand risk assessment revealed several noteworthy observations. Domain infringement was identified as a high-risk concern with a total risk score of 16, where indicators such as the presence of the target brand name in domain names and URLs, as well as the sale of items resembling the brand's products, were flagged. A low-risk issue involving trademark or copyright infringement scored 1 point. Social media impersonation demonstrated high-risk potential with a cumulative risk score of 16, considering indicators like the presence of similar logos and trademarked text, as

Test ID:	8.0
Tool:	Microsoft Excel
Platform:	Windows
Purpose:	To perform a risk assessment on Nike Inc.
Steps:	1. Open the Excel sheet containing the risk assessment framework developed during implementation phase. 2. Add the threat indicators identified in their respective categories. 3. If the conditions defined in the risk assessment matrix are satisfied then, allocate 1 point for each "Yes" and 0 points for each "No". 4. Calculate the total score for Impact and Likelihood 5. Multiply impact and likelihood for each feature. The product is the risk score. 6. Map the risk score on the heat map or 4x4 risk matrix developed to find the risk rating, i.e., high, medium, tolerable or low. 7. Align the threat indicators with the malicious tactics, techniques and procedures (TTPs) defined in the MITRE ATT&CK Framework.
Expected Result:	We should identify at least one high risk on conducting a brand risk assessment on Nike.
Actual Result:	We identified 2 high risks, 1 medium risk and 1 low risk as result of the brand risk assessment conducted on Nike (refer Figure 5.30).
Status:	Pass

well as the sale of brand-resembling items. The assessment highlighted a medium-risk scenario related to rogue applications, totaling a risk score of 9, where the malicious hash value of an application and the presence of similar trademarks were of concern.

Sl. No.	Brand Risks	MITRE ATT&CK Mapping	Source of Indicator	Threat Indicator	Conditions	Observations	Impact (x)	Likelihood (y)	Risk Rating
1	Domain Infringement	Tactic: Resource Development (TA0042) Technique: Acquire Infrastructure: Domains (T1583.001)	• Maltego • Recon-ng • OTX Alienvault • Microsoft Threat Defender Intelligence	Domain Name: nike.ink nikenflcheapjerseys.us nikeclearance.us nikeshang.shop	Is the target brand name present in URL or domain name, whose resolved IP reputation is poor?	Yes	1	1	High
					Does the website contain trademarked words of the target brand?	Yes	1	1	
					Does the website contain logos similar to target brand?	Yes	1	1	
					Is the website selling items that look similar to products of the target brand?	Yes	1	1	
Total Score							4	4	16
2	Trademark or Copyright Infringement	Tactic: Resource Development (TA0042) Technique: Acquire Infrastructure: Malvertising (T1583.008)	• Platform where the text was observed in use	Text Detected: Don't Dream It, Just Do It JUST DO IT. EVEN WITH NO ONE WATCHING. JUST DO IT.	Found text similar to the registered trademarks of the target brand?	Yes	1	1	Low
Total Score							1	1	1
3	Social Media Impersonation	Tactic: Resource Development (TA0042) Technique: Establish Accounts: Social Media Accounts (T1585.001)	• Instagram • Facebook • Twitter • LinkedIn	Account Name: Instagram: nike__colombia, coles__nike_slippers, fake_nikesneakerscommunity unbox.nike	Found text similar to the registered trademarks of the target brand?	Yes	1	1	High
					Found logos similar to the registered logos of the target brand?	Yes	1	1	
					Found items on sale that look similar to products of the target brand?	Yes	1	1	
					Is the user engagement ratio low?	Yes	1	1	
Total Score							4	4	16
4	Rogue Applications	Tactic: Privilege Escalation (TA0004) Technique: Abuse Elevation Control Mechanism (T1548)	• Android Playstore • Apple Playstore	Application Name: MEmu-setup-abroad-sdk.exe	Is the hash value of the application malicious?	Yes	1	1	Medium
					Found text similar to the registered trademarks of the target brand?	Yes	1	1	
					Found logos similar to the registered logos of the target brand?	Yes	1	1	
					Found items on sale that look similar to products of the target brand?	No	0	0	
Total Score							3	3	9

FIGURE 5.30: Brand Risk Assessment performed on Nike Inc.

In conclusion, the conducted risk assessment has provided valuable insights into the potential risks associated with Nike, showcasing the effectiveness of the developed risk assessment framework and its valuable contribution to the comprehensive toolkit of Scamsweep.

5.9 Use Case 9: Alert Generation

Use Case 9 involves the generation of alerts for reporting the high and medium risks identified using an open-source Intrusion Detection System (IDS), i.e., Snort.

5.9.1 Test Case 9.0: Testing the Snort rules developed using Snorpy

During the implementation phase, 2 rules were developed using Snorpy tool to generate Snort alerts for high and medium risks. In Test Case 9.0, we shall test rules by visiting the malicious website nike.ink to validate whether the Snort fires the rules successfully or not. We edited the rule slightly by including the hostname "nike.ink" in the content field with HTTP status code of 200. Given below is the rule to be used for this test case:

Test Rule: ***alert tcp any any → any any (msg:"Send an Email Alert to User when the Risk is High"; content:"Host: nike.ink"; http_stat_code:"200"; flags:AS; classtype:High; priority:1; sid:100005; rev:1;)***

Test ID:	9.0
Tool:	Snort
Platform:	Linux
Purpose:	To verify if Snort triggers the defined test rule on visiting "nike.ink".
Steps:	1. Use the command *sudo nano /etc/snort/rules/local.rules* to include the two rules given above in the local.rules file. 2. Use the command *cd /var/log/snort* to change the present working directory to *snort*. 3. Use the command *sudo snort -c /etc/snort/snort.conf -A* to run Snort on Alert mode (option -A stands for alert). 4. Open browser and go to "nike.ink". This should spawn a process to trigger the defined test alert. 5. Use the command *ps aux — grep snort* to list running processes related to Snort by searching for the keyword "snort" in the process list using grep. 6. Use the *ls* command to list the processes. We see that an "alert" file has been created (refer Figure). 7. Use the command *cat alert* to display the triggered rule
Expected Result:	Snort should display the message "Send an Email Alert to User when the Risk is High" along with a timestamp of the exact time when "nike.ink" was visited
Actual Result:	Snort did not display any message or timestamp. It displayed a blank "alert" file with no content (refer Figure 5.31).
Status:	Fail

Observations: This clearly shows that the rules must be fine-tuned further for generating alerts in real-time. To effectively trigger it, new fields must be added, which is

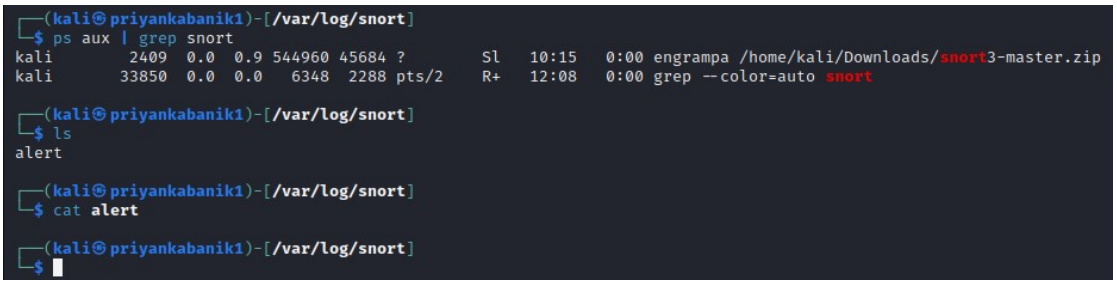


FIGURE 5.31: Screenshot of test rule deployed on Snort local.rules file

a task for the future. Therefore, to circumvent this failure, we shall manually send an email to report our findings to Nike at *counterfeits@nike.com* [70]. This email address has been provided in the official website of Nike to prevent illegal trafficking and sale of fake Nike products.

See Appendix **D.1** for the email template to initiate the take down process at client side, i.e., Nike.

Chapter 6

Discussion and Conclusion

This final chapter contains a critical evaluation of the overall work that was completed as part of this project. It outlines how the project goals were or were not met or answered. It also mentions the issues affecting the performance of the final toolkit and highlights the areas of improvement and scope for extension of the project in future.

6.1 Discussion

This section summarises to what extent the project goals were achieved and how well the project was handled. It also highlights new additional inputs to improve the current state of the proposed open-source toolkit for online brand protection.

- The data collection process was successful on leveraging open-source platforms like Kaggle and Gerben Trademark Library. These platforms contributed significantly in creating a centralised repository of digital assets pertaining to the brand being investigated.
- The web-reconnaissance process was also a productive test as we were able to scan the internet thoroughly using 4 open-source tools like: Maltego, Recon-ng, OTX Alienvault and Microsoft Defender Threat Intelligence. We were able to demonstrate the reconnaissance process successfully on Windows, Linux and Cloud environments. Thus, making Scamsweep a platform independent solution while performing web-reconnaissance. We also collected a large volume of data during this process, which allowed us to detect threats and investigate them in real-time while testing and evaluating various use cases defined Chapter 5.

- The domain infringement check was a productive test. We were able to analyse the live snapshot of a URL utilising an open-source URL sandbox like URLScan.io and check the reputation of the associated domain or IP address using Cisco Talos Intelligence. Additionally, tools like Sucuri and VirusTotal helped in determining the security risks and malware associated with the suspicious domain.

- The trademark infringement test was satisfactory with few identified shortcomings. Limitation of the trademark infringement script is that it is not intelligent enough to process long texts correctly for detecting copyright violations. So, the logic needs to be improved further by including more conditions such as: frequency of usage of trademarked words, calculating the percentage of trademarked words against the total number of words in the input text provided by user.

- On testing the image processing script, it was concluded that the script has a lot of room for improvement. At present, we have achieved the incorporation of only few very basic or fundamental features of image-processing, i.e., resizing the images and converting them to grayscale to maintain uniformity, generating histograms of images, handling angles of rotated images with Chi-square distance calculation. The main limitation of the image processing script is that it cannot differentiate between real and counterfeit logos correctly at all time using Chi-square distance as the only metric because on a slight mismatch in resolution or shape, the script declares the test image as a fake logo. To detect a real logo, the test image has to be an exact copy of one of the real images contained in the RealImage folder in Google Drive. Therefore to enhance the accuracy of the output generated by the script, we need to take a step further by including other vectors such as: keypoints, descriptors, image contours, etc. in the defined image processing functions. Also, the threshold value for detecting the similarity of images needs to be a concrete value. Setting this fixed threshold value that would work out fine for all brands, requires more research and literature review on computer vision techniques.

- It was found that Phlanx's user engagement ratio is not the best metric for social media monitoring of brand risks. The individual factors contributing to the engagement ratio calculation are unique values, where each value has a unique influence on the overall threat investigation. So, normalising them to arrive at a certain percentage value (also called user engagement ratio) and then using that percentage to evaluate brand risks requires inclusion of more factors that are directly or indirectly proportional to this percentage value. Then by combing all the these factors together, we can develop a more complex but efficient logic to evaluate the social media monitoring feature of Scamsweep. Phlanx on its own only is not a sufficient capability to meet the requirements of this feature.

- The tests conducted on malicious applications using HashCalc and PEStudio were productive ones. We were able to demonstrate a counterfeit application and provide a scientific justification that the application is malicious using malware analysis and reverse engineering techniques.
- During the brand risk assessment, we detected 2 high risks, 1 medium and 1 low risk each with our customised framework that was developed after going through NIST RMF, ISO 31000 and FAIR risk management models. To improve the reliability of the tailored framework, we also mapped the MITRE ATT&CK tactics and techniques with the identified threat indicators. The 4x4 risk matrix combined with the "Risk = Impact x Likelihood" formula proved to be an efficient risk assessment methodology.
- Two Snorts rules were successfully implemented without any errors. However, while testing these rules, they triggered a blank alert. We were not able to display the intended alert message due to which we decided to report the findings manually by sending an email to the appropriate target recipient. We also developed a sample email template that can be used to begin the incident management or takedown process for mitigating the identified risk. Taking approval from the customer to report abuse any IOC is the first step of brand protection. The remediation strategy involves contacting the domain registrant and requesting them to take down the fake domain. If they take down, then the incident is closed. Else, a legal battle goes on between the company filing the complaint and the company or individual being accused, which falls under the scope of cyber laws and is handled by the legal and marketing teams of the target organisation.

Based on the discussion points provided above, here is a summary of how well the research questions were answered:

1. **Can open-source tools be used to deliver actionable intelligence and enforcement solutions pertaining to online brand management?**

   The research demonstrated successful utilization of multiple open-source tools, such as Maltego, Recon-ng, OTX Alienvault and Microsoft Defender Threat Intelligence for performing web-reconnaissance. It also demonstrated the usage of open-source tools like URLScan.io and Cisco Talos Intelligence for domain analysis, HashCalc and PEStudio for malware analysis. This confirms that open-source tools can indeed provide actionable intelligence for online brand management.

2. **What method would be used to collect data such as: logos, marketing keywords, trademarks, copyrights, description or any form of intellectual property that defines a particular brand name?**

The data collection process involved leveraging open-source platforms like Kaggle and Gerben Trademark Library. This helped create a centralized repository of digital assets related to the brand under investigation. This method successfully collected various forms of intellectual property associated with the brand, including logos, trademarks and copyrights.

3. **How to build a risk register with a logical metric system that would allocate a threat score to an incident pertaining to brand abuse?**

   The research developed a tailored risk assessment framework, drawing inspiration from NIST RMF, ISO 31000 and FAIR risk management models. The framework utilized a 4x4 risk matrix combined with the "Risk = Impact x Likelihood" formula to assign threat scores to incidents. This approach logically quantified and assessed brand abuse threats, successfully constructing a risk register.

4. **Are there any limitations on what can or should be automated while developing a brand protection strategy?**

   The research identified limitations in the automation of certain processes. For example, the image processing script had room for improvement in distinguishing between real and counterfeit logos. The trademark infringement script also had shortcomings in processing longer texts accurately. This indicates that while automation can streamline certain aspects of brand protection, there are complexities and nuances that may require further human intervention or advanced techniques.

5. **Are pre-existing solutions in the market suitable for online brand protection or is there more work to be done?**

   The research provided insights into the limitations of existing solutions. For instance, the Phlanx user engagement ratio was found to be insufficient as a sole metric for social media monitoring of brand risks. This suggests that while pre-existing solutions may offer some value, there is room for enhancement and development of more comprehensive solutions to address specific brand protection needs.

Overall, the research conducted throughout the project effectively addressed the provided research questions, showcasing the successful utilization of open-source tools, data collection methods, risk assessment frameworks and identification of limitations in automation and pre-existing solutions for online brand protection.

6.2 Conclusion

In conclusion, this project has yielded productive results while also leaving certain aspects unresolved. Scamsweep achieved successful data collection from open-source platforms, conducted comprehensive web-reconnaissance and detected threats through trademark infringement checks and malicious application analysis. The project showcased strengths in risk assessment, domain, IP and URL analysis and outlining incident management procedures. However, challenges surfaced in text processing, image recognition and social media monitoring. While achievements are evident, continued development is essential to fulfill the toolkit's promise of comprehensive open-source online brand protection solution to conduct PoCs before investing in commercial brand protection solutions. The initial groundwork has been established to pave the way for future enhancements and practical applications. Asserting that the mitigation of online brand risks through open-source solutions is achievable, given the insights and progress from this project, would not be an overstatement. Nonetheless, absolute certainty in this claim is still lacking. Additional efforts are undeniably required and the suggested implementations must be fully realized before making definitive statements of this nature. This consideration naturally leads us to contemplate potential avenues for future work on this brand protection project.

6.3 Future Work

The future scope of work for Scamsweep holds a series of strategic enhancements to fortify its brand protection capabilities. One key focus will be on augmenting its existing design with a new dark web monitoring feature, extending its coverage to the hidden realms of the internet using The Onion Router (TOR) browser [71], where threats often emerge in the form of counterfeit products being sold illegally on online black markets hosted on the dark web. Dark web monitoring involves tracking illicit activities on the hidden part of the internet, aiming to identify threats and data breaches. Specialized tools crawl the dark web via the TOR network, collecting data from forums, marketplaces and chatrooms. Keyword recognition and pattern matching are used to pinpoint relevant information, which is then analyzed for credibility and context. Monitoring tools generate alerts when potential threats are detected, enabling timely action. Continuous monitoring is essential due to evolving risks. Tracking of stolen data helps individuals and organizations identify compromised information. Ethical and legal considerations are paramount, as certain activities are illegal. Many organizations opt for cybersecurity consulting firms or commercial brand monitoring services like ZeroFOX (one of the very few commercial tools to have this feature implemented in their brand

protection solution) to ensure effective dark web surveillance within legal and ethical bounds. Therefore, as a future scope of work we should try to come up with a strategy to implement the dark web monitoring feature in Scamsweep by integrating various open-source tools and technologies.

Substantial improvements are envisioned for the image processing and trademark infringement scripts, enhancing accuracy and versatility. Strengthening the Snort rules will enable more precise alert generation, contributing to proactive risk mitigation. Integrating an SMTP server will automate the email alert process, streamlining incident reporting. Establishing a MySQL database will enhance data management efficiency. It is an industry acknowledged platform for both storing and processing the data. On learning how to write SQL queries in future, we can process large volumes of data under one roof and can avoid the current complexity of storing it in on Google Drive and then managing it separately on MS Excel. Furthermore, linking a list of blacklisted IP addresses with the firewall system will enable real-time blocking of traffic to malicious websites.

Lastly, a GUI development initiative for the front-end architecture of Scamsweep shall make the toolkit more user-friendly and accessible, simplifying navigation and enhancing overall usability. This process involves creating the visual elements and interactive components of Scamsweep, enabling users to interact with the application through intuitive icons, buttons, forms and menus (refer Figure 3.2 in Chapter 3). It focuses on designing a user-friendly interface that enhances user experience and simplifies task execution. These concerted efforts promise to elevate Scamsweep's present effectiveness in safeguarding brands against diverse online threats.

Bibliography

[1] "Brandjacking," 2010. [Online]. Available: https://en.wikipedia.org/wiki/Brandjacking

[2] "Un online shopping statistics." [Online]. Available: https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows

[3] J. Amankwah-Amoah, Z. Khan, G. Wood, and G. Knight, "Covid-19 and digitalization: The great acceleration," *Journal of Business Research*, vol. 136, pp. 602–611, 2021.

[4] W. Tounsi and H. Rais, "A survey on technical threat intelligence in the age of sophisticated cyber attacks," *Computers & security*, vol. 72, pp. 212–233, 2018.

[5] "Forbes: E-commerce jumped 55% during covid to hit $1.7 trillion." [Online]. Available: https://www.forbes.com/sites/johnkoetsier/2022/03/15/pandemic-digital-spend-17-trillion/?sh=afbf63e50352

[6] S. Kemp, D. Buil-Gil, A. Moneva, F. Miró-Llinares, and N. Díaz-Castaño, "Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during covid-19," *Journal of Contemporary Criminal Justice*, vol. 37, no. 4, pp. 480–501, 2021.

[7] S. Rao, A. K. Verma, and T. Bhatia, "Online social networks misuse, cyber crimes, and counter mechanisms," in *Analyzing Global Social Media Consumption*. IGI Global, 2021, pp. 183–203.

[8] M. J. Saunders, "Criminal copyright infringement and the copyright felony act," *Denv. UL Rev.*, vol. 71, p. 671, 1993.

[9] "Cloudflare: What is a domain name?" [Online]. Available: https://www.cloudflare.com/learning/dns/glossary/what-is-a-domain-name

[10] K. Elliott, "The who, what, where, when, and why of whois: Privacy and accuracy concerns of the whois database," *SMU Sci. & Tech. L. Rev.*, vol. 12, p. 141, 2008.

[11] A. Chikada and A. Gupta, "Online brand protection," in *Handbook of Research on Counterfeiting and Illicit Trade*. Edward Elgar Publishing, 2017, pp. 340–365.

[12] S. Mackenzie and D. Yates, "What is grey about the "grey market" in antiquities," *The architecture of illegal markets: Towards an economic sociology of illegality in the economy*, pp. 70–86, 2017.

[13] "Redpoints: Online marketplace monitoring," 2022. [Online]. Available: https://www.redpoints.com/usecase/online-marketplace-monitoring/

[14] K. Y. Emerson, "From amazon's domination of e-commerce to its foray into patent litigation: Will amazon succeed as the district of amazon federal court," *NCJL & Tech.*, vol. 21, p. 71, 2019.

[15] "Brandshield." [Online]. Available: https://www.brandshield.com

[16] K. Zarei, R. Farahbakhsh, N. Crespi, and G. Tyson, "Impersonation on social media: a deep neural approach to identify ingenuine content," in *2020 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*. IEEE, 2020, pp. 11–15.

[17] J. L. Kröger, "Rogue apps, hidden web tracking and ubiquitous sensors," 2022.

[18] W. M. Lane and M. Daus, "Rogue'smartphone applications for taxicabs and limousines: Innovation or unfair competition," *New York: Windels Marx Lane and Mittendorf, LLP). http://www. windelsmarx. com/resources/documents/Rogue% 20Applications% 20Memo*, vol. 20, no. 20, p. 10777883, 2012.

[19] "What is a kaggle?" 2022. [Online]. Available: https://www.kaggle.com/discussions/general/328265

[20] T. Balamuralikrishna, N. Raghavendrasai, and M. S. Sukumar, "Mitigating online fraud by ant phishing model with url & image based webpage matching," *International Journal of Scientific & Engineering Research*, vol. 3, no. 3, pp. 1–6, 2012.

[21] "About urlscan.io," 2022. [Online]. Available: https://urlscan.io/about/

[22] "Cisco talos intelligence," 2023. [Online]. Available: https://blog.talosintelligence.com/

[23] "Iris investigate," 2023. [Online]. Available: https://www.domaintools.com/products/platform/iris-investigate/

[24] "Mitre att&ck - reconnaissance." [Online]. Available: https://attack.mitre.org/tactics/TA0043/

[25] "What is maltego community edition (ce)?" 2022. [Online]. Available: https://docs.maltego.com/support/solutions/articles/15000018947-what-is-maltego-community-edition-ce-

[26] "Reconng," 2022. [Online]. Available: https://github.com/lanmaster53/recon-ng/wiki

[27] "Hackertarget: Ip tools for security and network testing," 2022. [Online]. Available: https://hackertarget.com/ip-tools/

[28] P. Snyder and A. Vault, "Playing hackers at their own game," *Network Security*, vol. 2016, no. 11, pp. 14–16, 2016.

[29] "Passive total," 2022. [Online]. Available: https://community.riskiq.com/

[30] V. Rakesh, P. Chilukuri, P. Vaishnavi, P. Sreekaran, P. Sujala, and D. R. K. Yadav, "Real time object recognition using opencv and numpy in python," in *2023 International Conference on Innovative Data Communication Technologies and Application (ICIDCA)*. IEEE, 2023, pp. 421–426.

[31] V. Asha, N. U. Bhajantri, and P. Nagabhushan, "Glcm–based chi–square histogram distance for automatic detection of defects on patterned textures," *International Journal of Computational Vision and Robotics*, vol. 2, no. 4, pp. 302–313, 2011.

[32] "Converting colors rgb(0,255,63)." [Online]. Available: https://convertingcolors.com/rgb-color-0_255_63.pdf

[33] A. Adrakatti, R. Wodeyar, and K. Mulla, "Search by image: a novel approach to content based image retrieval system," *International Journal of Library Science*, vol. 14, no. 3, pp. 41–47, 2016.

[34] "About gerben," 2022. [Online]. Available: https://www.gerbenlaw.com/about/

[35] "Three-person all-wcl alumni trademark law firm achieves success—and national recognition," 2022. [Online]. Available: https://www.wcl.american.edu/news-events/news/three-person-all-wcl-alumni-trademark-law-firm-achieves-success-and-national-recognition/

[36] M. Hansen, "Plotting course," *ABAJ*, vol. 96, p. 26, 2010.

[37] "Gerben trademark library," 2022. [Online]. Available: https://www.gerbenlaw.com/trademarks/

[38] R. Manrique, N. Amézquita, and J. P. Carreño, "Oportunidades y desafíos en la aplicación de inteligencia artificial a procesos de validación marcaria," *Revista Ibérica de Sistemas e Tecnologias de Informação*, no. E24, pp. 221–233, 2019.

[39] A. Sary, "Social media as communication strategy for susi pudjiastuti to build maritime security awareness in indonesia."

[40] "How to measure instagram engagement," 2023. [Online]. Available: https://phlanx.com/tips/how-measure-instagram-engagement

[41] "Phlanx review," 2023. [Online]. Available: https://www.accuratereviews.com/influencer-marketing-platforms/phlanx-review/

[42] M. N. Hermanto *et al.*, "Analisis forensic berbasis web phising menggunakan metode national institute of standards and technology," *Jurnal Informasi dan Komputer*, vol. 11, no. 01, pp. 116–123, 2023.

[43] A. Amiruddin, C. Kurniawan, E. H. Ramadhani, and J. Rinaldi, "Learning the basic strcuture of several ransomwares using static analysis tecgnique," in *IOP Conference Series: Materials Science and Engineering*, vol. 1007, no. 1. IOP Publishing, 2020, p. 012072.

[44] A. Orebaugh, S. Biles, and J. Babbin, *Snort Cookbook: Solutions and Examples for Snort Administrators.* " O'Reilly Media, Inc.", 2005.

[45] "Why is risk management important?" 2022. [Online]. Available: https://www.ibm.com/topics/risk-management

[46] "Iso 31000 risk management," 2022. [Online]. Available: www.iso.org/iso-31000-risk-management.html

[47] "Nist risk management framework," 2022. [Online]. Available: https://csrc.nist.gov/Projects/risk-management

[48] "How to model controls in a fair risk analysis," 2022. [Online]. Available: https://www.fairinstitute.org/blog/how-to-model-controls-in-a-fair-risk-analysis

[49] "Mitre attck framework," 2023. [Online]. Available: https://attack.mitre.org/

[50] S. Roy, E. Panaousis, C. Noakes, A. Laszka, S. Panda, and G. Loukas, "Sok: The mitre att&ck framework in research and practice," *arXiv preprint arXiv:2304.07411*, 2023.

[51] W. J. Ma, "Bayesian decision models: A primer," *Neuron*, vol. 104, no. 1, pp. 164–175, 2019.

[52] T. Williams, "The two-dimensionality of project risk," *International Journal of Project Management*, vol. 14, no. 3, pp. 185–186, 1996.

[53] "Zerofox brand protection." [Online]. Available: https://www.zerofox.com/products/brand-protection/

[54] "Riskiq brand protection." [Online]. Available: https://www.riskiq.com/solutions/brand-protection/

[55] "urlscan.io - a sandbox for the web," 2023. [Online]. Available: https://phlanx.com/tips/how-measure-instagram-engagement

[56] "Ip domain reputation center," 2023. [Online]. Available: https://talosintelligence.com/reputation_center/

[57] "Free website malware and security checker," 2023. [Online]. Available: https://sitecheck.sucuri.net/

[58] "Virustotal," 2023. [Online]. Available: https://www.virustotal.com/gui/home/upload

[59] "Chi-square distance in python," 2022. [Online]. Available: https://www.geeksforgeeks.org/chi-square-distance-in-python/

[60] "Gerben trademark library," 2023. [Online]. Available: https://www.gerbenlaw.com/trademarks/

[61] A. Atar, *Hands-On Test Management with JIRA: End-to-end test management with Zephyr, synapseRT, and Jenkins in JIRA*. Packt Publishing Ltd, 2019.

[62] "Domain generation algorithm," 2022. [Online]. Available: https://en.wikipedia.org/wiki/Domain_generation_algorithm

[63] "How a spoofed email passed the spf check and landed in my inbox," 2022. [Online]. Available: https://www.welivesecurity.com/2022/08/16/spoofed-email-passed-spf-check-inbox/

[64] "Scammer abusing your ssl certificate," 2022. [Online]. Available: https://community.letsencrypt.org/t/scammer-abusing-your-ssl-certificate/52753

[65] "Namecheap inc," 2022. [Online]. Available: https://www.namecheap.com/about/

[66] "Mcafee anti-virus," 2023. [Online]. Available: https://www.mcafee.com/en-ie/antivirus.html

[67] G. co, "Nike dataset," aug 2022, visited on 2023-08-09. [Online]. Available: https://universe.roboflow.com/ghazal-co/nike-9ertk

[68] W. Zhou, H. Li, and Q. Tian, "Recent advance in content-based image retrieval: A literature survey," *arXiv preprint arXiv:1706.06064*, 2017.

[69] "Five red flags that will help you spot fake influencers," 2023. [Online]. Available: https://www.clickz.com/five-red-flags-fake-influencers/226462/

[70] "Have i bought fake nikes?" 2022. [Online]. Available: https://www.nike.com/help/a/nike-product-authenticity

[71] A. Macrina and E. Phetteplace, "The tor browser and intellectual freedom in the digital age," *Reference and User Services Quarterly*, vol. 54, no. 4, pp. 17–20, 2015.

[72] "What is a pr crisis? how to manage brand reputation swiftly," 2021. [Online]. Available: https://www.g2.com/articles/pr-crisis

[73] "The rise of counterfeiting and its effects on nike," 2014. [Online]. Available: https://soapboxie.com/economy/The-Rise-of-Counterfeiting-and-Its-Effects-on-Nike

[74] "Nike annual report 2022," 2022. [Online]. Available: https://s1.q4cdn.com/806093406/files/doc_financials/2022/NikeInc_2022_Annual_Report.pdf

[75] "Nike's four-phase covid-19 response strategy," 2020. [Online]. Available: https://www.warc.com/newsandopinion/news/nikes-four-phase-covid-19-response-strategy/en-gb/43437

[76] C. O'Kane, "Nike repurposing sneakers to create face shields for health care workers," 2020. [Online]. Available: https://www.cbsnews.com/news/nike-face-sheild-repurposing-air-max-sneakers-to-create-ppe-health-care-workers-coroanvirus-hosp

[77] "Nike: Play inside, play for the world," 2021. [Online]. Available: https://www.thedrum.com/creative-works/project/nike-play-inside-play-the-world

[78] "The best free workouts on the nike training club app," 2022. [Online]. Available: https://www.nike.com/ph/a/free-workout-plans

[79] "Challenges faced by nike to protect its intellectual property," 2023. [Online]. Available: https://blog.ipleaders.in/challenges-faced-nike-protect-intellectual-property/

[80] "Wipo," 2023. [Online]. Available: https://www.wipo.int/

[81] "Madrid protocol," 2023. [Online]. Available: https://www.wipo.int/madrid/en/

[82] "Nike, inc. reports fiscal 2019 fourth quarter and full year results," 2019. [Online]. Available: https://www.businesswire.com/news/home/20190627005883/en/NIKE-Inc.-Reports-Fiscal-2019-Fourth-Quarter-and-Full-Year-Results

[83] "A blown-out sneaker, an injured superstar and a night to forget for nike," 2019. [Online]. Available: https://www.npr.org/2019/02/21/696565989/a-blown-out-sneaker-an-injured-superstar-and-a-night-to-forget-for-nike

[84] "Exploding sneakers are only one reason for passing iot cyber-security regulations," 2023. [Online]. Available: https://diginomica.com/exploding-sneakers-are-only-one-reason-for-passing-iot-cyber-security-regulations

[85] "Nike website flaw exposed sensitive server data," 2018. [Online]. Available: https://www.zdnet.com/article/nike-website-flaw-exposed-access-to-sensitive-server-data/

[86] "Digital technologies and customer experience: How nike is leading the way," 2023. [Online]. Available: https://medium.com/digital-society/digital-technologies-and-customer-experience-how-nike-is-leading-the-way-ce24828e8bdd

[87] "Brand audit for nike," 2021. [Online]. Available: https://peachyessay.com/sample-essay/brand-audit-for-nike/

[88] "Organizational change: Improvement of information security of the nike company research paper," 2022. [Online]. Available: https://ivypanda.com/essays/organizational-change-improvement-of-information-security-of-the-nike-company/

[89] "How nike's digital transformation is monitored," 2018. [Online]. Available: https://medium.com/nikeengineering/how-nikes-digital-transformation-is-monitored-3c0799b3e443

[90] "Counterfeiting made easy through 3d-printing technology?" 2018. [Online]. Available: https://www.scribos.com/blog/counterfeiting-made-easy-through-3d-printing-technology

[91] "Nike qr code: How to use qr codes in footwear and apparel marketing," 2023. [Online]. Available: https://www.qrcode-tiger.com/nike-qr-code

[92] "Nike, adidas settle patent fights over shoe technology," 2022. [Online]. Available: https://www.reuters.com/legal/litigation/nike-adidas-settle-patent-fights-over-shoe-technology-2022-08-19/

[93] "United states: Trademark infringement- nike v. mschf- satan shoes case," 2021. [Online]. Available: https://www.mondaq.com/unitedstates/trademark/1061266/trademark-infringement--nike-v-mschf--satan-shoes-case

[94] "Why nike cut ties with amazon and what it means for other retailers," 2020. [Online]. Available: https://www.forbes.com/sites/forbesbusinesscouncil/2020/01/22/why-nike-cut-ties-with-amazon-and-what-it-means-for-other-retailers/?sh=425d9fd364ff

Appendix A

Case Study on Nike

A.1 Nike's Cyber Threat Response: A Case Study on Brand Protection

1. Introduction

This case study examines Nike's proactive defenses against cyber-attacks and brand protection. Companies have significant challenges in maintaining customer trust and protecting their intellectual property as their reliance on digital platforms expands and cybercrime increases. Nike, a leader in the global sportswear industry, has developed a thorough strategy to tackle online threats because it recognizes the importance of brand protection [72]. According to MSN Money, Nike falls in the list of top 10 most counterfeited brands [73]. The operations of Nike are examined in this case study, including cybersecurity safeguards, brand monitoring, legal actions and collaborations to offer insights into efficient brand protection in the digital age.

2. Background

In terms of sportswear, accessories and gears, Nike is one of the industry leaders. Over the course of five decades, Nike has become synonymous with innovation, performance and style. Nike consistently pushes the envelope to create innovative products that satisfy the needs of athletes all around the world, from its recognizable swoosh logo to its ground-breaking Air technology. Athletes of various levels and disciplines, including those in running, basketball, soccer and golf are drawn to the brand's diverse range. Nike stands out for its commitment to sustainability and social responsibility since it wants to positively impact society and the environment.

3. Purpose and Objective of the Case Study

By creating a specific goal and outlining specific objectives, this case study will provide an in-depth analysis of Nike's reaction to cyber risks and its effects on brand protection. For companies wishing to strengthen their own trademark protection practices, it will also be a helpful resource. The purpose and objective of this case study is to outline Nike's approach to cyber threat for brand protection.

Purpose:

- Analyze and understand Nike's preventative measures for addressing cyber dangers and protecting its brand in the digital era.
- To look into Nike's cyber-threat issues and how the company has handled them.
- To determine how well Nike's brand protection strategies manage cyber threats and maintain brand integrity.
- To collaborate with other businesses on ideas and lessons discovered when developing effective brand protection policies in the face of evolving cyber threats.

Objectives:

- Evaluate Nike's knowledge of cyber threats and their possible effects on the name and intellectual property of the company.
- Discover the specific brand protection techniques and tools used by Nike to thwart cyber risks such as counterfeiting and trademark infringement.
- Analyze the effects and results of Nike's brand protection initiatives, taking into account factors including the number of counterfeiting occurrences, consumer confidence and financial impact.
- Describe the difficulties Nike faced in putting into practice efficient trademark protection strategies and how the firm overcome them.
- Providing Nike and other firms with ideas for improving their brand protection policies in the digital age based on the case study's findings.

Refer Figure A.1 for a graphical view of Nike's revenue over the years.

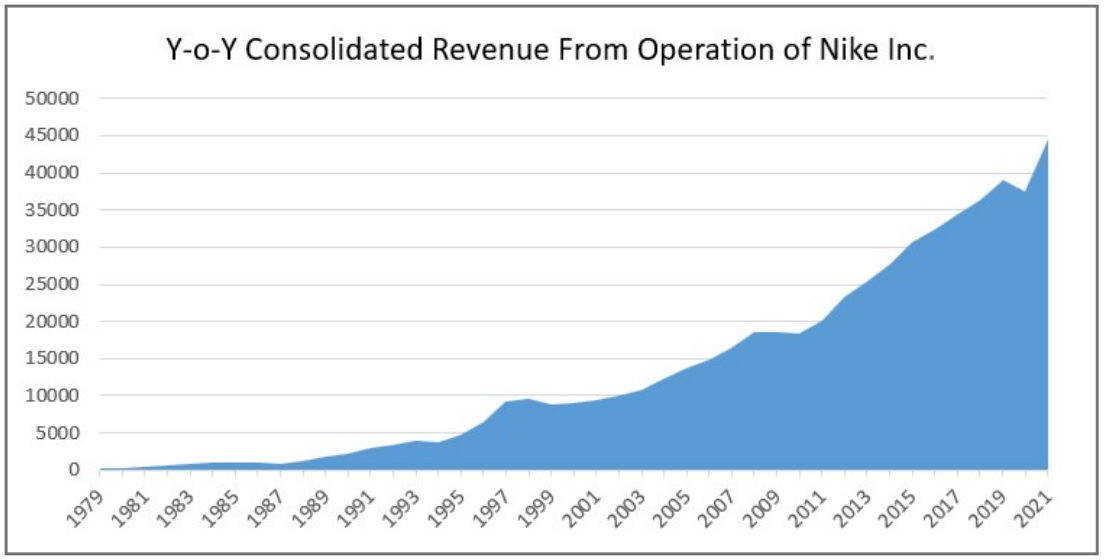


FIGURE A.1: Consolidated revenue earned by Nike Inc. Source: Nike's Annual Report [74]

4. Nike Brand Crisis

Nike adopted a four-phase global reaction to COVID-19, with containment, recovery, normalization and return to growth, based on the state of the market and other considerations [75]. The business contributed to the creation of Personal Protective Equipment (PPE) kit [76] for front-line physicians, nurses and healthcare professionals by utilizing its innovation and marketing teams. It also guaranteed workers that their pay would continue despite the closure of many of its retail locations. Nike's "Play Inside" digital campaign [77] for customers encourages individuals to keep healthy and active while staying at home during inclement weather. Customers could also download the company's well-liked exercise app for free for 90 days [78].

5. Overview of Cyber Threats faced by Nike

Opening up new market frontiers is not simple. A calculated effort, research, compliance, conversations and risk assessments are needed to enter a new market successfully. As it moved from a fashion brand to a lifestyle and athletic brand [79], Nike Inc. faced some intellectual property (IP) considerations. Based on its prowess at protecting and projecting its brand's logo, image and visibility—achieved through intellectual property protection, staff dedication, confidentiality, IP due diligence and in-depth research, endorsement, advertising and collaboration with customers and partners — Nike dominated sports and was able to break into new markets. There was a rise in demand for intellectual property rights to be preserved in many countries, which was typically expensive and effort-intensive because intellectual property is territorial. This drawback has been overcome by WIPO [80] through IP treaties that bind member nations that are

signatories to these treaties in a fashion that allows a mark to be registered throughout any selected state of choice through a single system, such as the Madrid Protocol [81].

6. Impact of Cyber Threat on Nike's Brand Reputation

Unauthorized trademark use by third parties has a number of negative effects on the brand, including dilution, financial losses, the deterioration of goodwill and the withdrawal of partners and investors. Emerging brands frequently assume they have the right to associate with a similar brand without seeking permission from the appropriate authorities first; some do this out of ignorance, but this is not an acceptable defense. Nike has not been exempt from this, and they frequently suffer enormous losses due to trademark dilution, which results in a number of cases with major financial repercussions.

The year 2019 wasn't nice for Nike [82]. Zion Williamson, the top college basketball prospect for Duke University, hurt his knee only 30 seconds into a game against North Carolina when his typical left Nike PG 2.5 shoe exploded on national television [83]. Early buyers of the highly-promoted Nike BB Adapt, a $350 self-lacing sneaker straight out of "Back to the Future II", also started contacting the company with complaints. Electronics comparable to those found in smartphones can be accessible on the BB Adapt using an Android or iPhone app. The Android app did not sync with both shoes, which was something that many early buyers noticed and started raising complaints [84]. Both incidents were embarrassing for Nike and temporarily decreased the company's stock price.

The chart given below shows the revenue breakup of Nike based on Segment Report (refer Figure A.2).

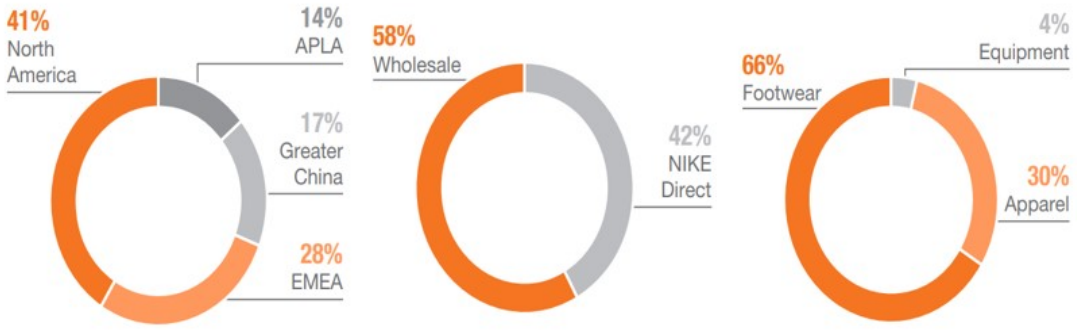


FIGURE A.2: Revenue break-up of Nike Inc. across various regions and segments, Source: Nike's Annual Report [74]

All of these IoT devices, objects, sensors and sneakers created a massive playground for hackers to launch Distributed Denial of Service (DDoS) attacks, which employ swarms

of inadequately protected consumer devices as botnets to attack critical infrastructure through massively coordinated misuse of communication channels.

7. Financial Implications of Brand Infringement on Nike

The financial cost of trademark infringement on brand reputation is significant. Loss of consumer confidence and a fall in sales can result from the misuse of a trademark in a way that hurts the reputation of the target organisation. The company may need to spend more money on advertising and public relations efforts to undo the harm caused by the infringing party's actions. Based on further market research it was found that the loss in brand reputation made Nike spend heavily on brand promotion activities and advertisements [74]. Figure A.3 and Figure A.4 highlights the administrative expense of Nike to combat such issues and the gross margin of profit earned after such expenses from Nike's Annual Report, 2022 [74].

TOTAL SELLING AND ADMINISTRATIVE EXPENSE

(Dollars in millions)	FISCAL 2022	FISCAL 2021	% CHANGE	FISCAL 2020	% CHANGE
Demand creation expense[(1)]	$ 3,850	$ 3,114	24%	$ 3,592	-13%
Operating overhead expense	10,954	9,911	11%	9,534	4%
Total selling and administrative expense	$ 14,804	$ 13,025	14%	$ 13,126	-1%
% of revenues	31.7%	29.2%	250 bps	35.1%	(590) bps

FIGURE A.3: Nike's total selling and administrative expense, Source: Nike's Annual Report [74]

GROSS MARGIN

FISCAL 2022 COMPARED TO FISCAL 2021

For fiscal 2022, our consolidated gross profit increased 8% to $21,479 million compared to $19,962 million for fiscal 2021. Gross margin increased 120 basis points to 46.0% for fiscal 2022 compared to 44.8% for fiscal 2021 due to the following:

FIGURE A.4: Nike's profit margin, Source: Nike's Annual Report [74]

8. Nike's Cyber Security Measures

Investment in Robust Cybersecurity Infrastructure:

Cyber attacks can be a big issue for Nike's brand value. Given that Nike collects a plethora of personal information from users of its many Nike applications. This data may contain personal information such as addresses and payment details, making it beneficial to hackers. Previously, an undocumented vulnerability on Nike's website permitted

anyone just a few lines of code to get server data, including passwords [85]. This implies that if Nike's security system is breached, all customer information will be made public, destroying Nike's reputation and image.

Significant investments are made by Nike in cybersecurity solutions for the protection of consumer data and the preservation of customer trust. The utilization of encryption and other cybersecurity measures is employed by Nike to safeguard customer data [86], making it exceedingly difficult for hackers to access. Collaboration with various IT companies has been undertaken by Nike to address data protection and cybersecurity concerns. In the realm of cybersecurity, partnerships have been established, such as with UpGuard, for the purpose of countering cyber attacks and data breaches [86]. Services encompassing threat intelligence and incident response are provided by UpGuard to aid Nike in promptly detecting and addressing potential security issues. Nevertheless, for the prevention of data breaches in their initial stages, investments in cybersecurity training for employees are considered by Nike.

Regular Security Assessments and Audits:

The purpose of a brand audit is to evaluate the brand's health, identify the sources of its equity and make recommendations for how to enhance and utilise that equity. Marketing professionals may keep a pulse on their brands by regularly conducting security risk assessments and brand audits, which enables them to manage their brands more pro-actively and quickly. A quality brand audit offers insightful information about customers, brands and their interactions. Figure A.5 is a visual illustration of SWOT analysis on Nike's brand image [87].

Collaboration with Cyber Security Experts:

As part of a diverse, cross-functional team that collaborates globally across the organization with stakeholders ranging from service desk technicians to system architects, developers and lawyers, Nike hires a large number of people to provide technical and tactical expertise to a 24x7 team of dedicated security engineers focused on maintaining operational stability while reducing risk.

Unrevealed website failures in the past had the potential to enable the access of server data, including passwords, by individuals possessing specific lines of code. This access could potentially facilitate a smoother entry into Nike's internal systems [85]. Going beyond its identity as a mere sportswear retailer, Nike has undergone a substantial transition recently, involving extensive forays into the realm of data collection. This integration encompasses the merging of sports and activity tracking functionalities into its products, resulting in the creation of wearables. The existence of such a gap in information security highlights the significance that should be attributed by Nike to the

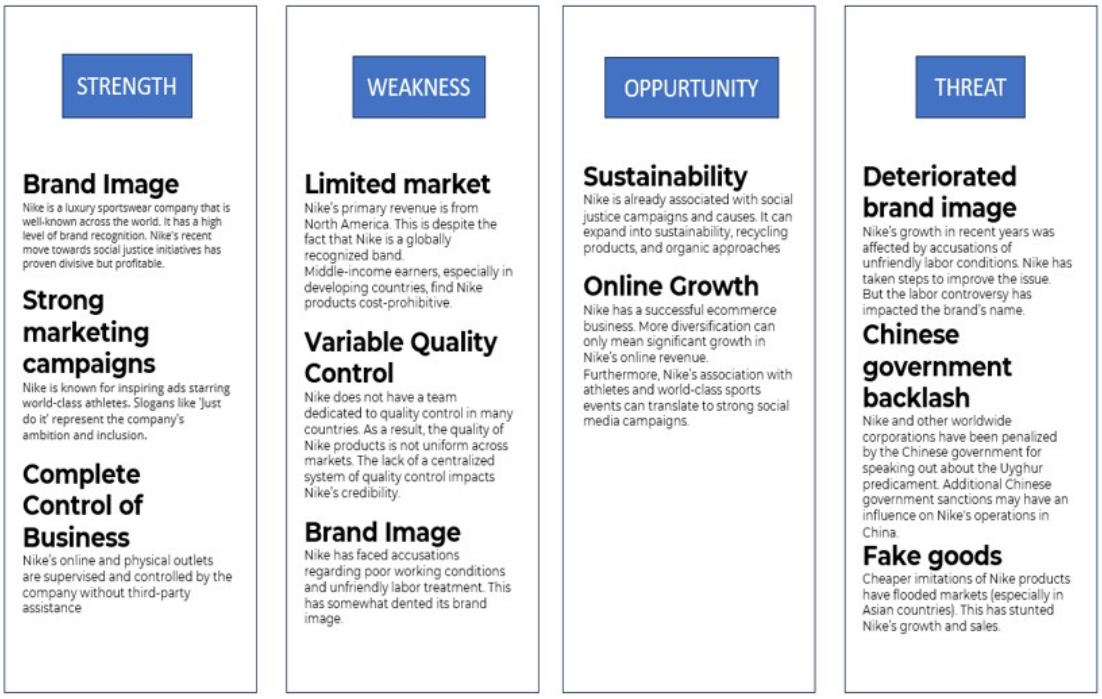


FIGURE A.5: SWOT analysis Nike Inc. [87]

protection of information. In order to address concerns related to information security, a new department has been established within the organization, with a dedicated focus on quality assurance and testing [88].

Monitoring Online Platforms and Social Media:

Starting in the summer of 2017, Nike adopted technology originally designed for high-demand releases to facilitate everyday online sales. This fulfilled the goal of using a single cloud-based service for multiple experiences. While launching key features and approaching the Christmas season, Nike ensured operational services. They chose a distributed micro-services architecture for scalability and recovery, encountering the challenge of monitoring. Custom metrics were identified as necessary to accurately track key performance indicators (KPIs) due to high data volume during launch events. After considering various providers, SignalFx was chosen [89]. However, the dashboard fell short as a monitoring tool, lacking insight into customer purchasing issues.

Identifying Counterfeit Products and Unauthorized Sellers:

The possibility of counterfeit products is one of Nike's biggest problems in the modern day [73]. Modern technology has made it easier for counterfeiters to produce and disseminate fake goods. For instance, utilizing digital methods like 3D printing, counterfeiters may produce remarkably lifelike copies of real goods [90]. Additionally, the growth of social media has made it simpler for counterfeiters to advertise their products online to

a global audience. Since customers cannot personally verify the goods before buying them, businesses frequently mislead them. As a result, both Nike's revenue and brand reputation suffer. Thus, Nike funds initiatives that can aid in solving this issue. For example, Nike developed a mobile application and website that allows people to scan a barcode on a product to verify its authenticity [91].

9. Legal Action and Enforcement

Trademark Infringement Cases and Legal Actions:

- **Nike Vs Adidas**

Nike sued Adidas in Oregon and also filed a complaint with the U.S. International Trade Commission (ITC) [92]. The lawsuits claimed that certain shoe designs by Adidas violate patents associated with Nike's lightweight Flyknit technology. The ITC launched an inquiry into Adidas' shoes based on the filed complaint.

- **Nike Vs MSCHF**

A dispute arose recently between Nike and the conceptual art collective MSCHF over the "Satan Shoes", a modified version of Nike Air Max 97s created with musician Lil Nas X. The shoes contained a pentagram pendant, a Gospel of Luke reference, "one drop of human blood", and crimson ink visible through the sole. MSCHF sold 666 pairs in under a minute, sparking religious and conservative boycott calls. MSCHF's previous "Jesus Shoes" faced no Nike concern but led to a lawsuit for trademark infringement. Nike filed a complaint in the US District Court, asserting that the customized "Satan Shoes" lacked approval or licensing. On April 2, 2021, a federal judge issued an interim injunction, favoring Nike and forbidding MSCHF from producing or marketing the contentious shoes with the Nike trademark [93].

10. Partnerships and Collaborations

Cooperation with online marketplace & e-commerce platforms:

In November 2019, it was announced by Nike that its participation as a first-party seller on Amazon would cease [94], concluding a test program that began in 2017. Nike thought they were losing ground to competitors by not having a sanctioned brand store on Amazon. Nike had initiated the direct distribution partnership with Amazon to counter counterfeit sales and gain better control over the expansive e-commerce platform. However, Nike's performance suffered within six months of the collaboration. The program failed to provide Nike with market dominance or essential control over their products. The attempt to reduce third-party sales did not guarantee increased first-party sales, showcasing the self-regulating nature of the market. Over half of Amazon's

products come from independent merchants earning transaction commissions. Prior to 2017, Amazon mainly hosted counterfeit or "grey market" Nike products [94]. The purpose of the agreement was to curtail unauthorized sales. By eliminating third-party sellers, Nike aimed to direct sales to their own platform, capitalizing on Amazon's retail scale for more consumer data acquisition [94].

11. Recommendations

As an outcome of the case study, below is a list of security recommendations that should be considered by Nike to mitigate brand abuse and enhance its cyber resilience:

• Trademark Monitoring and Enforcement: Implement a robust trademark monitoring system to identify and address any unauthorized use of Nike's brand and logo across various online platforms. Swiftly take legal action against infringing parties to deter unauthorized usage.

• Domain Name Management: Regularly audit domain registrations to identify any domains that might be similar to Nike's brand. Secure relevant domain names to prevent cybersquatting and phishing attempts.

• Social Media Monitoring: Continuously monitor social media platforms for fake accounts, impersonation and unauthorized usage of the Nike brand. Report and take down such accounts promptly.

• Educate Employees: Provide comprehensive training to employees about the importance of brand protection and security measures to prevent leaks of sensitive information.

• Supplier and Partner Vetting: Thoroughly screen suppliers, partners and distributors to ensure they adhere to brand guidelines and security protocols to prevent counterfeiting and unauthorized product sales.

• Anti-Counterfeiting Technologies: Integrate advanced anti-counterfeiting technologies, such as holograms, RFID tags or QR codes into product packaging to help consumers verify the authenticity of Nike products.

• Customer Education: Educate customers on how to identify genuine Nike products and provide them with resources to report suspected counterfeits.

• Digital Brand Protection Tools: Invest in digital brand protection solutions that utilize AI and machine learning to detect unauthorized usage of the Nike brand across websites, social media and online marketplaces.

• Legal Partnerships: Establish partnerships with legal firms specializing in intellectual property and brand protection to ensure a proactive and effective response to brand abuse incidents.

• Cybersecurity Measures: Implement strong cybersecurity measures to safeguard customer data, including encryption, regular security audits and monitoring for data breaches.

• Incident Response Plan: Develop a comprehensive incident response plan to address any brand abuse incidents promptly and effectively minimize potential damage.

• Regular Audits: Conduct regular audits of brand assets, online presence and security protocols to identify vulnerabilities and areas for improvement.

• Community Engagement: Foster a strong relationship with loyal customers and brand advocates through community engagement, building a network that can help report and address brand abuse incidents.

By implementing these recommendations, Nike can enhance its brand protection efforts and minimize the risks associated with brand abuse and unauthorized usage.

12. Conclusion

In conclusion, given the evident need for robust brand protection, characterized by the presence of counterfeited domains, applications and products in plain view, Nike stands out as the optimal choice for testing or running a proof of concept for Scamsweep. With these visible vulnerabilities, Nike's extensive experience in guarding against brand abuse and unauthorized exploitation uniquely positions them to rigorously assess the capabilities of Scamsweep.

Appendix B

Code Snippets

B.1 Detecting Trademark or Copyright Infringements

```
# Determines if a company's registered trademark has been violated
import difflib
import re

# List of trademarked words for the selected brand
trademarked_words = [ "AIRPHORIA", "JUST DO IT", "AIR MAX", "NIKE", "NIKE
STRIDE", "AEROGAMI", "NIKE INFINITYRN", "CRATER", ".SWOOSH", "DOTSWOOSH",
"WINFLO", "NIKE MOTIVA", "CRYPTOKICKS", "NIKE UNIVERSA", "NIKE GO", "NIKE
ZENVY", "INFINALOCK", "INFINASOFT", "SENSEADAPT", "FLYPRINT", "AIRADAPT",
"FITADAPT", "METADUNGEON", "LOOT POD", "D.A.R.T X", "PODX", "SPACE POD",
"MNLTH", "NIKELAND", "WHERE SPORT HAS NO RULES", "DREAM IT. MAKE IT. PLAY
IT.", "AIR JORDAN", "JORDAN", "WAFFLE SUITE", "NEXT NATURE", "BO KNOWS",
"ALPHAFLY", "NO", "SNKRS", "NIKECONNECT", "FLIGHT", "SUPERREP", "23
ENGINEERED", "WAFFLE IRON ENTERTAINMENT", "BRS BLUE RIBBON SPORTS",
"KICKCHECK", "S", "INFINALON", "SNKSTR", "SNKRS STASH", "MOVE TO ZERO",
"GA", "NIKE BY YOU", "FOOTWARE", "M", "AEROADAPT", "OBJ", "SNEAKEASY",
"VAPORMAX", "SPACE HIPPIE", "TECHKNIT", "PEGASUS", "FLYLEATHER", "TRACEME",
"BIKETOWN", "FLYEASE", "METCON", "BETTER FOR IT", "VOMERO", "NIKE LUNAR",
"KICKS LOUNGE", "NIKE AEROSHIELD", "NIKE AIR VAPORMAX", "K I", "VAPOR",
"NIKE VAPOR", "NIKE AEROLOFT", "MAGISTA", "HYPERSTRONG", "KD",
"HYPERVENOM", "MATT MATTHEW KNIGHT ARENA", "NIKESKIN", "FLYKNIT", "LJ" ]

# This function preprocesses the text by removing special characters
```

```
def preprocess_text(text):
    # Remove special characters using regular expression
    processed_text = re.sub(r"[^\w\s]", "", text)
    return processed_text

# This function checks for trademark infringement
def check_trademark_infringement(user_input):
    # Preprocess the user input and convert it to uppercase for comparison
    user_input_processed = preprocess_text(user_input).upper()

    # Iterate over each trademark word
    for word in trademarked_words:
        # Preprocess the trademark word and convert it to uppercase for comparison
        trademark_word_processed = preprocess_text(word).upper()

        # Compare the user input with the trademark word, accounting for
        typographical errors
        similarity_ratio = difflib.SequenceMatcher(None, user_input_processed,
        trademark_word_processed).ratio()

        # Check if the similarity ratio is above a threshold (adjust as needed)
        if similarity_ratio >= 0.8:
            print(f"The similarity ratio: {similarity_ratio:.2f}")
            return True

    print(f"The similarity ratio: {similarity_ratio:%.2f}")
    return False

# Get input from user
user_input = input("Enter a sentence: ")

# Check for trademark infringement
if check_trademark_infringement(user_input):
    print("Trademark infringement observed.")
else:
    print("Not a trademark infringement.")
```

B.2 Differentiating between Real and Fake Logos

```
import cv2

from google.colab import drive
drive.mount('/content/drive')

import os
os.chdir('/content/drive/My Drive/Scamsweep/Nike Logos')

# This function preprocesses real logos to a consistent size and color
def image_preprocessing_real(ImagePath):
    if not os.path.exists(ImagePath):
        raise FileNotFoundError(f"The image file '{ImagePath}' does not exist.")

    image = cv2.imread(ImagePath)
    if image is None:
        raise ValueError(f"Failed to read the image at '{ImagePath}'. Please check
        if the file is a valid image.")

    resized_image = cv2.resize(image, (300, 300))
    processed_image = cv2.cvtColor(resized_image, cv2.COLOR_BGR2GRAY)
    return processed_image

# This function calculates the color histogram of real brand logos
def generate_histogram_real(image):
    hist = cv2.calcHist([image], [0], None, [255], [0, 255])
    return hist.flatten()

# This function uses Chi-square distance to compare two histograms
def generate_histogram_distance(hist1, hist2):
    return cv2.compareHist(hist1, hist2, cv2.HISTCMP_CHISQR)

# This function checks if test image matches any real logo based on threshold value
def is_image_real(ImagePath, threshold):
    path = "/content/drive/My Drive/Scamsweep/Nike Logos/RealNike"
    files = os.listdir(path)

    real_images = []
```

```
    for file in files:
        if file[-4:] == ".jpg" or file[-4:] == ".png" or file[-4:] == ".gif":
            real_image = image_preprocessing_real(path + "/" + file)
            real_images.append((real_image, file))

    image = image_preprocessing_real(ImagePath)
    histogram = generate_histogram_real(image)

    for real_image, filename in real_images:

        real_histogram = generate_histogram_real(real_image)
        histogram_distance = generate_histogram_distance(real_histogram, histogram)

        if histogram_distance < threshold:
            return "Real", filename

    return "Fake", None

# Test Case: Example Usage
ImagePath = "/content/drive/My Drive/Scamsweep/Nike Logos/TestNike/000008.jpg"
threshold = 0.5
try:
    result, matched_real_logo = is_image_real(ImagePath, threshold)
    if matched_real_logo:
        print("This test image appears to be a REAL brand logo.")
        print("Match found with:", matched_real_logo)
    else:
        print("This test image appears to be a FAKE brand logo.")

except (FileNotFoundError, ValueError) as e:
    print("Error:", e)
```

Appendix C

Linux Commands and Outputs

C.1 Reconnaissance Activity on Recon-ng

```
--(kali@priyankabanik1)-[~]
-$ recon-ng
[*] Version check disabled.
    _/_/_/   _/_/_/_/   _/_/_/   _/_/_/   _/      _/      _/      _/   _/_/_/
   _/    _/ _/       _/       _/      _/ _/_/    _/      _/_/    _/ _/
  _/_/_/   _/_/_/   _/       _/      _/ _/  _/  _/ _/_/ _/  _/  _/ _/  _/_/_/
 _/    _/ _/       _/       _/      _/ _/    _/_/      _/    _/_/ _/      _/
_/    _/ _/_/_/_/   _/_/_/   _/_/_/   _/      _/      _/      _/   _/_/_/

                                   /\
                                  / \\ /\
    Sponsored by...             /\  /\/  \\V  \/\
                               / \\/ // \\\\\ \\ \/\
                              // // BLACK HILLS \/ \\
                             www.blackhillsinfosec.com

                 ____   ____   ____   ____ _____ _  ____   ____  ____
                |____] | ___/ |____| |      |   | |____  |____ |
                |      |   \_ |    | |____  |   |  ____| |____ |____
                                 www.practisec.com

                      [recon-ng v5.1.2, Tim Tomes (@lanmaster53)]
```

```
[95] Recon modules
[8]  Reporting modules
[4]  Import modules
[3]  Disabled modules
[2]  Exploitation modules
[2]  Discovery modules

[recon-ng][default] > help

Commands (type [help|?] <topic>):
---------------------------------
back            Exits the current context
dashboard       Displays a summary of activity
db              Interfaces with the workspace's database
exit            Exits the framework
help            Displays this menu
index           Creates a module index (dev only)
keys            Manages third party resource credentials
marketplace     Interfaces with the module marketplace
modules         Interfaces with installed modules
options         Manages the current context options
pdb             Starts a Python Debugger session (dev only)
script          Records and executes command scripts
shell           Executes shell commands
show            Shows various framework items
snapshots       Manages workspace snapshots
spool           Spools output to a file
workspaces      Manages workspaces

[recon-ng][default] > show
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|
netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > marketplace refresh
[*] Marketplace index refreshed.
[recon-ng][default] > marketplace install all
[*] Module installed: discovery/info_disclosure/cache_snoop
```

```
[*] Module installed: discovery/info_disclosure/interesting_files
[*] Module installed: exploitation/injection/command_injector
[*] Module installed: exploitation/injection/xpath_bruter
[*] Module installed: import/csv_file
[*] Module installed: import/list
[*] Module installed: import/masscan
[*] Module installed: import/nmap
[*] Module installed: recon/companies-contacts/bing_linkedin_cache
[*] Module installed: recon/companies-contacts/censys_email_address
[*] Module installed: recon/companies-contacts/pen
[*] Module installed: recon/companies-domains/censys_subdomains
[*] Module installed: recon/companies-domains/pen
[*] Module installed: recon/companies-domains/viewdns_reverse_whois
[*] Module installed: recon/companies-domains/whoxy_dns
[*] Module installed: recon/companies-hosts/censys_org
[*] Module installed: recon/companies-hosts/censys_tls_subjects
[*] Module installed: recon/companies-multi/github_miner
[*] Module installed: recon/companies-multi/shodan_org
[*] Module installed: recon/companies-multi/whois_miner
[*] Module installed: recon/contacts-contacts/abc
[*] Module installed: recon/contacts-contacts/mailtester
[*] Module installed: recon/contacts-contacts/mangle
[*] Module installed: recon/contacts-contacts/unmangle
[*] Module installed: recon/contacts-credentials/hibp_breach
[*] Module installed: recon/contacts-credentials/hibp_paste
[*] Module installed: recon/contacts-domains/migrate_contacts
[*] Module installed: recon/contacts-profiles/fullcontact
[*] Module installed: recon/credentials-credentials/adobe
[*] Module installed: recon/credentials-credentials/bozocrack
[*] Module installed: recon/credentials-credentials/hashes_org
[*] Module installed: recon/domains-companies/censys_companies
[*] Module installed: recon/domains-companies/pen
[*] Module installed: recon/domains-companies/whoxy_whois
[*] Module installed: recon/domains-contacts/hunter_io
[*] Module installed: recon/domains-contacts/metacrawler
[*] Module installed: recon/domains-contacts/pen
[*] Module installed: recon/domains-contacts/pgp_search
[*] Module installed: recon/domains-contacts/whois_pocs
[*] Module installed: recon/domains-contacts/wikileaker
```

```
[*] Module installed: recon/domains-credentials/pwnedlist/account_creds
[*] Module installed: recon/domains-credentials/pwnedlist/api_usage
[*] Module installed: recon/domains-credentials/pwnedlist/domain_creds
[*] Module installed: recon/domains-credentials/pwnedlist/domain_ispwned
[*] Module installed: recon/domains-credentials/pwnedlist/leak_lookup
[*] Module installed: recon/domains-credentials/pwnedlist/leaks_dump
[*] Module installed: recon/domains-domains/brute_suffix
[*] Module installed: recon/domains-hosts/binaryedge
[*] Module installed: recon/domains-hosts/bing_domain_api
[*] Module installed: recon/domains-hosts/bing_domain_web
[*] Module installed: recon/domains-hosts/brute_hosts
[*] Module installed: recon/domains-hosts/builtwith
[*] Module installed: recon/domains-hosts/censys_domain
[*] Module installed: recon/domains-hosts/certificate_transparency
[*] Module installed: recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/hackertarget
[*] Module installed: recon/domains-hosts/mx_spf_ip
[*] Module installed: recon/domains-hosts/netcraft
[*] Module installed: recon/domains-hosts/shodan_hostname
[*] Module installed: recon/domains-hosts/spyse_subdomains
[*] Module installed: recon/domains-hosts/ssl_san
[*] Module installed: recon/domains-hosts/threatcrowd
[*] Module installed: recon/domains-hosts/threatminer
[*] Module installed: recon/domains-vulnerabilities/ghdb
[*] Module installed: recon/domains-vulnerabilities/xssed
[*] Module installed: recon/hosts-domains/migrate_hosts
[*] Module installed: recon/hosts-hosts/bing_ip
[*] Module installed: recon/hosts-hosts/censys_hostname
[*] Module installed: recon/hosts-hosts/censys_ip
[*] Module installed: recon/hosts-hosts/censys_query
[*] Module installed: recon/hosts-hosts/ipinfodb
[*] Module installed: recon/hosts-hosts/ipstack
[*] Module installed: recon/hosts-hosts/resolve
[*] Module installed: recon/hosts-hosts/reverse_resolve
[*] Module installed: recon/hosts-hosts/ssltools
[*] Module installed: recon/hosts-hosts/virustotal
[*] Module installed: recon/hosts-locations/migrate_hosts
[*] Module installed: recon/hosts-ports/binaryedge
[*] Module installed: recon/hosts-ports/shodan_ip
```

```
[*] Module installed: recon/locations-locations/geocode
[*] Module installed: recon/locations-locations/reverse_geocode
[*] Module installed: recon/locations-pushpins/flickr
[*] Module installed: recon/locations-pushpins/shodan
[*] Module installed: recon/locations-pushpins/twitter
[*] Module installed: recon/locations-pushpins/youtube
[*] Module installed: recon/netblocks-companies/censys_netblock_company
[*] Module installed: recon/netblocks-companies/whois_orgs
[*] Module installed: recon/netblocks-hosts/censys_netblock
[*] Module installed: recon/netblocks-hosts/reverse_resolve
[*] Module installed: recon/netblocks-hosts/shodan_net
[*] Module installed: recon/netblocks-hosts/virustotal
[*] Module installed: recon/netblocks-ports/census_2012
[*] Module installed: recon/netblocks-ports/censysio
[*] Module installed: recon/ports-hosts/migrate_ports
[*] Module installed: recon/ports-hosts/ssl_scan
[*] Module installed: recon/profiles-contacts/bing_linkedin_contacts
[*] Module installed: recon/profiles-contacts/dev_diver
[*] Module installed: recon/profiles-contacts/github_users
[*] Module installed: recon/profiles-profiles/namechk
[*] Module installed: recon/profiles-profiles/profiler
[*] Module installed: recon/profiles-profiles/twitter_mentioned
[*] Module installed: recon/profiles-profiles/twitter_mentions
[*] Module installed: recon/profiles-repositories/github_repos
[*] Module installed: recon/repositories-profiles/github_commits
[*] Module installed: recon/repositories-vulnerabilities/gists_search
[*] Module installed: recon/repositories-vulnerabilities/github_dorks
[*] Module installed: reporting/csv
[*] Module installed: reporting/html
[*] Module installed: reporting/json
[*] Module installed: reporting/list
[*] Module installed: reporting/proxifier
[*] Module installed: reporting/pushpin
[*] Module installed: reporting/xlsx
[*] Module installed: reporting/xml
[*] Reloading modules...

[recon-ng][default] > marketplace search hackertarget
[*] Searching module index for 'hackertarget'...
```

```
  +-------------------------------------------------------------------------+
  |               Path               | Version |   Status  |  Updated   |D|K|
  +-------------------------------------------------------------------------+
  | recon/domains-hosts/hackertarget | 1.1     | installed | 2020-05-17 | | |
  +-------------------------------------------------------------------------+

  D = Has dependencies. See info for details.
  K = Requires keys. See info for details.

[recon-ng][default][hackertarget] > modules load recon/domains-hosts/
                                    hackertarget
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table
  with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  default        yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] > options set SOURCE nike.com
SOURCE => nike.com
[recon-ng][default][hackertarget] > info

      Name: HackerTarget Lookup
    Author: Michael Henriksen (@michenriksen)
```

```
   Version: 1.1

Description:
  Uses the HackerTarget.com API to find host names. Updates the 'hosts' table
  with the results.

Options:
  Name    Current Value  Required  Description
  ------  -------------  --------  -----------
  SOURCE  nike.com       yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

[recon-ng][default][hackertarget] > run

--------
NIKE.COM
--------
[*] Country: None
[*] Host: nike.com
[*] Ip_Address: 13.249.85.128
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
[*] Host: nke-win-epo-p10.nike.com
[*] Ip_Address: 146.197.27.27
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -------------------------------------------------
[*] Country: None
```

```
[*] Host: nkehkgf20.nike.com
[*] Ip_Address: 202.130.133.174
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkebosf20.nike.com
[*] Ip_Address: 146.197.250.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkehlvf20.nike.com
[*] Ip_Address: 156.37.253.120
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nnqwhqcf30.nike.com
[*] Ip_Address: 146.197.246.71
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ss-440.nike.com
[*] Ip_Address: 146.197.184.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: ss-450.nike.com
[*] Ip_Address: 146.197.176.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-242-1.nike.com
[*] Ip_Address: 146.197.242.95
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-243-1.nike.com
[*] Ip_Address: 146.197.243.95
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-027-1.nike.com
[*] Ip_Address: 146.197.27.95
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nxp-con-1.nike.com
[*] Ip_Address: 146.197.27.102
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: retailjim-na01.nike.com
[*] Ip_Address: 146.197.185.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: usaweb01.nike.com
[*] Ip_Address: 146.197.61.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cambwd01.nike.com
[*] Ip_Address: 146.197.3.119
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: navaexpe01.nike.com
[*] Ip_Address: 146.197.44.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nasjcexpe01.nike.com
[*] Ip_Address: 146.197.46.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cvnahqbosexpe01.nike.com
[*] Ip_Address: 146.197.250.225
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikehkdcvcse01.nike.com
[*] Ip_Address: 202.130.133.178
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkecmaf01.nike.com
[*] Ip_Address: 209.150.75.68
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkapshanhubbf01.nike.com
[*] Ip_Address: 221.181.84.20
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkapbjsnhubbf01.nike.com
[*] Ip_Address: 223.71.122.84
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkepaif01.nike.com
[*] Ip_Address: 200.55.199.162
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkeolif01.nike.com
[*] Ip_Address: 181.30.174.134
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkegdlf01.nike.com
[*] Ip_Address: 189.211.127.28
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nlgsaopf01.nike.com
[*] Ip_Address: 146.197.16.38
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkebrrf01.nike.com
[*] Ip_Address: 146.197.16.38
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: csg01.nike.com
[*] Ip_Address: 146.197.27.22
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nke-win-dsm-p01.nike.com
[*] Ip_Address: 146.197.27.179
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nke-win-tms-p01.nike.com
[*] Ip_Address: 146.197.27.188
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap01.nike.com
[*] Ip_Address: 146.197.20.155
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camwrs01.nike.com
[*] Ip_Address: 146.197.1.50
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cambws01.nike.com
[*] Ip_Address: 146.197.3.50
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: retailjss-na-ext01.nike.com
[*] Ip_Address: 146.197.185.216
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cmext01.nike.com
[*] Ip_Address: 146.197.27.217
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jssext01.nike.com
[*] Ip_Address: 146.197.27.125
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap11.nike.com
```

```
[*] Ip_Address: 146.197.3.117
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nngashbf21.nike.com
[*] Ip_Address: 146.197.53.234
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barriera241.nike.com
[*] Ip_Address: 146.197.246.30
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barrierb241.nike.com
[*] Ip_Address: 146.197.27.90
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nbarrierc241.nike.com
[*] Ip_Address: 146.197.27.16
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: barriere241.nike.com
[*] Ip_Address: 146.197.27.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barrierl241.nike.com
[*] Ip_Address: 146.197.27.90
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barrierm241.nike.com
[*] Ip_Address: 146.197.27.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barriern241.nike.com
[*] Ip_Address: 146.197.27.91
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barrier241.nike.com
[*] Ip_Address: 146.197.27.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: camsap51.nike.com
[*] Ip_Address: 146.197.251.139
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: sineusp1abomaa1.nike.com
[*] Ip_Address: 156.53.224.77
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-c1.nike.com
[*] Ip_Address: 205.251.196.213
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: limapsd1.nike.com
[*] Ip_Address: 146.197.27.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: splashpage1.nike.com
[*] Ip_Address: 146.197.27.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-search1.nike.com
[*] Ip_Address: 146.197.184.26
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-n1.nike.com
[*] Ip_Address: 205.251.197.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikemacdmzdp1.nike.com
[*] Ip_Address: 146.197.27.177
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: longnsp1aexprep1.nike.com
[*] Ip_Address: 156.37.224.73
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: fragnsp1aexprp1.nike.com
[*] Ip_Address: 156.37.232.73
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camptaq1.nike.com
[*] Ip_Address: 146.197.3.85
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: campteq1.nike.com
[*] Ip_Address: 146.197.251.133
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-r1.nike.com
[*] Ip_Address: 205.251.196.46
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: longnsp1aexpres1.nike.com
[*] Ip_Address: 156.37.224.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-v1.nike.com
[*] Ip_Address: 205.251.197.62
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: www1.nike.com
[*] Ip_Address: 209.118.185.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-242-2.nike.com
[*] Ip_Address: 146.197.242.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-243-2.nike.com
[*] Ip_Address: 146.197.243.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-027-2.nike.com
[*] Ip_Address: 146.197.27.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nspwechat-uat-2.nike.com
[*] Ip_Address: 47.103.21.208
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: sinnetp1aexpe002.nike.com
[*] Ip_Address: 156.53.224.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: usaweb02.nike.com
[*] Ip_Address: 146.197.61.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: navaexpe02.nike.com
[*] Ip_Address: 146.197.44.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nasjcexpe02.nike.com
[*] Ip_Address: 146.197.46.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cvnahqbosexpe02.nike.com
[*] Ip_Address: 146.197.250.226
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkeabof02.nike.com
[*] Ip_Address: 203.49.111.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nke-win-dsm-p02.nike.com
[*] Ip_Address: 146.197.27.178
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap12.nike.com
[*] Ip_Address: 146.197.3.118
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nngashbf22.nike.com
[*] Ip_Address: 146.197.53.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap22.nike.com
```

```
[*] Ip_Address: 146.197.3.248
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap52.nike.com
[*] Ip_Address: 146.197.251.145
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: int-osb8-v-qa2.nike.com
[*] Ip_Address: 146.197.65.215
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: smtp-ex1-va2.nike.com
[*] Ip_Address: 146.197.185.243
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: smtp-ex2-va2.nike.com
[*] Ip_Address: 146.197.185.244
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: ns-c2.nike.com
[*] Ip_Address: 205.251.198.95
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: wechat-origin.gc2.nike.com
[*] Ip_Address: 13.251.168.148
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mp-admin.gc2.nike.com
[*] Ip_Address: 99.86.229.75
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: limapsd2.nike.com
[*] Ip_Address: 146.197.27.26
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-search2.nike.com
[*] Ip_Address: 146.197.184.26
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: ns-n2.nike.com
[*] Ip_Address: 205.251.198.251
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: teamcenterapp2.nike.com
[*] Ip_Address: 10.238.244.107
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: fragnsp1aexprp2.nike.com
[*] Ip_Address: 156.37.232.74
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-r2.nike.com
[*] Ip_Address: 205.251.199.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nspwechat2.nike.com
[*] Ip_Address: 47.101.17.239
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-v2.nike.com
[*] Ip_Address: 205.251.199.216
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: www2.nike.com
[*] Ip_Address: 209.118.185.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-242-3.nike.com
[*] Ip_Address: 146.197.242.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-243-3.nike.com
[*] Ip_Address: 146.197.243.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eai-027-3.nike.com
[*] Ip_Address: 146.197.27.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: navaexpe03.nike.com
[*] Ip_Address: 146.197.44.212
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nasjcexpe03.nike.com
[*] Ip_Address: 146.197.46.212
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkaumelsmocf03.nike.com
[*] Ip_Address: 203.39.203.102
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nngashbf23.nike.com
[*] Ip_Address: 146.197.53.236
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jumpman23.nike.com
[*] Ip_Address: 99.86.229.126
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap23.nike.com
[*] Ip_Address: 146.197.3.247
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-c3.nike.com
[*] Ip_Address: 205.251.192.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-n3.nike.com
[*] Ip_Address: 205.251.192.219
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-r3.nike.com
[*] Ip_Address: 205.251.193.111
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-v3.nike.com
[*] Ip_Address: 205.251.192.45
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nngashbf24.nike.com
[*] Ip_Address: 146.197.53.237
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap24.nike.com
[*] Ip_Address: 146.197.3.246
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap54.nike.com
[*] Ip_Address: 146.197.251.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-c4.nike.com
[*] Ip_Address: 205.251.195.139
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-n4.nike.com
[*] Ip_Address: 205.251.195.67
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-r4.nike.com
[*] Ip_Address: 205.251.194.99
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns-v4.nike.com
[*] Ip_Address: 205.251.194.154
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkeufragwanbf05.nike.com
[*] Ip_Address: 156.37.232.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: neglondf05.nike.com
[*] Ip_Address: 156.37.224.41
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: negfranf05.nike.com
```

```
[*] Ip_Address: 156.37.232.40
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: neqhilvf05.nike.com
[*] Ip_Address: 156.37.253.125
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap25.nike.com
[*] Ip_Address: 146.197.3.245
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ns5.nike.com
[*] Ip_Address: 146.197.187.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: neglondf06.nike.com
[*] Ip_Address: 156.37.224.42
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: negfranf06.nike.com
[*] Ip_Address: 156.37.232.41
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: neqhilvf06.nike.com
[*] Ip_Address: 156.37.253.124
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap26.nike.com
[*] Ip_Address: 146.197.3.244
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barrierz156.nike.com
[*] Ip_Address: 202.130.133.130
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap56.nike.com
[*] Ip_Address: 146.197.251.179
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: api-tie6.nike.com
[*] Ip_Address: 50.18.73.185
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkeulongwanbf07.nike.com
[*] Ip_Address: 156.37.224.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nagtkyof07.nike.com
[*] Ip_Address: 156.53.232.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: neqhilvf07.nike.com
[*] Ip_Address: 156.37.253.123
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: camsap27.nike.com
[*] Ip_Address: 146.197.3.243
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: neqhilvf08.nike.com
[*] Ip_Address: 156.37.253.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkewhqmhf28.nike.com
[*] Ip_Address: 146.197.246.73
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkewhqmsf28.nike.com
[*] Ip_Address: 146.197.246.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nke-win-epo-p09.nike.com
[*] Ip_Address: 146.197.27.73
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nkesaiob-f19.nike.com
[*] Ip_Address: 58.247.50.68
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: nkesaicc-f19.nike.com
[*] Ip_Address: 210.13.75.188
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: nkehkgf19.nike.com
[*] Ip_Address: 202.130.133.170
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: nkememf19.nike.com
[*] Ip_Address: 4.14.92.130
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: nkebosf19.nike.com
[*] Ip_Address: 146.197.250.13
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: nkehlvf19.nike.com
[*] Ip_Address: 156.37.253.125
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nnqwhqcf29.nike.com
[*] Ip_Address: 146.197.246.70
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: hk-eusp1abomaaa.nike.com
[*] Ip_Address: 202.130.133.177
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: euheusp5abomeaa.nike.com
[*] Ip_Address: 156.37.253.32
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: usheusp2abomuaa.nike.com
[*] Ip_Address: 146.197.27.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: support-en-ca.nike.com
[*] Ip_Address: 99.86.229.5
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: support-fr-ca.nike.com
[*] Ip_Address: 99.86.229.127
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: northamerica.nike.com
[*] Ip_Address: 40.80.155.102
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: da.nike.com
[*] Ip_Address: 146.197.242.30
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ada.nike.com
[*] Ip_Address: 99.84.108.117
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: emea.nike.com
[*] Ip_Address: 52.174.193.210
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: help-es-la.nike.com
[*] Ip_Address: 99.86.229.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: support-es-la.nike.com
[*] Ip_Address: 99.86.229.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: remotesupport-tnode-na.nike.com
[*] Ip_Address: 20.109.187.200
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: awrelayuat-na.nike.com
[*] Ip_Address: 146.197.61.88
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: awrelayuat-rt-na.nike.com
```

```
[*] Ip_Address: 146.197.61.92
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: awrelay-na.nike.com
[*] Ip_Address: 146.197.61.52
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dna.nike.com
[*] Ip_Address: 52.42.173.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: qa.dna.nike.com
[*] Ip_Address: 35.82.236.117
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: hasura.dna.nike.com
[*] Ip_Address: 52.42.173.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: staging.dna.nike.com
[*] Ip_Address: 52.42.173.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: develop.dna.nike.com
[*] Ip_Address: 35.82.236.117
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: cms.dna.nike.com
[*] Ip_Address: 52.42.173.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-secure-china.nike.com
[*] Ip_Address: 146.197.181.6
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-drprd-secure-china.nike.com
[*] Ip_Address: 146.197.181.6
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: origin-secure-china.nike.com
[*] Ip_Address: 66.54.56.6
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vdi-china.nike.com
[*] Ip_Address: 117.184.132.32
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: csr-china.nike.com
[*] Ip_Address: 66.54.56.6
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-csr-china.nike.com
[*] Ip_Address: 146.197.181.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: privateappschina.nike.com
[*] Ip_Address: 18.160.46.113
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: bk.privateappschina.nike.com
[*] Ip_Address: 99.84.208.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: zodiac-qa.nike.com
[*] Ip_Address: 35.231.232.180
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nisc-qa.nike.com
[*] Ip_Address: 52.159.174.129
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: bnxsend-qa.nike.com
[*] Ip_Address: 146.197.179.238
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: thehud-qa.nike.com
[*] Ip_Address: 100.26.57.182
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: boe-qa.nike.com
[*] Ip_Address: 146.197.179.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: digitalportal-qa.nike.com
[*] Ip_Address: 66.54.18.203
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: zero-qa.nike.com
[*] Ip_Address: 99.84.208.111
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: slides.zero-qa.nike.com
[*] Ip_Address: 10.239.90.28
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: plm-app-qa.nike.com
[*] Ip_Address: 168.62.168.203
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: poq-qa.nike.com
[*] Ip_Address: 146.197.65.112
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: locker-qa.nike.com
[*] Ip_Address: 146.197.64.209
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: boe-redirect-qa.nike.com
[*] Ip_Address: 146.197.179.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mft-qa.nike.com
[*] Ip_Address: 146.197.27.192
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: emft-qa.nike.com
[*] Ip_Address: 146.197.27.181
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: brandapi-ext-qa.nike.com
[*] Ip_Address: 146.197.179.236
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: int-osb2-v-qa.nike.com
[*] Ip_Address: 146.197.64.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: int-osb3-v-qa.nike.com
[*] Ip_Address: 146.197.64.231
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rv-qa.nike.com
[*] Ip_Address: 146.197.179.227
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: plm-ftw-qa.nike.com
[*] Ip_Address: 40.76.28.12
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rtuscorpserviceslbqa.nike.com
[*] Ip_Address: 146.197.65.125
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: maximsqa.nike.com
[*] Ip_Address: 23.101.207.250
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-conbizextqa.nike.com
[*] Ip_Address: 20.99.137.175
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: whqlabasa.nike.com
[*] Ip_Address: 146.197.246.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: api-gsm-vendordelta.nike.com
```

```
[*] Ip_Address: 40.112.177.204
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-elcweb-ua.nike.com
[*] Ip_Address: 156.37.224.141
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-elc-primetime-ua.nike.com
[*] Ip_Address: 156.37.224.137
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: zebraconnectva.nike.com
[*] Ip_Address: 146.197.185.222
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: towa.nike.com
[*] Ip_Address: 146.197.27.60
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: vsplab.nike.com
[*] Ip_Address: 146.197.27.109
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: elcweb.nike.com
[*] Ip_Address: 156.37.224.135
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-elcweb.nike.com
[*] Ip_Address: 156.37.224.140
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: euroweb.nike.com
[*] Ip_Address: 156.37.253.45
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: panoramaphotoweb.nike.com
[*] Ip_Address: 156.53.224.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: cssweb.nike.com
[*] Ip_Address: 146.197.27.48
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: sfb.nike.com
[*] Ip_Address: 156.37.253.88
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ballersfb.nike.com
[*] Ip_Address: 206.188.27.82
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: help-en-gb.nike.com
[*] Ip_Address: 18.160.46.93
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: support-en-gb.nike.com
[*] Ip_Address: 99.86.229.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: rtuscorpserviceslb.nike.com
[*] Ip_Address: 146.197.65.126
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: barb.nike.com
[*] Ip_Address: 146.197.27.17
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: digihub.nike.com
[*] Ip_Address: 146.197.184.248
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gbmhub.nike.com
[*] Ip_Address: 99.86.229.126
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gsmhub.nike.com
[*] Ip_Address: 52.25.204.60
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: teamcity1.b2c.nike.com
[*] Ip_Address: 10.11.55.229
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jira-p-00.va2.b2c.nike.com
[*] Ip_Address: 10.12.111.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: confluence-p-00.va2.b2c.nike.com
[*] Ip_Address: 10.12.111.29
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ip-10-12-111-251.va2.b2c.nike.com
[*] Ip_Address: 10.12.111.251
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: smtp-ex1.va2.b2c.nike.com
[*] Ip_Address: 146.197.185.243
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: smtp-ex2.va2.b2c.nike.com
[*] Ip_Address: 146.197.185.244
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: teamcity2.b2c.nike.com
[*] Ip_Address: 10.11.55.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jira.b2c.nike.com
[*] Ip_Address: 10.11.55.225
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jenkins-oc.b2c.nike.com
[*] Ip_Address: 10.11.55.231
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: crowd.b2c.nike.com
[*] Ip_Address: 10.11.55.222
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: confluence.b2c.nike.com
[*] Ip_Address: 10.11.55.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: fisheye.b2c.nike.com
[*] Ip_Address: 10.11.55.223
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: artifactoryha-p-sj-1.sj.b2c.nike.com
[*] Ip_Address: 10.11.56.17
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ip-10-11-47-164.sj.b2c.nike.com
[*] Ip_Address: 10.11.47.164
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: svn.b2c.nike.com
[*] Ip_Address: 10.11.55.228
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: svnrepo.b2c.nike.com
[*] Ip_Address: 10.11.55.228
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jira-np.b2c.nike.com
[*] Ip_Address: 10.12.191.186
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: sonar.b2c.nike.com
[*] Ip_Address: 10.11.55.226
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jenkins.b2c.nike.com
[*] Ip_Address: 10.11.55.224
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: bitbucket.b2c.nike.com
```

```
[*] Ip_Address: 10.11.55.227
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: bb-ext.b2c.nike.com
[*] Ip_Address: 146.197.186.242
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jira-np-ext.b2c.nike.com
[*] Ip_Address: 146.197.178.254
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: wac.nike.com
[*] Ip_Address: 156.37.253.87
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nasbc.nike.com
[*] Ip_Address: 146.197.46.200
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: nwdc.nike.com
[*] Ip_Address: 146.197.27.159
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eemnwdc.nike.com
[*] Ip_Address: 146.197.27.204
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eemtestnwdc.nike.com
[*] Ip_Address: 146.197.27.147
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: conbizdevnwdc.nike.com
[*] Ip_Address: 146.197.27.148
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: conbiznwdc.nike.com
[*] Ip_Address: 146.197.27.175
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: winmagic.nike.com
[*] Ip_Address: 146.197.27.170
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vdi-elc.nike.com
[*] Ip_Address: 156.37.224.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: myelc.nike.com
[*] Ip_Address: 99.86.229.126
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: jenkins-oc.nike.com
[*] Ip_Address: 146.197.186.237
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: crashplanpoc.nike.com
[*] Ip_Address: 146.197.27.70
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: qc.nike.com
[*] Ip_Address: 146.197.27.168
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nisc.nike.com
[*] Ip_Address: 52.159.174.129
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: wmbsvc.nike.com
[*] Ip_Address: 146.197.27.36
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: scinyc.nike.com
[*] Ip_Address: 35.193.143.29
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lead.nike.com
[*] Ip_Address: 99.86.229.111
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-nikeplus-upload.nike.com
[*] Ip_Address: 146.197.184.19
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: whqdfed.nike.com
[*] Ip_Address: 146.197.27.112
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: whqpfed.nike.com
[*] Ip_Address: 146.197.27.114
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-nikeid.nike.com
[*] Ip_Address: 146.197.181.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-drprd-nikeid.nike.com
[*] Ip_Address: 146.197.181.10
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-secure-nikeid.nike.com
[*] Ip_Address: 146.197.181.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-secure-nikeid.nike.com
[*] Ip_Address: 146.197.184.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-secure-nikeid.nike.com
[*] Ip_Address: 156.37.192.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-nikeid.nike.com
[*] Ip_Address: 146.197.184.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: preview-nikeid.nike.com
[*] Ip_Address: 66.54.56.131
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-nikeid.nike.com
[*] Ip_Address: 156.37.192.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: p7wweb90001.outfield.nike.com
[*] Ip_Address: 13.67.88.37
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gameonworld.nike.com
[*] Ip_Address: 99.86.229.111
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: umd.nike.com
[*] Ip_Address: 10.238.105.136
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-secure-api-backend.nike.com
[*] Ip_Address: 146.197.184.20
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: stg-api-backend.nike.com
[*] Ip_Address: 66.54.57.184
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-api-backend.nike.com
[*] Ip_Address: 146.197.184.20
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: bnxsend.nike.com
[*] Ip_Address: 146.197.184.253
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: find.nike.com
[*] Ip_Address: 99.86.229.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dev.find.nike.com
```

```
[*] Ip_Address: 99.86.229.26
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: behind.nike.com
[*] Ip_Address: 99.84.208.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: n7fund.nike.com
[*] Ip_Address: 18.160.10.47
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: securid-prod.nike.com
[*] Ip_Address: 146.197.27.163
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dna.pes-prod.nike.com
[*] Ip_Address: 10.178.137.82
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: gsm-dpe-prodtrack-prod.pes-prod.nike.com
[*] Ip_Address: 99.86.229.111
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gsm-capviz-client-prod.pes-prod.nike.com
[*] Ip_Address: 99.84.108.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: parc-nginx-proxy-lib-s-ext-prod.pes-prod.nike.com
[*] Ip_Address: 44.240.49.1
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: prod-parc-app-dashboard.pes-prod.nike.com
[*] Ip_Address: 52.12.181.114
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rsltesting.pes-prod.nike.com
[*] Ip_Address: 52.85.132.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: productlineplan-api.pes-prod.nike.com
[*] Ip_Address: 18.155.181.51
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dataloader-api.pes-prod.nike.com
[*] Ip_Address: 54.213.82.0
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-tfob-ui.pes-prod.nike.com
[*] Ip_Address: 54.148.111.53
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-fobc-ui.pes-prod.nike.com
[*] Ip_Address: 35.163.44.84
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: prod-parc-cbd-ui.pes-prod.nike.com
[*] Ip_Address: 52.39.155.66
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dataloader-prod-ui.pes-prod.nike.com
[*] Ip_Address: 54.214.85.230
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-materialprice-ui.pes-prod.nike.com
[*] Ip_Address: 35.160.115.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: prod-parc-library-sharing-ui.pes-prod.nike.com
[*] Ip_Address: 54.200.231.27
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-bombol-ui.pes-prod.nike.com
[*] Ip_Address: 35.81.21.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: prod-parc-material-lab-form-ui.pes-prod.nike.com
[*] Ip_Address: 44.237.99.66
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-coststandards-ui.pes-prod.nike.com
[*] Ip_Address: 54.186.137.148
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: prod-parc-colorway-status-ui.pes-prod.nike.com
[*] Ip_Address: 52.35.249.206
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-quotemanagement-ui.pes-prod.nike.com
[*] Ip_Address: 52.42.47.164
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-nby-ui.pes-prod.nike.com
[*] Ip_Address: 35.163.204.155
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: spil.pes-prod.nike.com
[*] Ip_Address: 54.184.45.233
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: productlineplan-adapter.pes-prod.nike.com
[*] Ip_Address: 143.204.146.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-psm-server.pes-prod.nike.com
[*] Ip_Address: 10.179.25.113
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lpm-nikebyyou-server.pes-prod.nike.com
[*] Ip_Address: 52.39.23.206
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: api.internal.zoom.k8s.pes-prod.nike.com
[*] Ip_Address: 10.178.231.206
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: av-services.pes-prod.nike.com
[*] Ip_Address: 10.178.227.104
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: zebrazombie-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.208.37
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: globalsourcing-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.108.40
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lastengineering-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.86.229.84
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: materialtesting-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.108.63
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: costing-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 52.85.132.57
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: linemanagement-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.108.85
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: materialmanagement-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 52.85.132.55
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vendormanagement-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.108.46
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: colormanagement-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 52.85.132.44
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: materialdevelopment-internal.api-product.pes-prod.nike.com
```

```
[*] Ip_Address: 52.85.132.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: productdevelopment-internal.api-product.pes-prod.nike.com
[*] Ip_Address: 99.84.208.35
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: spot.pes-prod.nike.com
[*] Ip_Address: 99.86.229.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lpm-nikebyyou.pes-prod.nike.com
[*] Ip_Address: 99.84.108.35
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: praprod.nike.com
[*] Ip_Address: 146.197.1.43
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: aunikestoreprod.nike.com
[*] Ip_Address: 146.197.27.218
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-team20.pes-preprod.nike.com
[*] Ip_Address: 10.179.5.99
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-localdev13.pes-preprod.nike.com
[*] Ip_Address: 10.179.6.165
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-lhaye5.pes-preprod.nike.com
[*] Ip_Address: 10.179.5.69
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-team06.pes-preprod.nike.com
[*] Ip_Address: 10.179.8.24
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: ptc-pcx-team08.pes-preprod.nike.com
[*] Ip_Address: 10.179.9.52
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-localdev08.pes-preprod.nike.com
[*] Ip_Address: 10.179.5.112
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-localdev09.pes-preprod.nike.com
[*] Ip_Address: 10.179.6.71
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ptc-pcx-configa.pes-preprod.nike.com
[*] Ip_Address: 10.179.9.81
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: spil-qa.pes-preprod.nike.com
[*] Ip_Address: 52.42.54.48
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ---------------------------------------------------
[*] Country: None
[*] Host: productlineplan-mmx-inbound-adapter-qa.pes-preprod.nike.com
[*] Ip_Address: 99.86.229.67
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: dmc.pes-preprod.nike.com
[*] Ip_Address: 54.185.145.146
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: stg-parc-app-dashboard.pes-preprod.nike.com
[*] Ip_Address: 10.178.246.34
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: bizsim-parc-app-dashboard.pes-preprod.nike.com
[*] Ip_Address: 52.26.93.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: train-parc-app-dashboard.pes-preprod.nike.com
[*] Ip_Address: 52.34.16.25
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: dev-parc-app-dashboard.pes-preprod.nike.com
[*] Ip_Address: 52.10.98.192
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: gsm-dpe-prodtrack-stage.pes-preprod.nike.com
[*] Ip_Address: 99.86.229.119
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: gsm-capviz-client-stage.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.60
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: authentise.pes-preprod.nike.com
[*] Ip_Address: 10.178.146.246
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: dataloader-api-perf.pes-preprod.nike.com
[*] Ip_Address: 52.27.117.12
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rsltesting.pes-preprod.nike.com
[*] Ip_Address: 52.85.132.55
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dataloader-api-stg.pes-preprod.nike.com
[*] Ip_Address: 35.155.203.114
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-itemspec-sync-ui-stg.pes-preprod.nike.com
[*] Ip_Address: 52.85.132.119
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: productlineplan-mmx-inbound-adapter-stg.pes-preprod.nike.com
[*] Ip_Address: 18.165.98.39
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: productlineplan-stg-api.pes-preprod.nike.com
[*] Ip_Address: 13.226.39.70
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dataloader-stg-api.pes-preprod.nike.com
[*] Ip_Address: 34.214.143.240
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: hello-api.pes-preprod.nike.com
[*] Ip_Address: 54.201.38.125
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dataloader-api.pes-preprod.nike.com
[*] Ip_Address: 44.241.129.143
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: aesir-api.pes-preprod.nike.com
[*] Ip_Address: 44.238.26.195
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-tfob-ui.pes-preprod.nike.com
[*] Ip_Address: 52.32.75.231
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: sc-parc-cbd-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.245.168
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: devc-parc-cbd-ui.pes-preprod.nike.com
[*] Ip_Address: 52.35.60.23
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: bizsim-parc-cbd-ui.pes-preprod.nike.com
[*] Ip_Address: 35.164.191.118
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: train-parc-cbd-ui.pes-preprod.nike.com
[*] Ip_Address: 44.240.255.225
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: dev-parc-cbd-ui.pes-preprod.nike.com
```

```
[*] Ip_Address: 44.236.16.116
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-materialprice-ui.pes-preprod.nike.com
[*] Ip_Address: 52.26.206.106
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: train-parc-library-sharing-ui.pes-preprod.nike.com
[*] Ip_Address: 52.38.100.157
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dev-parc-library-sharing-ui.pes-preprod.nike.com
[*] Ip_Address: 52.11.59.133
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dataloader-stg-ui.pes-preprod.nike.com
[*] Ip_Address: 44.235.25.175
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: pcx-dla-bombol-ui.pes-preprod.nike.com
[*] Ip_Address: 35.82.176.165
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: stg-parc-material-lab-form-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.242.129
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: train-parc-material-lab-form-ui.pes-preprod.nike.com
[*] Ip_Address: 35.167.29.211
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dev-parc-material-lab-form-ui.pes-preprod.nike.com
[*] Ip_Address: 54.190.64.57
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-coststandards-ui.pes-preprod.nike.com
[*] Ip_Address: 35.155.196.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: sc-parc-colorway-status-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.245.253
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: stg-parc-colorway-status-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.245.253
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: train-parc-colorway-status-ui.pes-preprod.nike.com
[*] Ip_Address: 35.80.130.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dev-parc-colorway-status-ui.pes-preprod.nike.com
[*] Ip_Address: 44.230.184.175
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-quotemanagement-ui.pes-preprod.nike.com
[*] Ip_Address: 44.235.199.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: dev-amplify-mass-cbd-export-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.246.34
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-sensu-ui.pes-preprod.nike.com
[*] Ip_Address: 10.178.246.104
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dataloader-dev-ui.pes-preprod.nike.com
[*] Ip_Address: 54.212.147.201
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-dla-nby-ui.pes-preprod.nike.com
[*] Ip_Address: 50.112.159.218
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: capvis-api-non.pes-preprod.nike.com
[*] Ip_Address: 99.86.229.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: productlineplan-stg-adapter.pes-preprod.nike.com
[*] Ip_Address: 13.225.223.107
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: lpm-nikebyyou-server.pes-preprod.nike.com
[*] Ip_Address: 52.10.2.156
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: aesir.pes-preprod.nike.com
[*] Ip_Address: 52.27.210.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: aesir-api-eks.pes-preprod.nike.com
[*] Ip_Address: 10.178.247.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: api-dev.appps.pes-preprod.nike.com
[*] Ip_Address: 52.10.178.134
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: zebrazombie-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.115
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: globalsourcing-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 108.138.246.7
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lastengineering-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.92
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: materialtesting-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 52.85.132.55
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: costing-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.126
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: linemanagement-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.108.77
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: materialmanagement-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 52.85.132.92
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: vendormanagement-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.86.229.28
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: colormanagement-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.51
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------------
[*] Country: None
[*] Host: materialdevelopment-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.125
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: productdevelopment-internal.api-product.pes-preprod.nike.com
[*] Ip_Address: 99.84.108.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: chatbot.pes-preprod.nike.com
[*] Ip_Address: 35.82.8.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-securityapp-api-test.pes-preprod.nike.com
[*] Ip_Address: 99.84.108.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: aesir-api-test.pes-preprod.nike.com
[*] Ip_Address: 34.208.217.61
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: aesir-test.pes-preprod.nike.com
```

```
[*] Ip_Address: 10.178.247.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: parc-nginx-proxy-ext.pes-preprod.nike.com
[*] Ip_Address: 54.69.232.96
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: lpm-nikebyyou.pes-preprod.nike.com
[*] Ip_Address: 13.227.74.40
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-itemspec-sync-api-dev.pes-preprod.nike.com
[*] Ip_Address: 35.155.236.164
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gemini-bom-api-dev.pes-preprod.nike.com
[*] Ip_Address: 34.211.159.189
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: pcx-securityapp-api-dev.pes-preprod.nike.com
[*] Ip_Address: 18.155.202.99
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dataloader-api-dev.pes-preprod.nike.com
[*] Ip_Address: 52.27.95.51
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: aesir-api-dev.pes-preprod.nike.com
[*] Ip_Address: 10.178.247.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: capvis-api-dev.pes-preprod.nike.com
[*] Ip_Address: 99.84.108.21
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: dpe-uamaas-data-ingest-api-dev.pes-preprod.nike.com
[*] Ip_Address: 99.84.208.123
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: pcx-itemspec-sync-ui-dev.pes-preprod.nike.com
[*] Ip_Address: 99.84.108.118
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pcx-securityapp-dev.pes-preprod.nike.com
[*] Ip_Address: 18.164.96.13
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: aesir-dev.pes-preprod.nike.com
[*] Ip_Address: 10.178.247.97
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gsm-capviz-client-dev.pes-preprod.nike.com
[*] Ip_Address: 99.86.229.27
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: sapprod.nike.com
[*] Ip_Address: 146.197.3.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: giftcard.nike.com
[*] Ip_Address: 99.86.229.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: naquality.dashboard.nike.com
[*] Ip_Address: 10.230.78.228
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: pop-prd.nike.com
[*] Ip_Address: 146.197.64.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: emft-prd.nike.com
[*] Ip_Address: 146.197.27.183
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikeflow-prd.nike.com
[*] Ip_Address: 20.123.129.108
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vim-office.nike.com
[*] Ip_Address: 200.32.43.31
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: boxselfservice.nike.com
[*] Ip_Address: 13.66.244.249
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nvttecommerce.nike.com
[*] Ip_Address: 146.197.27.41
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: help-de-de.nike.com
[*] Ip_Address: 18.160.46.103
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: support-de-de.nike.com
[*] Ip_Address: 99.86.229.5
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: emea-code.nike.com
[*] Ip_Address: 52.236.156.93
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: profile-image.nike.com
[*] Ip_Address: 146.197.184.137
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-profile-image.nike.com
[*] Ip_Address: 146.197.184.137
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: stage.nike.com
[*] Ip_Address: 207.87.4.129
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: edge.nike.com
[*] Ip_Address: 146.197.27.215
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: naquality.intake.nike.com
[*] Ip_Address: 10.230.33.78
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: converse-employeesale.nike.com
[*] Ip_Address: 106.15.226.183
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: gcsamplesale.nike.com
[*] Ip_Address: 156.53.224.76
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: waffle.nike.com
[*] Ip_Address: 146.197.184.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-waffle.nike.com
[*] Ip_Address: 146.197.181.8
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-drprd-waffle.nike.com
[*] Ip_Address: 146.197.181.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-waffle.nike.com
[*] Ip_Address: 146.197.184.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-apps-waffle.nike.com
[*] Ip_Address: 146.197.184.72
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rtnawfmqamobile.nike.com
[*] Ip_Address: 146.197.27.222
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: rtnawfmappdevmobile.nike.com
```

```
[*] Ip_Address: 146.197.27.221
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: na-myschedule.nike.com
[*] Ip_Address: 146.197.27.86
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: freestyle.nike.com
[*] Ip_Address: 194.192.82.210
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-elc-primetime.nike.com
[*] Ip_Address: 156.37.224.136
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: callme.nike.com
[*] Ip_Address: 52.35.135.182
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: consume.nike.com
[*] Ip_Address: 99.84.208.107
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: octosquid.ap-southeast-1.consume.nike.com
[*] Ip_Address: 10.90.169.185
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: octosquid.consume.nike.com
[*] Ip_Address: 10.90.169.185
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: test.consume.nike.com
[*] Ip_Address: 99.84.108.108
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: iphone.nike.com
[*] Ip_Address: 146.197.27.173
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: devone.nike.com
[*] Ip_Address: 18.160.10.62
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: boe.nike.com
[*] Ip_Address: 146.197.184.249
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikeid-europe.nike.com
[*] Ip_Address: 194.192.82.253
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: api.prod.bre.nike.com
[*] Ip_Address: 54.243.125.102
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: status.api.prod.bre.nike.com
[*] Ip_Address: 34.205.123.133
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: api.preprod.bre.nike.com
[*] Ip_Address: 35.155.132.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: status.api.preprod.bre.nike.com
[*] Ip_Address: 34.225.163.198
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: status.api.dev.bre.nike.com
[*] Ip_Address: 52.25.44.127
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ss-ecn4-store.nike.com
[*] Ip_Address: 146.197.176.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-store.nike.com
[*] Ip_Address: 146.197.181.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-drprd-store.nike.com
[*] Ip_Address: 146.197.181.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-secure-store.nike.com
[*] Ip_Address: 146.197.181.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-drprd-secure-store.nike.com
[*] Ip_Address: 146.197.181.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-secure-store.nike.com
[*] Ip_Address: 146.197.184.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-secure-store.nike.com
[*] Ip_Address: 156.37.192.11
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-store.nike.com
[*] Ip_Address: 146.197.184.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: csr-store.nike.com
[*] Ip_Address: 146.197.184.9
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ecn25-csr-store.nike.com
[*] Ip_Address: 146.197.176.8
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: beta-csr-store.nike.com
[*] Ip_Address: 146.197.184.116
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: drprd-csr-store.nike.com
[*] Ip_Address: 146.197.181.9
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ext-csr-store.nike.com
[*] Ip_Address: 146.197.184.9
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: ss-store.nike.com
[*] Ip_Address: 146.197.184.150
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-store.nike.com
[*] Ip_Address: 156.37.192.11
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikefactorystore.nike.com
[*] Ip_Address: 18.155.202.53
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: www.nikefactorystore.nike.com
[*] Ip_Address: 52.85.132.42
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: secure.nike.com
[*] Ip_Address: 146.197.20.189
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vdi-azure.nike.com
[*] Ip_Address: 52.178.94.30
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: help-sv-se.nike.com
[*] Ip_Address: 18.160.46.113
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: staging01-app-purpose.nike.com
[*] Ip_Address: 54.191.242.203
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: staging01-cms-purpose.nike.com
```

```
[*] Ip_Address: 18.236.10.195
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: prod-cms-purpose.nike.com
[*] Ip_Address: 35.160.109.47
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-elite.nike.com
[*] Ip_Address: 156.37.192.16
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-secure-nikeelite.nike.com
[*] Ip_Address: 146.197.184.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-secure-nikeelite.nike.com
[*] Ip_Address: 156.37.192.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
```

```
[*] Host: origin-nikeelite.nike.com
[*] Ip_Address: 146.197.184.10
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-nikeelite.nike.com
[*] Ip_Address: 156.37.192.4
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mow-unite.nike.com
[*] Ip_Address: 156.37.192.15
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: vote.nike.com
[*] Ip_Address: 18.160.41.101
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: employeesvote.nike.com
[*] Ip_Address: 35.168.121.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
```

```
[*] Country: None
[*] Host: www.highfive.nike.com
[*] Ip_Address: 99.84.208.90
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: purpose-archive.nike.com
[*] Ip_Address: 99.84.108.60
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: 50thstories-archive.nike.com
[*] Ip_Address: 52.85.132.95
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: news-archive.nike.com
[*] Ip_Address: 99.86.229.17
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-nikeplusactive.nike.com
[*] Ip_Address: 146.197.184.19
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

```
[*] ------------------------------------------------
[*] Country: None
[*] Host: timeoff.nike.com
[*] Ip_Address: 99.84.108.82
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nikegolf.nike.com
[*] Ip_Address: 99.86.229.126
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: origin-nikegolf.nike.com
[*] Ip_Address: 99.86.229.88
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: webconf.nike.com
[*] Ip_Address: 156.37.253.84
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: eventurf.nike.com
[*] Ip_Address: 13.51.132.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
```

```
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: mag.nike.com
[*] Ip_Address: 146.197.27.234
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: seg.nike.com
[*] Ip_Address: 146.197.27.235
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: proxy.us-east-1.golang.nike.com
[*] Ip_Address: 10.235.9.218
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: proxy.ap-southeast-1.golang.nike.com
[*] Ip_Address: 10.90.169.176
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: proxy.eu-west-1.golang.nike.com
[*] Ip_Address: 10.34.241.174
[*] Latitude: None
[*] Longitude: None
```

```
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: proxy.golang.nike.com
[*] Ip_Address: 10.235.9.77
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: serenawilliamsbuilding.nike.com
[*] Ip_Address: 18.160.41.23
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: qa.serenawilliamsbuilding.nike.com
[*] Ip_Address: 99.84.208.18
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: staging.serenawilliamsbuilding.nike.com
[*] Ip_Address: 52.85.132.5
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ----------------------------------------------
[*] Country: None
[*] Host: dev.serenawilliamsbuilding.nike.com
[*] Ip_Address: 99.84.208.117
[*] Latitude: None
```

```
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: onboarding.nike.com
[*] Ip_Address: 99.86.229.122
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: brandingpackaging.nike.com
[*] Ip_Address: 54.69.241.17
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: nspwechat-uat-skywalking.nike.com
[*] Ip_Address: 47.103.21.208
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: running.nike.com
[*] Ip_Address: 99.86.229.2
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ------------------------------------------------
[*] Country: None
[*] Host: marketing.nike.com
[*] Ip_Address: 10.240.120.138
```

```
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------
[*] Country: None
[*] Host: thevan-sg.nike.com
[*] Ip_Address: 99.86.229.2
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] ---------------------------------------------------

-------
SUMMARY
-------
[*] 501 total (501 new) hosts found.
[recon-ng][default][hackertarget] >
```

Appendix D

Incident Management

D.1 Email Template for Customer to Initiate the Take-down Process

---

Subject: Urgent Action Required: Brand Protection Threat Identified

Dear [Customer's Name],

Hope this email finds you well.

We would like to draw your immediate attention to a critical brand protection issue that emerged during a Proof of Concept (POC) of our open-source solution - "Scamsweep", conducted for [insert Company Name].

Scamsweep identified a significant threat that poses a "insert risk rating, i.e., High or Medium" level of risk to your brand's integrity.
This threat involves [briefly describe the nature of the identified threat, e.g., unauthorized usage of registered trademarks, counterfeit products, false information, etc.].

Enclosed with this email, you will find the necessary documents, including the Risk Assessment Report and Incident Investigation Report.
Please review the documents carefully and kindly provide your signature below to signify your approval for immediate action:

[Insert Signature Box Here]

[Signature: _____]
[Date: _____]

Once we receive your approved signature, we will take the necessary steps to eliminate the threat and safeguard the interests of [insert Company Name].

Should you require any further information or have questions regarding this matter, please do not hesitate to reach out to us at [insert contact email/phone number].

Your proactive cooperation in addressing this issue is highly appreciated.

Thank you for your attention and support.

Sincerely,

[Your Name]
[Your Title/Position]
[Your Contact Information]