ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL SCIENCES



INVESTIGATING CYBER THREATS ON SOCIAL MEDIA USING MACHINE LEARNING

M.Sc. Thesis by

Emre ÇAMALAN

Department of Computer Engineering

September, 2019

ANKARA

INVESTIGATING CYBER THREATS ON SOCIAL MEDIA USING MACHINE LEARNING

A Thesis Submitted to

The Graduate School of Natural Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Computer Engineering, Department of Computer Engineering

by

Emre ÇAMALAN

September, 2019

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"INVESTIGATING CYBER THREATS ON SOCIAL MEDIA USING MACHINE LEARNING"** completed by **EMRE ÇAMALAN** under the supervision of **ASSIST. PROF. DR. AHMET ERCAN TOPCU** and we certify that in our opinion it is fully adequate, in scope and in quality, as a thesis for the degree of Master of Science.

Assist. Prof. Dr. Ahmet Ercan TOPCU

Supervisor

Asst. Prof. Mustafa YENİAD

Jury Member

Assoc. Prof. Dr. Hasan Şakir BİLGE

Jury Member

Prof. Dr. Ergün ERASLAN

Director

Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural Sciences,

- All data, information and documents are obtained in the framework of academic and ethical rules,
- All information, documents and assessments are presented in accordance with scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of above statements, I accept to renounce all my legal rights.

Date: **Signature:……..**

2019, 30 September **Name & Surname: Emre ÇAMALAN**

ACKNOWLEDGEMENTS

First, I would like to express my sincere gratitude to my supervisor, Dr. Ahmet Ercan Topcu, for his tremendous support, motivation and patience during my study. I was having a hard time during the initial phase of my research work but his trust and encouragement kept me going. His immense knowledge and valuable recommendations enabled the milestones of this study, and his guidance assisted me through all of my research and while writing this thesis.

I must also express my very profound gratitude to my wife, my son, my parents, and my sister for providing me with unfailing support and continuous encouragement throughout my years of study and through the process of researching and writing this thesis. This accomplishment would not have been possible without them. Thank you.

2019, 30 September **Emre ÇAMALAN**

INVESTIGATING CYBER THREATS ON SOCIAL MEDIA USING MACHINE LEARNING

ABSTRACT

Internet platforms are places where data can be found easily and communication is fast. Thus, in this information age, knowledge can be used as a dangerous weapon for terror attacks in the cyber world. Such an attack can threaten the systems of a company or sometimes even the safety of society. Besides protecting individuals and systems from such attacks, the attack risks must also be determined because an unknown threat cannot be precluded.

New threats such as malware, exploit, and fraud are often noticed too late. When these threats are first discovered, they are defined as zero-day; the weaknesses are then exploited due to the vulnerability of the computers and major damages arise. No manufacturer of security products such as IPS or IDS can succeed without fixing these risks immediately.

To address these issues, this thesis employs social media resources (i.e. Twitter) to identify these weaknesses as quickly as possible. The aim is to determine zero-day attacks by gathering information published by people who are not aware that they are facing a known zero-day attack. The study uses data from social media and processes the data by implementing machine learning principles such as word classification. As a result, a program is developed that identifies vulnerabilities and notifies the relevant manufacturers or vendors. In this way, it is possible for vendors to remove the vulnerabilities in a more efficient manner by identifying zero-day attacks via social media data.

In this thesis, a literature review has been undertaken to address the basic concepts of risk, security and social media, and a new-generation program has been developed for finding probable attacks that have been alluded to on social media.

Keywords: Internet, cyber security, machine learning, word classification, zero-day attack, Twitter, TensorFlow

MAKİNE ÖĞRENMESİ KULLANARAK SOSYAL MEDYA ÜZERİNDE SİBER TEHDİTLERİN ARAŞTIRILMASI

ÖZ

İnternet platformları verilerin kolayca bulunabileceği ve iletişimin hızlı olduğu yerlerdir. Böylece, bu bilgi çağında, bilgi siber dünyadaki terör saldırıları için tehlikeli bir silah olarak kullanılabilir. Böyle bir saldırı bir şirketin sistemlerini veya bazen de toplumun güvenliğini tehdit edebilir. Bireyleri ve sistemleri bu tür saldırılardan korumanın yanı sıra, bilinmeyen bir tehdidin önlenemeyeceği için saldırı riskleri de belirlenmelidir.

Kötü amaçlı yazılım, istismar ve sahtekarlık gibi yeni tehditler genellikle çok geç fark edilir. Bu tehditler ilk keşfedildiğinde, sıfır gün olarak tanımlanır; zayıflıklar daha sonra bilgisayarların zayıf yönlerinin olması nedeniyle değerlendirilmekte ve büyük zararlar ortaya çıkmaktadır. IPS veya IDS gibi hiçbir güvenlik ürünü üreticisi bu riskleri derhal düzeltmeden onları tespit etmeyi başaramaz.

Bu tez, bu zayıf yönleri mümkün olduğunca çabuk belirlemek için sosyal medya kaynaklarını (örneğin Twitter) kullanmaktadır. Amaç, bilinen bir sıfır günlük saldırıya maruz kaldıklarının farkında olmayan kişilerin yayınladığı bilgileri toplayarak sıfır günlük saldırıların belirlenmesidir. Çalışma sosyal medyadaki verileri kullanıyor ve kelime sınıflandırma gibi makine öğrenme ilkelerini uygulayarak verileri işler. Sonuç olarak, güvenlik açıklarını tanımlayan ve ilgili üreticileri veya satıcıları bilgilendiren bir program geliştirilmiştir. Bu yolla, sosyal medya verileri üzerinden sıfır günlük saldırılar tespit ederek satıcıların güvenlik açıklarını daha etkin bir şekilde gidermeleri mümkündür.

Bu tezde, risk, güvenlik ve sosyal medya ile ilgili temel kavramları ele almak için bir literatür taraması yapılmış ve sosyal medyada saldırıya uğraması muhtemel saldırıları bulmak için yeni nesil bir program geliştirilmiştir.

Anahtar Kelimeler: İnternet, siber güvenlik, makine öğrenmesi, kelime sınıflandırma, sıfır günlük saldırı, Twitter, TensorFlow

NOMENCLATURE

Acronyms

PHP	Php Hypertext Preprocessor
HTML	HyperText Markup Language
HDD	Hard Disk
CIRT	Computer Incident Response Teams
OSINT	Open-Source Intelligence
DDoS	Distributed Denial of Service
BGP	Border Gateway Protocol
DNS	Domain Name System
CERT	Computer Emergency Readiness Team
APT	Advanced Persistent Threat
MITM	Man In The Middle
UI	User Interface
API	Application Programming Interface

CONTENTS

M.Sc. THESIS EXAMINATION RESULT FORM i
ETHICAL DECLARATION ii
ACKNOWLEDGEMENTS iii
ABSTRACT iv
ÖZ v
NOMENCLATURE vi
LIST OF TABLES ix
LIST OF FIGURES x

CHAPTER 1- INTRODUCTION 1
CHAPTER 2- BACKGROUND INFORMATION 4
2.1 Definition of Security 4
2.1.1 Concepts Related to Security 5
2.1.2 Definition of Terror and Threats 6
2.2 The Internet and Cyber Environment 7
2.2.1 Definition of Internet and a Short History 7
2.2.2 Cyber Environment Security 8
2.3 Security Systems Used in Cyber Environments 10
2.4 Definition of Communication 12
2.5 Definition of Social Media 12
2.6 Security Intelligence 13

CHAPTER 3- RELATION OF SOCIAL MEDIA COMMUNICATION AND CYBER SECURITY 16
3.1 Cyber Security Strategies in the World 16
3.1.1 The USA 19
3.1.2 Europe 20
3.1.3 Turkey 22
3.2 Social Media and Security Relations 22
3.2.1 Cyber Crime 23
3.2.2 Cyber Attack 23
3.2.3 Cyber Threats 25
3.2.4 Cyber Terrorism 31
3.2.5 Cyber War 33
3.3 Cyber Security Intelligence 33

3.3.1 CyberTwitter 38
CHAPTER 4- ARCHITECTURE 40
4.1 System Design 40
4.2 Technical Architecture 42
4.3 TensorFlow Machine Learning Library 43
4.4 NLTK Natural Language Toolkit 49

CHAPTER 5- AN APPLICATION ON TWITTER 53
5.1 Importance of the Study 53
5.2 Purpose of the Study 53
5.3 Hypotheses 53
5.4 Environment and Sample 54
5.4.1 Twitter 55
5.4.2 Searched Words 57
5.5 Limitations 59
5.6 Codes and Application 60

CHAPTER 6- PERFORMANCE 66
6.1 Performance 66
CHAPTER 7- RESULTS 71
CHAPTER 8- CONCLUSION 75
CHAPTER 9- FUTURE WORK 77
REFERENCES 78
CURRICULUM VITAE 83

LIST OF TABLES

Table 2.1 Pre-modern Security Intelligence and Modern Security Intelligence (Özçoban, 2014: 30) 14
Table 5.1 Pie Chart of Searched Words, Sorted 58
Table 6.1 Comparison of Finding Zero-Day Tweet Success Rate 70
Table 6.2 Research Application Table Interface 70
Table 7.1 Twitter Flot Chart 1 72
Table 7.2 Twitter Flot Chart 2 72
Table 7.3 Word Classification 73
Table 7.4 Word Classification 2 73
Table 7.5 Retweet Count 74

LIST OF FIGURES

Figure 2.1 The Security Systems Used in the Cyber Environment 11
Figure 3.1 Social Engineering Process 35
Figure 3.2 Determining the Positions of Senior State Executives with Their Photographs 36
Figure 3.3 Search Engine – Legal Google Hack Style 38
Figure 3.4 CyberTwitter 39
Figure 4.1 Architecture of the Study 40
Figure 4.2 Input Parameter 41
Figure 4.3 Input Parameter HTML & PHP Form Code 41
Figure 4.4 Search Word Parameter HTML & PHP Form Code 41
Figure 4.5 Technical Architecture Flow Diagram 42
Figure 4.6 Equation of Softmax From Tensorflow Library 44
Figure 4.7 Softmax Classifier Logical Algorithm Schema 44
Figure 4.8 Noise Classifier Logical Algorithm Schema 45
Figure 4.9 Example of Tensorflow Successful Result 45
Figure 4.10 TensorFlow Vector Dimensionality for Zero-Day 46
Figure 4.11 Most Valuable Tweet Found from Program 46
Figure 5.1 Tables Shown by the Software 54
Figure 5.2 Zero-Day Tweet Example 54
Figure 5.3 Dashboard of Applications for Web UI 57
Figure 5.4 Searched Words List 57
Figure 5.5 Table of Tweets with Details 58
Figure 5.6 Limitations of HDD 59
Figure 5.7 Limitations of Twitter Rules 59
Figure 5.8 Frontend of Web UI 60
Figure 5.9 Compatibility Part of Internet Explore and Edge 61
Figure 5.10 Code of Web UI 61
Figure 5.11 Code of Server Side PHP of Web UI 62
Figure 5.12 Code of Web UI 62
Figure 5.13 Code of Scripting 63
Figure 5.14 Code of Scrolling Page Imitating a Person 63

Figure 5.15 Input Parameter 64
Figure 5.16 Input Parameter HTML & PHP Form Code 64
Figure 5.17 Search Word Parameter HTML & PHP Form Code 65
Figure 5.18 Architecture of NLTK and TensorFlow Libraries Working Together 65
Figure 6.1 Performance of 1-Page Scrolling and Collection of Information from Twitter Page 66
Figure 6.2 Performance of 5-Page Scrolling and Collection of Information from Twitter Page 67
Figure 6.3 Performance of 10-Page Scrolling and Collection of Information from Twitter Page 67
Figure 6.4 Performance of 15-Page Scrolling and Collection of Information from Twitter Page 68
Figure 6.5 Collecting Tweet Time vs. Tweets 68
Figure 6.6 Data Size vs. Tweet Counts 69
Figure 6.7 Comparison of Tweets Collection Performance with BOT vs. Twitter API 69

CHAPTER 1

INTRODUCTION

The Internet is the fastest, most practical, and cheapest global avenue of communication in the 21st century. This makes the Internet popular and its users increase hourly every day around the globe. However, this also creates serious risks in terms of security and safety for people, information, systems, companies, and even governments. Internet communications cannot be followed constantly; at the same time, the activities of some Internet users may be damaging for themselves or for others. Thus, the development of Internet systems and the concepts of security, risk, safety, and accessibility are extremely important in terms of their applications in daily life.

The global number of active Internet users has reached at least 2.5 billion. However, many violations of Internet security and online privacy are arising as a result of the use of state surveillance technologies on the Internet, and in the cyber environment Internet service providers and companies collect personal data online for marketing purposes. The malicious activities of hackers also cause many violations in terms of Internet security and online privacy, among other examples. The online activities of people cannot always be exactly known and this may often allow room for the infringement of rules and laws.

These changes in our daily life have led people to question the safety and the security of individuals, companies, and governments. Research about safety and security in cyber environments has shown that most individuals think that Internet security is solely the government's problem and responsibility. This attitude, however, is absolutely wrong as all individuals and legal entities have their own responsibility to strive to avoid danger. All such parties must be careful about sharing information and must learn to use the Internet safely. Internet security and safety systems must also be taught to all users.

Social media platforms such as Facebook, Twitter, YouTube, and others have millions of users who are communicating, sharing information, and engaging in entertainment. These virtual social platforms can also be used by public enterprises and companies to reach the broader society and continue their marketing activities. Malicious software and users may sometimes acquire personal data or trigger uncontrollable data flows. This creates terrorism risks and challenges to safety and security.

In this thesis, the basic objective is determining how to control malicious sharing on social media and how to prevent online or physical attacks. To answer this question, first of all, the basic concepts of the study must be defined. In the first chapter, definitions of security, Internet, cyber environment, communication, social media, and security intelligence are given.

In the second chapter, the most important attacks to date are highlighted. In the USA, Europe, and Turkey, some cyber attacks have been waged by using the Internet and those attacks have damaged the systems of companies, airports, and other such organizations or institutions. These have been terrorist actions in the technology age of the 21st century.

Security systems continue developing daily and security companies have especially serious competition while they are building technological systems. These include some software, the presence of which is a major advantage for Internet users. In this study, codes have been written to try to comb out malicious posts on Twitter.

Twitter is one of the most popular social media platforms; if a threat can be detected in its system, that would help governments and/or individuals to be protected. For this thesis, a program has been created that searches the desired words in tweets, and it can learn other related words and determine whether any tweet has been written about a threat or not. For example, the words “Zero Day”, “0day”, and “0-day” may be fed as input to the program to catch tweets that include those words.

The program can be developed by teaching it new words, and beyond the realm of security, it can be used to reach people who are discussing any other topics. It can

also determine who is the user and the user's address. This is one of the most important advantages of the program.

This study is important in increasing the knowledge about security and safe Internet usage, and for establishing national safety systems. If these codes work and if they fulfill their planned goals, the program could be sold to other countries and/or be used to prevent terror attacks before they occur by searching for selected words.

In this thesis, the relevant concepts are first defined. A literature review has been conducted regarding the ideas of security, terror, threat, cyber environment, and cyber environment security systems. For a better understanding of the importance of the subject and to see how people may be attacked via the Internet and how terror activities might be planned, it is also helpful to define communication, social media, and cyber security strategies. Among these, some examples of cyber terrorism are given.

In the final section of the thesis, details of the application are given and an implementation on Twitter is performed. The program has Web UI to be user-friendly because the system has different scripts and many of them need to work in orchestration. Web UI takes parameters from the input box and then starts interpretation with serialization with parameters such as figures and codes. First the user enters a word such as "zero-day" and then clicks a search button. Web UI calls system procedures with PHP and Python codes. The codes can obtain relevant tweets and store them in MariaDB, working on the Ubuntu Operating System. Other employed systems and processes include Python and Bash Script, other libraries, and the driver. The words 0-day, 0day, zero-day, and zero-day are sought as special words for investigating searches for zero-day vulnerabilities and to make sense of the TensorFlow machine learning framework.

CHAPTER 2

BACKGROUND INFORMATION

2.1 Definition of Security

Security is one of the main concepts of the discipline of international relations. Thus, many studies of security have been carried out since the establishment of this field. However, no consensus definition has been reached regarding what the concept of "security" means and so debates on the issue continue. For individuals, security can be defined as being safe. Every living creature in the world would like to continue to live, but for systems, companies, and countries, the term "security" has gained more meanings (Sancak, 2013: 124; Pawar and Anuradha, 2015: 504).

Degaut notes that security is the guarantee of having comfort and the ability to make one's own decisions. For countries and companies, security is the fundamental issue for their workers/citizens because security is a basic human right (Degaut, 2015: 2).

The Oxford Dictionary defines "security" as a noun meaning freedom from danger or threat. For countries, security means "safety of a state or organization against criminal activity such as terrorism, theft, or espionage" (Oxford Dictionary, 2018).

The definition of security continues to change over time. With the development of technology, the notion of security and the understanding of its necessity have grown. Especially during the Cold War, the definition of security changed to imply "control ability". Since the 1990s, security for a nation began to signify more than not only avoiding war and having a powerful military. After the 1990s, with globalization, the idea of "security" gained an economic nuance. Today, in the 21st century, security means keeping information from unauthorized people (Bachmann and Gunneriusson, 2015: 79; Matthews, 2011: 64).

2.1.1 Concepts Related to Security

For a better understanding of security, the related concepts should also be explained. As stated above, the Oxford Dictionary defines security as the lack of threats and risks. Therefore, the term “risk” should first be defined.

Today the most important resource is information; thus, the concepts related to information security must be addressed. Information security can be defined as prevention of both the deterioration of information and access to information by individuals who are not authorized for that information. The seizure, leakage, destruction, alteration, or dissemination of information by unwitting or unauthorized people indicates a lack of security. It is further necessary to highlight the principles of information security (RFC 2828, May 2000, Internet Security Glossary; RFC 4949, Aug 2007, Internet Security Glossary, Version 2):

i. Confidentiality: The confidentiality of access to information by authorized persons only. A security service that protects data from unauthorized disclosure.
ii. Integrity: The property signifying that data have not been changed, destroyed, or lost in an unauthorized or accidental manner. The inability of unauthorized people to change information. For example, the integrity of information can be maintained with an electronic signature or open key structure.
iii. Availability: The property of a system or a system resource being accessible, or usable or operational upon demand, by an authorized system entity, according to performance specifications for the system; i.e. a system is available if it provides services according to the system design whenever users request them.
iv. Authentication: An authentication process that verifies an identity by requiring correct authentication information to be provided in response to a challenge.
v. Accountability: The property of a system (including all of its system resources) that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions.

2.1.2 Definition of Terror and Threats

"Threat" is defined as "someone or something that is likely to cause harm or damage" in the Cambridge Dictionary and "terror" is defined as "violent action or threats designed to cause fear among ordinary people, in order to achieve political aims" (Cambridge, 2018). Bruce Hoffman defines terrorism as "the deliberate creation and exploitation of fear through violence or the threat of violence in the pursuit of political change" (Brickey, 2012: 4). Terrorism aims to create panic and fear in society. For an action to be defined as terrorism, the following specifications should be met (Nasrat, 2015: 15):

i. Violence or use of force,

ii. Political purpose,

iii. Terrifying,

iv. One or more threats, and

v. Psychological impact on society.

As seen from these definitions, "threat" and "terror" are related concepts. Both of them have the purpose of damaging society by creating fear. Terrorism has been one of the greatest dangers to societies and states for centuries. States have taken various precautions to combat terrorism and they are working together to solve their terror problems. Here it must be stressed that terrorism is not a unique problem of any country, society, or geographical area. With the increase of the usage of the Internet in particular, terror activities have become more common as people can easily find each other and share their ideologies (Şimşek, 2016: 319).

2.2 The Internet and Cyber Environment

The Internet can be thought of as a wire that connects computers and computer-based appliances to each other. It basically gives every computer/device an ID and lets users travel from one address to another. These addresses are web pages. Users enter an address into their computers and continue traveling via links. These addresses may be social media platforms or links to news, companies, shopping platforms, and even banks. The Internet delivers whatever we want to use within seconds, providing this service 24 hours a day and 7 days a week (Sade-Beck, 2004: 46).

The simplest definition of this technology is that many computer systems are interconnected and it can be expressed as a worldwide and widespread network of communication. The Internet is a world-class computer network that connects huge amounts of computers across the world. Via the Internet, thousands of computer networks allow billions of users to share computer resources and information via millions of computers (Kahn and Cerf, 1999: 2). This means that the Internet is a crowded and unsafe platform. Here, more details about the Internet and its short history will be provided to understand how fast it has developed and how significantly its number of users has increased.

2.2.1 Definition of Internet and a Short History

There are many definitions of “Internet”. According to some of these definitions, it is a communication system that is becoming more widespread every moment and is growing worldwide. The Internet is a communication tool that can adapt itself to the fast changes in societies, cultures, and technology; it can also cause these changes. It is a sum of all communication methodologies. It creates economic opportunities (Solmaz et al., 2013: 24). It can be defined as an electronic network that provides a systematic relationship between individuals, groups, or institutions.

Internet technology began with the Arpanet Advanced Research Projects Agency in the 1960s. It was a network system that could be used to share information between authorized computers. Due to the World Wars and the Cold War in particular, countries tried to keep information in their hands and find resources for creating technology. The Internet was invented with a scientific project of the US Army and

developed with another project called NSFNET (National Science Foundation Network) in 1986. NSFNET was a project to make the Internet a commercial product. This development allowed for new networks and more and more computers started to enter this network day by day. The last important step in the development of the Internet was the development of the World Wide Web (www). The World Wide Web has played an important role in increasing Internet usage and the number of users. In January 1993, there were only 50 websites on the Internet. The number of websites on the Internet reached 500 in October of 1993. In 1994, new browser programs were introduced with the creation of Internet-related standards. Information was expanded with the organization of the first web conference in Geneva in 1994 (Altınbaşak and Karaca, 2009: 466; Keefer and Baiget, ND: 90).

2.2.2 Cyber Environment Security

Security on the Internet starts with authorization, commonly with a username and a password of the user. On every platform on the Internet today, there is a membership system, and for security every website or mobile application has an entry field for the password and username. However, for high security, these are not enough because every day new software systems are been produced to steal such information. Here the idea of network security must be understood. It consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, modifications to the system, misuse, or denial of a computer network and network-accessible resources (Bachmann and Gunneriusson, 2015: 79; Pawar and Anuradha, 2015: 504).

Cybersecurity has become a matter of global interest and importance. More than 50 nations have already officially published some form of strategy document outlining their official stance on cyber space, cyber crime, and/or cyber security, but only a few of these sources seem to make a distinction between the concepts of cyber security and information security. The International Telecommunications Union (ITU) states that cyber security is: “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets

include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment" (Solms and Niekerk, 2013: 97-98).

According to the Digital in 2018 Q2 Global Overview Report (We are Social, 2018), which was prepared by the digital marketing agency We Are Social and Hootsuite, there are 4.021 billion Internet accounts in the world. In terms of social networking, Facebook ranks in the top three with 2.167 billion users, YouTube has 1.5 billion users, and WhatsApp has 1.3 billion users. According to the same survey, there are 51 million active Facebook user accounts in Turkey. One of the main reasons for security vulnerabilities in social media is that privacy cannot be protected and users can make themselves targets by sharing personal information, photos, or texts via their accounts and profiles. The increase in the use of the Internet and its spread among users of almost every age range has made this realm more dangerous (Yavanoğlu, 2012: 17).

Especially during the Jasmine Revolution, the subject of Internet security started to become a main topic of both governments and individuals. An opinion or simple ideological change can enlarge or destroy a governmental system by rallying supporters. In 2011, the Middle East faced such a situation, which started in Tunisia and continued to Egypt, Bahrain, and Syria. Individuals who were asking for more democracy came together and with civil disobedience they overthrew governments. In the literature, some authors cite these as terror examples, but some others think that it was a result of shortcomings in those societies. Both opinions in these cases show that communication and the speed of technology can affect societies very quickly and this can help people to find others who have similar ideologies (Bachmann and Gunneriusson, 2015: 87). This also showed that terrorist ideologies can easily rally supporters and also that people can plan attacks using the Internet.

2.3 Security Systems Used in Cyber Environments

For providing cyber security there are various systems that should be used at the same time because the expansion of Internet usage increases the risks of attack. The concept of corporate cyber security is an issue that should not be ignored in the present day when cyber threats and risks are increasing non-linearly and becoming more complex.

The definition of the term “zero-day” is relevant here. Zero-day can be described as a vulnerability that has just been discovered in the security world, but no one else knows about it yet, such as the manufacturers, the operators of the system in question, or the developers. Some of these openings to threats are closed immediately and some vulnerabilities remain open for many years; the important thing is how long it takes them to be detected. It is not possible to close an unknown opening.

Therefore, it is necessary to determine zero-day vulnerabilities first. It is not possible to take action to work on an unknown situation. For example, when a vulnerability is detected by a hacker, he or she often does not announce it because this vulnerability being unknown by others makes things easier for hackers. For Intel processors, two weaknesses, Meltdown and Specter, were announced on the same day, but later it was seen that the hacker community had already known about these for 15 years. In other words, this showed that there were zero-day openings that had remained in hiding for 15 years (Sanders, 2019).

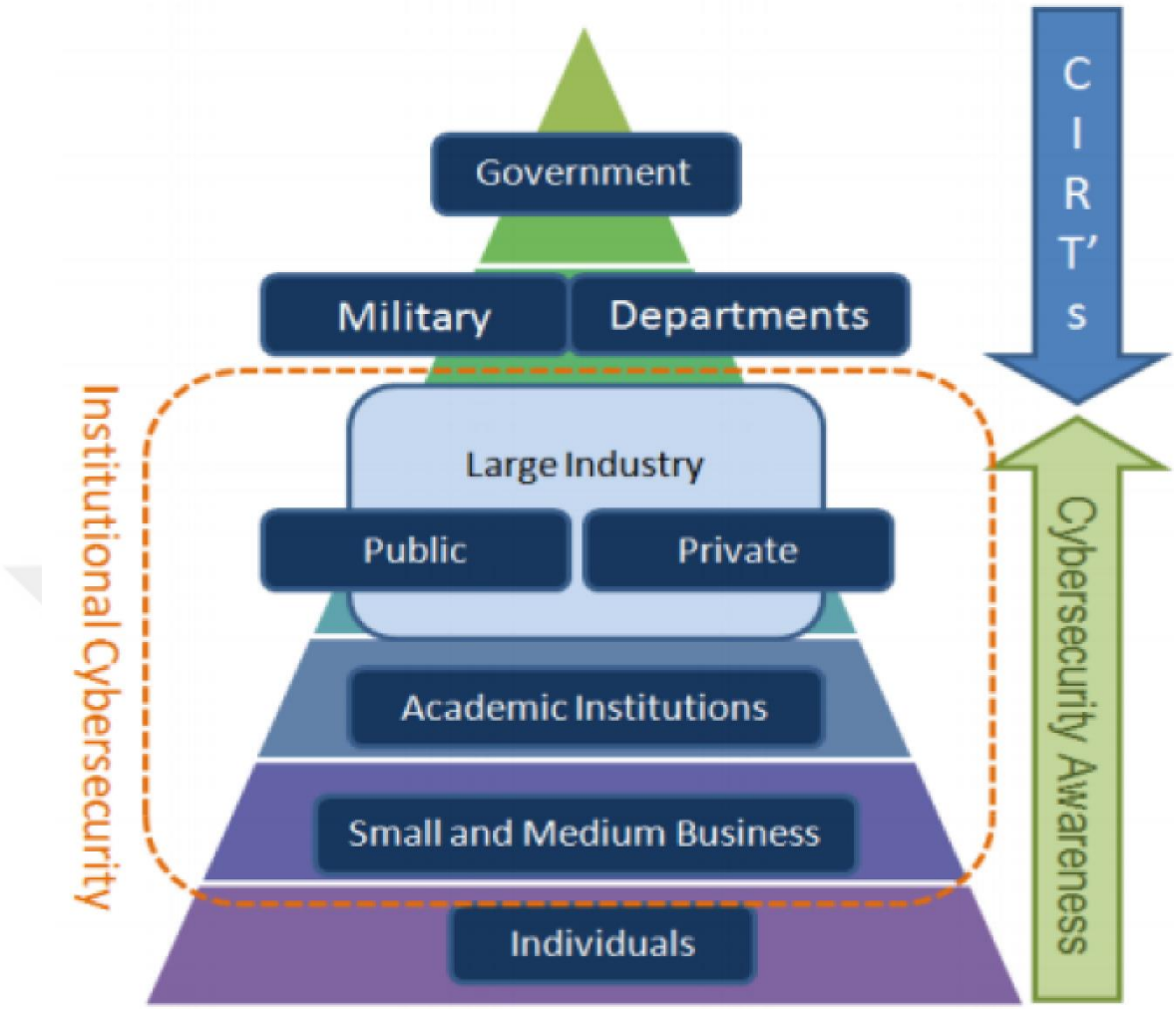


Figure 2.1 The Security Systems Used in the Cyber Environment

There are systems that investigate abnormal behavior, such as OSINT (Open Source Threat Intelligence), the Symantec zero-day detection device, and other threats for zero-day threats. OSINT is a component of any good threat intelligence operation. It is essentially a collection of indicators that point to heightened risk and provide information about a particular threat. Such data are key to helping security leaders recognize danger and make informed decisions about their next steps. OSINT information can come from many sources in the public domain, which is why experts refer to it as open-source (Ribeiro, 2018). Symantec's core protection against known and unknown threats uses a layered approach to defense. The comprehensive approach protects the network before, during, and after an attack. Symantec reduces

the risk of exposure by providing tools to increase the security posture ahead of any attack (Symantec, 2019).

2.4 Definition of Communication

Communication can be described as a message from a person or group that reaches its goal. However, these messages must be understandable between the parties. There are five methods people use for communication. These are internal communication or self-communication, interpersonal communication, group communication, transnational communication, and mass communication (Lunenburg, 2010: 2).

The Internet can be defined as a mass media tool but at the same time it lets people conduct personal and interpersonal communications, and by this specification it can be separated from all traditional communication tools. While traditional channels of communication, such as television and print media, are visually impressive, they are thought to be manipulative in achieving their goals because they establish one-way communication. In the web applications provided by the Internet, simultaneous and two-way information flow is provided between the communicating parties. Like mass media, a message can be sent to society via the Internet, but it also helps to understand the reactions of people (Solmaz et al., 2013: 24).

2.5 Definition of Social Media

A social network means people communicating with each other via Internet communication methods. The users are people who can easily meet others who have the same cultural variables. Via social media, people identify themselves within community life and also create social communication in virtual environments. They can also communicate by sharing symbolic images and actions from normal social life, such as by using photos, videos, hashtags, etc. One of the first definitions of the term “social network” was given in 1984 by Barnes. According to Barnes, social networks consist of individuals who interact with each other and they have psychological significance for people. According to Boyd and Ellison, social networking sites include web-based services where a part of the user’s information is

available to other users, where they can communicate and send friend requests and share various things via social media (Ermişoğlu, 2016: 41).

Social media is now widely preferred by institutions and individuals as a form of mass media communication. The most important factors that make social media so attractive are undoubtedly its speed, success, and price. The target audience can also be easily selected. A better way to serve capitalism would be unthinkable, as it was also determined that people's thoughts and especially their purchasing decisions are changed due to the interactions that people have via social media.

2.6 Security Intelligence

Security intelligence is a concept that has existed since the establishment of the first relationships between people. It is the process of acquiring economic, political, humanitarian, and similar information about people who are in contact or people who want to be in contact. For states, intelligence means survival, and for this reason we can say that the very existence of a country or government that does not have effective security intelligence is at risk. Like international relations, intelligence science has also been recognized as an academic discipline for nearly half a century. In the period leading up to the end of the Second World War, military leaders thought that there was no need for an intelligence service in peacetime. However, after the Second World War, countries started to make huge investments in their intelligence organizations. As a result of studies in this field, there have been great developments in security intelligence, especially in parallel with technological developments. Today, as outlined in Table 1, there is a huge difference between modern security intelligence systems and the traditional ones (Özçoban, 2014: 34).

Table 2.1 Pre-modern Security Intelligence and Modern Security Intelligence (Özçoban, 2014: 30)

	Pre-modern Security Intelligence	**Modern Security Intelligence**
Information Source	Completely human sources	Internet, open resources, human resources
Reliability	Low reliability; verifications difficult; prone to being used for deception	Relatively high, verifiable; can be supported by various intelligence sources
Obtainability	Slow; too late to be important	Quick; available if necessary
Importance and Demand for Intelligence	Important but not vital; generally pessimistic and negative attitude for intelligence	Very high demand even in peace, vital, positive attitude for intelligence
Analysis	Limited information	Increasing information and computer support

When it comes to intelligence, national security should also come to mind. For a better understanding of intelligence we must therefore also discuss the term "national security". Technological advances in the defense field have particularly changed the balance and the importance of the military power of countries. Today war has become not only a situation involving military power; cyber wars, chemical and biological wars, and policy battles have also become concepts of everyday life. For this reason, cultural, social, and even biological security should be ensured for national security. This situation also changes the understanding of security. In this context, the definition of intelligence should be changed and the studied subjects regarding intelligence risks should be enlarged. The concept of national security has no universally accepted meaning today. Especially with the development of the Internet, many issues that were not risks before became risks for national security

because it has become possible for people to find supporters on every issue on the Internet (Miş, 2011: 348). In this context, the concept of national security involves the taking of measures against all kinds of risks that may pose a threat to the integrity of the state and to the constitutional and social order. Thus, the term “intelligence” has gained more importance.

CHAPTER 3

RELATION OF SOCIAL MEDIA COMMUNICATION AND CYBER SECURITY

3.1 Cyber Security Strategies in the World

Sony Pictures Entertainment produced a film entitled "Interview" about an assassination attempt against North Korean leader Kim Jong Un. Korea said that this film was derogatory and told the company not to release it. They organized a cyber attack on the company to destroy the film before it was aired. After this attack, the PS3 system was damaged. An activist hacker group had undertaken the attacks. Sony then stated that the attacks against the film were an attack on freedom of expression rather than a cyber security problem. However, the cyber security aspects of the attack were also quite severe. As a result of the process, losses of more than $100 million were suffered. According to Sony's explanations, the personal information of more than 11 million users of the PlayStation network was also seized. After the attack, Barack Obama said in a statement that the United States would not be turned into a country where dictators demand censorship (Roman, 2014).

The Sony attack was the first attack in which the name "Anonymous" was heard. This group immediately attacked the basic information network of the Lockheed Martin company serving the US military after attacking Sony. When investigations were made about this activist hacker group, it was seen that they had also intervened in the Irish elections in the past. During the Arab Spring, this group, which cooperated with Tunisian hackers, attacked the websites of the Tunisian state and decommissioned eight sites for a while (Roman, 2014; Disimone and Horton, 2017: 16).

In April 2007, the Estonian government said that the country's websites had been under intense attacks for three weeks and that they thought that Russia was responsible. The cyber attack began on 27 April 2007, with the commemoration of the Russian soldiers who died in battle against the German Army during World War II in Tallinn. During the protests of the Russian minority, opposing the relocation of

a monument, they claimed to represent the struggle against fascism, a person was killed, and many were wounded and more than a thousand arrested. The Estonian government stated that the attacks started immediately after those events and showed that the events were the reason for the attacks. In Estonia, which is a country very dependent on the Internet, DDoS service was stopped by the attacks and these attacks affected many institutions and organizations, such as the presidency, ministries, political parties, the country's largest banks, and communication institutions, all at the same moment. Estonian experts stated that the attacks came from all over the world, but at first, some of the attackers' addresses were identified and the vast majority of these addresses belonged to Russian public institutions. The attacks continued with great intensity, especially on 8 and 9 May, which are celebrated as Victory Day in Russia. All banking services, citizenship services, company setups, and even parliamentary elections were brought to a halt during these attacks on the Internet. NATO spokesman James Appathurai announced that they would provide technical assistance to the Estonian government (Schmidt, 2012: 2-3).

On 30 January 2017 many institutions around the world as well as the Atatürk Airport systems were exposed to harmful software and were damaged. Research has shown that a virus named Conficker spread to the computer system of the airport in İstanbul. This harmful software can spread to many files in a short time and can cause damage that is difficult or even impossible to repair. During this period, the systems used to organize the international terminal were especially damaged (PWC, 2017).

With the entry of the virus into the system, there were losses in the systems of passenger and baggage operations at the airport's international terminal. According to TAV, which is the operator company of the airport, the attack was staged such that the time required for the cleaning of the virus was done by hand, and this situation caused the timing problems. The virus had entered the airport systems in order to use the system operated by an international computer company called SITA CUTE C in the operator's international terminal. The same problem arose in other airports around the world where this system was used and there was a great panic. The virus

damaged more than 400 files of the airport's database system (Şenol, 2016: 11; Chip, 2009).

Another attack occurred in 2015. On the 14th of December 2015, slowness and access problems were experienced in accessing domain names ending with .tr. In five different regions of Turkey and abroad, 6 servers faced DDoS attacks. According to UlakNet's instantaneous backbone data indicator, a load of over 35-50 Gbps in size occurred, above the capacity. That means that the attack caused huge traffic on the Internet and the capacity of the sites was surpassed. On 14 December, a statement by Romeo Zwart, authorized by the RIPE, was published. This statement reported that the attack began around UTC 08:00 and various precautions were taken by the RIPE; these precautions were effective for a while but the size of the attack was huge in comparison to the precautions. The attack was spoofed on fake IP addresses for the necessary measures to be taken by service providers regarding the issue, and the application of BCP-38 for resource address validation and the need to reduce the enforcement of networks in this way. According to the literature, the reason for these attacks was the tension between Turkey and Russia. A Russian military plane had been brought down in Turkey's airspace in that period and both countries were considered to be reasons for this war in cyber space (Zwart, 2015).

However, unlike these literature reports, the group that undertook the attacks was called Anonymous and this group said that the attacks were because of Turkey's support of ISIS (Bolton, 2015) (see Figure 3.1).

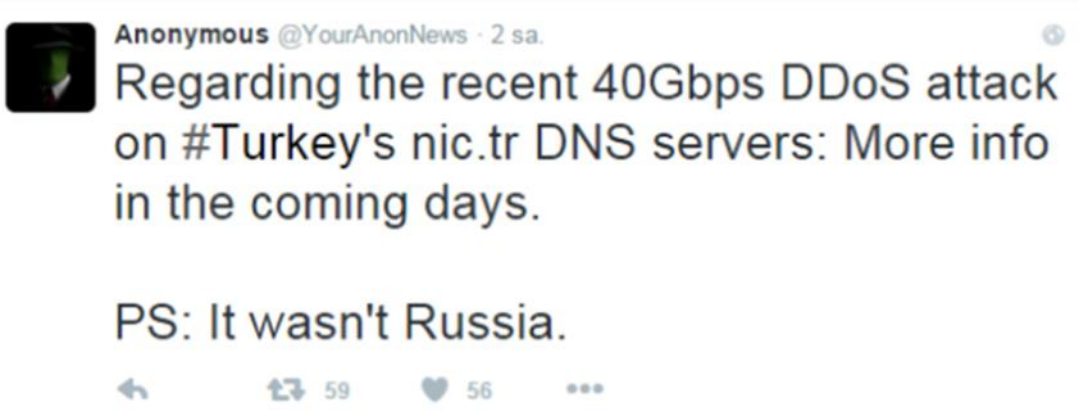


Figure 3.1 Anonymous Tweet (Bolton, 2015)

To prevent damage, access to the IP addresses of the servers where DNS records were kept was cut. Border Gateway Protocol (BGP) registration was sent to overseas operators. Only local servers were open for workaround (Darıcılı and Özdal, 2017: 25-26).

As seen from this brief history, many cyber attacks have occurred in the last years and governments and/or private sectors of different countries have been injured. These attacks have blocked systems and economic losses have occurred. Because of these attacks, countries have to make their security strategies accordingly, as will be discussed in the following subsections. The lack of a security strategy brings political, military, economic, and social risks.

3.1.1 The USA

When it comes to the USA and cyber security, the first institutions that come to mind are undoubtedly the Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), United States Department of Homeland Security (DHS), USCYBERCOM, and the National Security Agency (NSA). Cyber security for the country does not only concern information theft; it also explores issues in space-related research, state security, and protection of personal information and state secrets. Especially after 2000, there has been serious competition regarding the technological opportunities originating from cyber space among the developed countries. Within the scope of its current political, economic, and military power, the

USA, which is one of the hegemonic powers in the global system, has begun to follow continuous improvement strategies in both state and private sectors in order to not lose power in the digital arena, to continue its leadership, and to ensure its security (Ada, 2018: 44-45).

The USA is one of the most powerful countries in the world in terms of cyber attacks and security. However, the country still faces constant attacks. Since 2001, cyber security has been on the state agenda. In 2003, during the period of George Bush's presidency, the National Cyber Space Security Strategy was prepared. In this strategy, issues such as federal government, local governments, the private sector, and the public were focused on. In each published strategic plan, the objectives were shaped in the context of the protection of America's critical infrastructures against cyber attacks for reducing national sensitivity to cyber attacks and minimizing the damage after such attacks. The strategy has five critical priorities. These are as follows (Çakır and Ada, 2017: 633):

i. National Cyber Space Security Intervention System,

ii. National Cyber Space Security Threat and Vulnerability Reduction Program,

iii. National Cyber Space Security Awareness and Training Program,

iv. Public Cyber Space Protection, National Security, and

v. International Cyber Space Security Cooperation.

3.1.2 Europe

The first strategic steps of the European Union in cyber security were begun in 2004. At this time, the EU Commission considered the issue of cyber security as any kind of technological threat that would harm units of people and nations, which would have a negative impact on the effective and productive economic prosperity of the member governments and would pose a risk for terrorism. In the same way, the definitions of the infrastructure of the units dealing with security and technology issues, and how they should be formed, were defined for the first time regarding such

protection. The Commission chose financial centers and finance-related units, communication and information technology companies and public institutions, energy facilities, and communication networks as the most important centers to be protected. In addition, transportation to clean and reliable food, energy production, and public transport networks were also marked as important and the Commission wanted to take necessary precautions to regulate the security infrastructure (Çakır and Ada, 2017: 633-634).

In 2005, in the European Union, the Green Book was published, after the large cyber attacks on the USA and other countries caused panic in the EU. The Green Book is a document containing action plans on cyber security. The plans provide information on what should be done to minimize the risk of cyber attacks. In addition, estimations were made about what kind of damage might occur in possible attacks. The Critical Infrastructure Warning Information Network was launched at the same time. In 2010, the EU Commission launched the Digital Agenda. The aim of this step was to ensure the security of the network and information, and to identify potential risks and take measures against them (NSA-CSS, 2016).

In 2010, it was decided in Lisbon that the EU and NATO should have more regulations of national security. It was also decided at this meeting that a center on cyber security should be established. As a result, the EC3 (European Cybercrime Center) and CERT (Computer Emergency Readiness Team) were established (Çakır and Ada, 2017: 635).

The cyber security policies in the EU were revised in 2016. With these regulations, the authorities of ENISA (European Union Agency for Network and Information Technology), which was authorized in 2010, were increased. Today, ENISA carries out projects with the USA and other countries all around the world to take precautions regarding cyber security, not only in the EU (European Commission, 2010).

3.1.3 Turkey

The Cyber Security Council of Turkey was established on 11 June 2016 by the decision of the Council of Ministers. In accordance with the decision, a Cyber Security Council was formed, and the Ministry of Transport, Maritime Affairs, and Communications was assigned the authority and duty for it. It was further decided that working groups and temporary boards related to cyber security would be formed. The Cyber Security Council is regulated by Article 1 added to Electronic Communication Law No. 5809. To determine the precautions to be taken by public institutions and organizations and real and legal persons in relation to cyber security, the Security Board was established. The level of representation of the ministries and public institutions and the organizations and members to be included in the Cyber Security Council is determined by the Council of Ministers. In line with the increasing security requirements and developing information and communication technologies, the need for updating the national cyber security strategy and determining relevant actions for the years 2016-2020 was recognized (Bilgi Teknolojileri ve İletişim Kurumu, 2018). It can be said that Turkey is trying to enlarge its cyber security precautions day by day and the different ministries are working together, but more technology should be developed.

3.2 Social Media and Security Relations

Social media platforms are very popular among every age group and all around the world. Users can create profiles there and share entertainment such as videos, links, or blogs. They also share information with others by communicating person to person, or they can use these platforms for mass communication. However, it must be remembered that every user faces a risk on social media. With the new “sharing trend”, people have started to post about their private lives on the Internet, and if a user does not have enough knowledge of or attention to security, he or she can be harassed or have information stolen.

Social media platforms are also popular areas for attracting sympathizers to terrorist groups. These platforms are places where people can easily share their opinions and attract others. Especially after terror actions, terrorist groups can share details about

the attack or other information on social media. Social media platforms are also suitable places for cyber violence. The literature reports that cyber violence can be the starting point of cyber threats or even cyber terror (Nasrat, 2015: 26).

3.2.1 Cyber Crime

For understanding cyber crime, cyber terrorism, cyber threats, and other related concepts, first of all the term "cyber" should be defined. This word is an abbreviation of the word "cybernetic", which was used by Norbert Weiner in 1948 for the first time to refer to "the science of communication and control in animals and machines". Today this word still does not have a very specific definition but its generally accepted meaning is data processing/IT/informatics. Informatics is used in a regular and reasonable manner by human beings in communication in technical, economic, and social fields and for knowledge that is the basis of science, especially through electronic machines. From these definitions we can say that "cyber" means to have control over machines and systems by using computers (Beer, 2002: 210).

Cyber crime is one of the most complicated concepts. Any criminal offense committed against cyber space will not be included in this definition. Before giving more details on this subject, it is necessary to address the concept of cyber crime.

Briefly, cyber crime can be defined as crimes committed on the Internet using a computer as either a tool or a targeted victim. It is very difficult to classify crimes in general into distinct groups as many crimes evolve on a daily basis. Such as in the real world, crimes in cyber space cannot be easily separated because one attack can cause more than one crime. However, all cyber crimes involve both a computer and the person behind it as victims (Aghatise, 2006: 2).

3.2.2 Cyber Attack

All kinds of changes to programs, distortion, production, interruption, or destruction of data in cyber space are called cyber attacks. Cyber attacks can be classified as follows (Özçoban, 2014: 55):

i. Virus attacks with email attachments,

ii. Making computer systems that provide public services become overloaded and inoperable,

iii. Destroying the websites of states or commercial organizations for disinformation or propaganda,

iv. Unauthorized access to computer systems to obtain information.

Cyber attacks occur with two basic elements, which are attacks on data or attacks to control systems. To control systems, the attacks mostly focus on making a physical infrastructure unusable or misleading. Attacks in cyber space are referred to by various names according to the motivations, identities, and aims of the attackers. Actions carried out to create concern in society for political reasons by terrorist organizations or unidentified people can be called cyber terror; actions carried out in order to gain personal advantage or threaten social order and peace are called cyber crime. “Cyber war” refers to the fact that states/governments may carry a conflict between themselves into cyber space. The most common methodologies for conducting cyber attacks are as follows (Aslay, 2017: 25; Nasrat, 2015: 9):

i. Data Diddling: In this method, the wrong information is entered when entering data into the computer or changing the data using special methods. In some cases, records are deleted.

ii. Salami Techniques: Usually used in the banking sector. The last number or the last two digits of the value after a comma are transferred to another account and accumulated there by this methodology.

iii. Super Zapping: In this methodology, systems can be corrected in the case of a locked system with a failure. The methodology can be used for overcoming security controls. The security is disabled when this method is abused.

iv. Spyware: Hackers can access the system through the “backdoor” and change the system structure of the computer, and this methodology is called “spyware”.

v. Logic Bombs: A malicious code is inserted into a program. Logic bombs are often used to completely destroy information on targeted computers or networks, or to make them unusable.

vi. Malicious software: This is code prepared for a specific negative purpose, such as viruses.

vii. Chameleon: These software programs work like normal ones, but in the background the program copies usernames and passwords and sells or shares this information on other platforms.

viii. Phishing: Usually fake websites are used. For example, an end user who thinks that he has received an email from a bank or shopping site may answer the mail or follow the link in the mail, entering personal information, and his data can then be stolen.

ix. Spam: These are emails that are unwanted and disturbing. These mails are huge in size and have commercial purposes most of the time.

x. Scavenging: This is a methodology used to restore the deleted information of a computer.

3.2.3 Cyber Threats

Cyber threats can be defined as risks that have the potential to damage computer hardware and software systems. They can include virus software, information changing, or plagiarism. There is not a consensus definition of cyber threats, but by looking at the political and legal arrangements of various countries, a definition can be summarized here. There are differences of opinion about the subject and this also hampers an international joint effort in this regard. The lack of implementation standards for preventing cyber threats reduces the power of national administrations to cope with them. For example, Richard A. Clarke and Robert K. Knake say that cyber threats are the risk of cyber attacks of countries for damaging others' computers and administrative systems. Michael Hayden, who is the former president of the CIA, notes that cyber threats are the preconceived malicious actions for

deactivating the computer networks of a country or a company by another country, company, or person (Nasrat, 2015: 6).

The Oxford Dictionary defines a cyber threat as “the possibility of a malicious attempt to damage or disrupt a computer network or system” (Oxford Dictionary, 2018); the Australian Computer Society says that “threat is more closely identified with the actor or adversary attempting to gain access to a system. Or a threat might be identified by the damage being done, what is being stolen or the Tactics, Techniques and Procedures (TTP) being used” (ACS, 2016).

For a better understanding of cyber threats, their sources should also be defined, because in order to prevent cyber damages, first of all the actors behind the threat should be known. It must not be forgotten that in every case of threat there is a human element. Someone seeking his or her rights or someone taking unusual actions may be the “person behind the attack”, or sometimes a rivalry can cause such actions. Sometimes the threats can come from people who are trying to earn money easily. Organized crime groups, terrorists, business competitors, disgruntled insiders, or nation states or national governments can all be the starting point of a threat.

3.2.3.1 Cyber Threats Categorization

While cyber threats were named on their own at the time of their first release, they were now categorized and named because of increasing threats and similarities. At the same time, the categorization of attack types provides convenience in terms of defense and prevention methods and shapes the types of measures we will take.

3.2.3.1.1 Advanced Persistent Threat (APT)

An APT is an ongoing set of stealthy and hidden attack processes and threats designed to infiltrate a system or network. Multiple threat types (e.g., malware and phishing), as well as different attack vectors (e.g., email and social engineering), are often used.

3.2.3.2 Adware

Adware is a type of malicious software that installs or renders advertising on a computing system to generate revenue. Advertisements often appear as pop-ups in windows that the user is unable to close. Sometimes adware is designed with multiple objectives. For example, in addition to advertising, adware may include spyware that observes the user's computing activities without his knowledge, or the adware may include stolen certificates that deactivate the system's antivirus or antimalware protection. Adware can affect any computing system, including computers, tablets, and mobile phones.

3.2.3.3 Backdoor

Malware that targets a hidden entrance or method to bypass traditional security within a system, device, computer, or software.

3.2.3.4 Bot

An Internet-connected individual device within a botnet is called a bot. A bot is most often a computer, but a smartphone, tablet, or Internet of Things device (such as a router or Internet-connected refrigerator) can also be part of a botnet. A bot receives operational instructions from a command and control server, directly from the botmaster, or sometimes from other bots within the network.

3.2.3.5 Botnet

A botnet is a network of Internet-connected and malware-infected devices that have been co-opted by cyber criminals. It is used to distribute spam and malware, or to launch distributed denial-of-service attacks. Botnets can comprise as many as 500,000 to 1,000,000 devices and send up to 60 billion spam emails in a day. The term "botnet" derives from the combination of the words "roBOT NETwork". Botnets can be used for click-fraud, special event ticketing, online polls, and social media manipulation, as well as the distribution of spam and phishing emails.

3.2.3.6 Business Email Compromise (BEC)

BEC is a type of phishing attack intended to scam organizations out of money through the impersonation of executives. First, criminals gain access to a corporate

system through a spear-phishing attack or malware. The criminals then research the organization's vendors, the finance systems, and the executive's email style and schedule. Often when the executive is away, the criminals send a fake email from the executive to a targeted employee (usually in finance), with a request for an immediate wire transfer to a trusted vendor. However, the wire transfer is in actuality directed to an account controlled by a criminal group.

3.2.3.7 Distributed Denial-of-Service (DDoS) Attacks

Using the computers attached to a botnet, cybercriminals shut down—or deny service to—a victim's system users by overloading the computational resources of the website or system with data.

3.2.3.8 Exploit

Malware that takes advantage of a software vulnerability to gain access to a computer or system.

3.2.3.9 Keyloggers

With keylogging software, bots collect information related to a specific type of keyboard strokes, such as alpha-numeric/special character sequences associated with certain keywords, such as "bankofamerica.com" or "paypal.com". If the keylogger is running on thousands of computers connected to the botnet, then the cyber criminal has the ability to quickly harvest sensitive information.

3.2.3.10 Macro

A virus written in a macro language and distributed in a Microsoft Word or Excel file attachment.

3.2.3.11 Malware

A combination of the words "malicious" and "software", malware is specifically designed to harm a computer, a system, or data. It encompasses several types of malicious tools, including adware, ransomware, scareware, spyware, Trojans, viruses, and worms.

3.2.3.12 Man-in-the-Middle (MITM) Attack

MITM is an attack in which a cybercriminal inserts himself between two parties in a communication, with the intent of impersonating one or both parties to intercept, send, and receive sensitive or confidential data, such as bank account information, passwords, or documents.

3.2.3.13 Phishing

A homophone of the word "fishing", phishing is an attempt to entice a person into providing sensitive or confidential information that can be used or monetized by the phisher. In a phishing scam, cybercriminals distribute electronic content (email or online advertisements) to a series of victims, in which the content is specifically designed to trick the user into engaging in a specific activity, such as clicking a link or responding to the email. The victims, thinking the content is real, provide the phisher with personally sensitive information such as usernames, passwords, and banking, financial, and/or credit card details. Methods of phishing distribution include email, online advertising, and SMS.

2.2.3.14. Ransomware

A form of malware, ransomware limits or blocks users from accessing individual files or entire systems until a ransom is paid.

2.2.3.15. Rootkit

Malicious software that enables access to sections of the computer, software, or system that would normally not be accessible. Malware often contains rootkits to allow concealment by modifying the operating system so that the malware remains hidden from the user.

2.2.3.16 Sniffing

Bots can also be used to watch or "sniff" for specific types of text and data passing through a compromised machine, such as usernames and passwords. Sometimes if a machine is infected with malware from several different botnets, the machine can be

used to sniff packets from other botnet's messages, gather key information, and "steal" the botnet.

2.2.3.17 Spyware

Malicious software that spies on the computer user, capturing keystrokes, emails, and documents or even turning on the video camera. It is sometimes embedded in adware.

2.2.3.18 Steganography

Digital steganography is a method of concealing a file, message, image, or video within another file, message, image, or video. Bots use this technology by downloading seemingly innocuous image files that actually contain complex message streams sent by the C&C for use by the bot. The images can be stored on any compromised website or even image-sharing services. This makes detection of such downloads virtually indistinguishable from normal Internet browsing traffic.

2.2.3.19 Social Engineering

In the context of cyber crime, social engineering refers to using psychological manipulation to convince potential victims to engage in a type of activity (such as clicking on a malicious link or document) or divulging sensitive information (such as usernames and passwords).

2.2.3.20 Trojan

Derived from the ancient Greek tale of the Trojan Horse, in which soldiers hide inside a large wooden horse, in computer parlance a Trojan is a form of non-replicating malicious software that contains hidden functionality. A Trojan typically does not attempt to propagate or inject itself into other files.

2.2.3.21 Virus

A form of malicious software that infects a system or computer and damages or alters the data in the system.

2.2.3.22 Vishing

A combination of the words “voice” and “phishing”, vishing uses social engineering via a phone call to obtain personally sensitive information, such as bank account numbers, PINs, or credit card numbers. Typically, the victim receives a call with an automated message from someone claiming to represent a financial institution, Internet provider, or technology company. The message may ask the victim to enter an account number or pin. Once entered, the call redirects to an attacker via a voice-over-IP service, who then requests additional sensitive personal information.

2.2.3.23 Watering Hole

A type of attack in which the cyber criminal ascertains (usually through observation or guesswork) the websites most commonly frequented by a target individual or organization. The criminal then infects one or more of these websites with malware, with the targets eventually getting infected.

2.2.3.24 Worm

Malicious software designed to continually propagate itself, often using a computer network. May consume excessive system bandwidth as it propagates.

2.2.3.25 Zero-day Attack

A type of attack in which a cybercriminal leverages a system, software, or network vulnerability that is otherwise unknown to the public, cybersecurity professionals, and sometimes the software or system developers.

3.2.4 Cyber Terrorism

The definition of terrorism has expanded beyond the traditional areas of air, land, and sea; the cyber area can also be an environment for terrorism. The technological developments regarding computers, communication, and IT tools have caused this situation. Cyber terrorism can be defined as terrifying and damaging actions in the cyber environment that have political purposes. These actions can be undertaken by a person, group, or country against a group of people or institutions such as banks or

universities, government network systems, etc. These actions are done in order to panic governments or societies and block the systems for a period of time, damaging the systems and causing psychological harm and/or economic losses (Nasrat, 2015: 16).

The term "cyber terrorism" was first used in 1980 by Barry Collin, who defined it as actions done to realize physical terror actions or terror campaigns in the digital environment by damaging information systems, networks, or computer-based systems (Collin, 1997: 16). From the definition we can say that cyber terrorism constitutes harmful actions for creating panic in the cyber environment and for damaging systems. Here, however, we can also note that among these harmful actions, cyber terrorism can be conducted in order to attract supporters to an ideology in illegal ways. Terrorist groups in real life can use the Internet to reach people and penetrate into other communities such as groups of young people, national groups, etc. Furthermore, the FBI says that the actions for stealing and transferring money to illegal groups by using Internet technologies and hacking systems can also be thought of as cyber terrorism (Özcan, 2002: 309).

In any kind of terrorist action there must be an ideological purpose. Lawrence Brown defines cyber terrorism as "using computers for ideological purposes as a gun". Ronald Dick, the former director of the FBI's National Infrastructure Protection Center, thinks that cyber terrorism is a new kind of terrorism in which it is hard to predict what will be done and hard to find the assailant. For a better understanding, it is necessary to explain the unique aspects of cyber terrorism (Nasrat, 2015: 21):

i. Identification of perpetrators is harder than in other kinds of terrorism.

ii. There are many targets and various target types in cyber terrorism. Cyber terrorists can choose many targets, such as governments, individuals, utilities, private airlines, etc.

iii. Cyber terrorism acts are independent of physical conditions.

iv. Terror groups can move to the top of the agenda with cyber terrorism attacks and can become popular in a very short time.

3.2.5 Cyber War

The mechanism of economic damage or defeat is called cyber warfare. Cyber war simply means damaging the enemy's communication systems and computer networks via illegal digital operations in cyber space. However, from this definition, it is difficult to distinguish between cyber warfare and cyber terror. For a more realistic definition, it is necessary to include more specific details. According to the Informatics Association of Turkey (Türkiye Bilişim Derneği: TBD), cyber war activities are conducted to support policy and military objectives in times of peace, crisis, and war. These activities are carried out for the purpose of preventing, destroying, disrupting, and exploiting the information infrastructure, systems, and processes of the enemy. Like traditional war, the goal of a cyber war is to assert an actor's dominance (a country, institution, group of people, etc.) by using cyber methodologies. Here the purpose is not only to terrify; it is also to show power to others. As in the concept of traditional war, in a cyber war the involved parties should produce propaganda, use digital weapons, and provide intelligence (Ustaoğlu, 2015: 6).

3.3 Cyber Security Intelligence

The cyber world is expanding day by day, and from individuals to governments all parts of society can collect and save data by using new-generation technological devices. The saving and producing of information particularly requires much protection for a continuous information security system. Daily life is intertwined with the Internet, and the capturing of user accounts of individuals or private companies and government agencies is frequently experienced over the Internet. Cyber security intelligence is a system of different methodologies for saving and searching information that is important or could damage national interests (Conti et al., 2018: 2).

The Secureworks Counter Threat Unit has an analysis group that has been publishing threat analyses since 2005. The working group uses threat visibility across thousands of customer networks to identify emerging threats, and security communities, agencies of governments, investigators' studies, and malware samples are just a few

of their resources. The group says that for the best security intelligence, the following questions should be answered during a threat survey (Secureworks, 2018):

i. What does the threat mean?

ii. How do you resist it?

iii. What action should you take?

Answering these questions would help determine who is behind cyber terror or threats and what they want. The next step of the terrorist action can also be guessed and prevented. Technological developments have caused new kinds of cyber risks but these developments can also be used for a new age of cyber security intelligence methodologies. It is difficult to provide a clear definition of cyber intelligence. The reason for this is the use of different methods for cyber intelligence and the search for different information in each intelligence system. However, it should be said that every kind of cyber intelligence methodology is based on high technology. The usage of high technology saves time and costs. In addition, labor and capital advantages are also achieved. Information is obtained more clearly by technological follow-up. Here the following cyber intelligence methodologies can be listed:

i. Social Engineering:

It is not possible to provide information and system security and to protect data with only technological solutions in a cyber environment (Gündüz and Daş, 2016: 11). The "art" of influencing people to divulge sensitive information is known as social engineering. There are various definitions of social engineering and also a number of different models of social engineering attacks. In brief, social engineering means gathering information about the target person or institution by using human relations or people's carelessness (Mouton et al., 2016: 187).

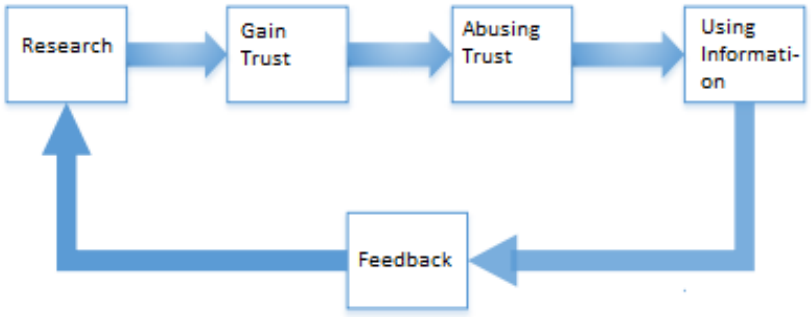


Figure 3.1 Social Engineering Process(Mounton et al., 2016: 187)

The purpose of social engineering is to collect data about the target person's or institution's structure, the structure of the corporate network of the target, personal information of the employees/managers, passwords, and all other kinds of materials that can be used for a cyber attack. Persuasion and influence methods are used in social engineering and thus information is obtained (Özçoban, 2014: 76).

ii. Spywares:

Spywares are software programs that send data to certain servers outside of the users' control and permission by using Trojan horses, rootkits, keyboard listeners, etc. With such software, all data on the computer can be stolen without the user's knowledge. In some countries, governments or companies introduce software for public use and they can place spyware in such software. The Prosecution Management Information System (PROMIS) can be shown as an example. This program was alerting users' about their expenses but at the same time it had a Trojan horse and was collecting data from the users. Many countries such as Egypt, Pakistan, and Syria bought information about individuals via this spyware system (Özçoban, 2014: 79).

In brief, spyware is a silent program that runs in the background, collects data, and saves the data and/or sends data to the owner of the software. By collecting such data, the personal information of individuals, their purchasing and consumption habits, and their preferences can be known. Their communications can also be monitored. By doing this, threats or terror actions can be prevented, but spyware can also be used to abuse or manipulate people. For example, by learning details of customers' preferences, retail marketing would be easier.

iii. Social Media:

Social media usage is improving every day and new social media websites are being introduced each day, as well. The huge amount of data generated on social media websites is like a source of treasure for research and analysis (Savaş and Topaloğlu, 2015: 51). Social media platforms are the best places for cyber security intelligence research because on these platforms people are sharing who they are, their jobs, and what they do in daily life. Beyond this, people on social media may share their ideas about terrorist groups, governments, or any other political situations. Using social media, such information can be collected about a person, people, governments, or any group (Agnihotri et al., 2013: 335).

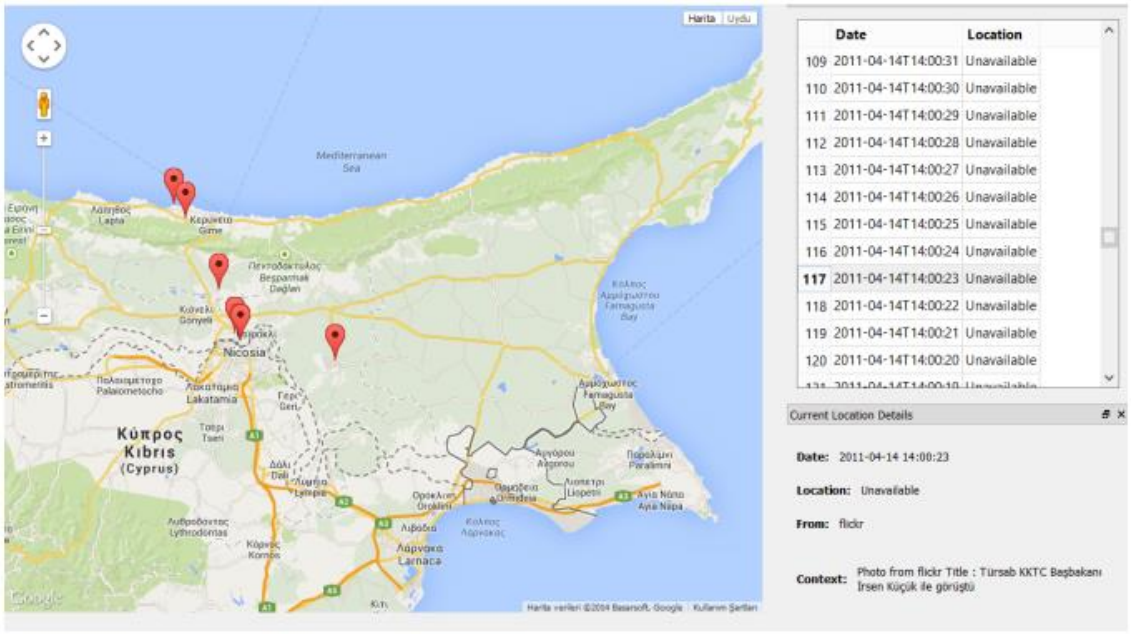


Figure 3.2 Determining the Positions of Senior State Executives with Their Photographs (Karaman and Çatalkaya, 2014)

Social media platforms also provide information about the cultural structure of a group of people or an individual. For this reason, companies are always active on social media platforms because they use this information to gain more sales (Savaş and Topaloğlu, 2015: 54).

The founder of WikiLeaks, Julian Assange, says that on social media platforms intelligence researchers can find much more data than is immediately apparent. For example, in a photo, the place, building specifications, weather, street names, etc. can be seen. From a photo, a stranger can determine the address of a house or any other details about the owner of the photo. Messages on social media can be hacked, or when a friend is added to a profile, the information about any other person who has befriended that profile can be seen. Furthermore, by sharing things such as videos or photos, other people can be reached who do not have a profile. Data collected by Facebook are compiled by all intelligence agencies (Sabah, 2011).

As seen from Figure 3.2 shared photos can be used to understand the location of an individual or group. This figure shows an analysis of the correct locations of a state official from his shared photos on Twitter.

iv. Websites:

A variety of services provided on the Internet (email, storage, messaging, etc.) are free to the users and this seems to be an advantage for individuals. However, on the other hand, these services can be thought of as "information libraries". It must be asked why these services are free and how their quality is increasing day by day. Özçoban notes that free file storage and web space sites, free programs, and free web-based virus scanning sites are among the tools used to obtain cyber intelligence (Özçoban, 2014: 82).

v. Search Engines:

Since the second half of the 20th century, the information revolution has focused more on data collection, storage, analysis, and transformation of information for use. A search engine is a query and retrieval mechanism that interrogates each of the records of information that has come to a conclusion, performs the necessary actions for the acceptability of a query, and ensures that the captured data provide high performance. A search engine is a mechanism used to search for content on the Internet. It consists of three components: a web robot, search index, and user

interface. The search results are often given as a list of frequently clicked web pages (Yurdakul and Bat, 2011: 47).



Figure 3.3 Search Engine – Legal Google Hack Style (Karaman and Çatalkaya, 2014)

Search engines are one of the best ways to perform intelligence actions. Today, an individual can reach much information about a person or a place by using search engines. It is possible to reach the results by result-oriented filtering by entering various parameters in many programs that collect automatic information from the internet.

3.3.1 CyberTwitter

Various informal sources such as blogs, developer forums, chat rooms, and social media platforms like Twitter provide information related to security vulnerabilities, threats, and attacks. A huge amount of information is published by these sources on a daily basis, making it nearly impossible for a human analyst to manually comb it all. As was seen above, there are many ways to approach security intelligence in the digital environment. These are sometimes frightening, but when it comes to terror, threats, or cyber wars, monitoring people is necessary for the security of government systems or society. For this reason, engineers and researchers are trying to find new solutions for intelligence technologies.

CyberTwitter can be defined as a program for researching social media in real time and defining the risks and hazardous communications. CyberTwitter is a system to

discover and analyze cyber security intelligence on Twitter and serve as an OSINT source. While the program is running, it analyzes tweets and finds the threats. It starts by collecting the data from Twitter, checks the tweets, and picks the ones that are about an attack. With this program, it is possible to identify, tag, and extract various real-world conceptual entities related to cyber security vulnerabilities, such as the means of an attack, consequences of an attack, or the affected software, hardware, vendors, etc. using a security vulnerability concept extractor (SVCE) (Mittal et al., 2016).



Figure 3.4 CyberTwitter (Mittal et al., 2016)

Here, for a better understanding, the concept of OSINT, introduced in Section 1.3, must be defined further. OSINT comprises intelligence gathered from publicly available overt sources such as newspapers, magazines, social networking sites, video sharing sites, wikis, blogs, etc. In the cyber security domain, information available through OSINT can complement data obtained through traditional security systems and monitoring tools like an intrusion detection and prevention system (IDPS). CyberTwitter begins by collecting relevant tweets by querying the Twitter API. The tweet collection module collects, cleans, and stores tweets returned by the API. Every tweet is further processed by the SVCE (Mittal et al., 2016).

CHAPTER 4

ARCHITECTURE

4.1 System Design

The architecture of the study is shown below, which contains default systems and a library.

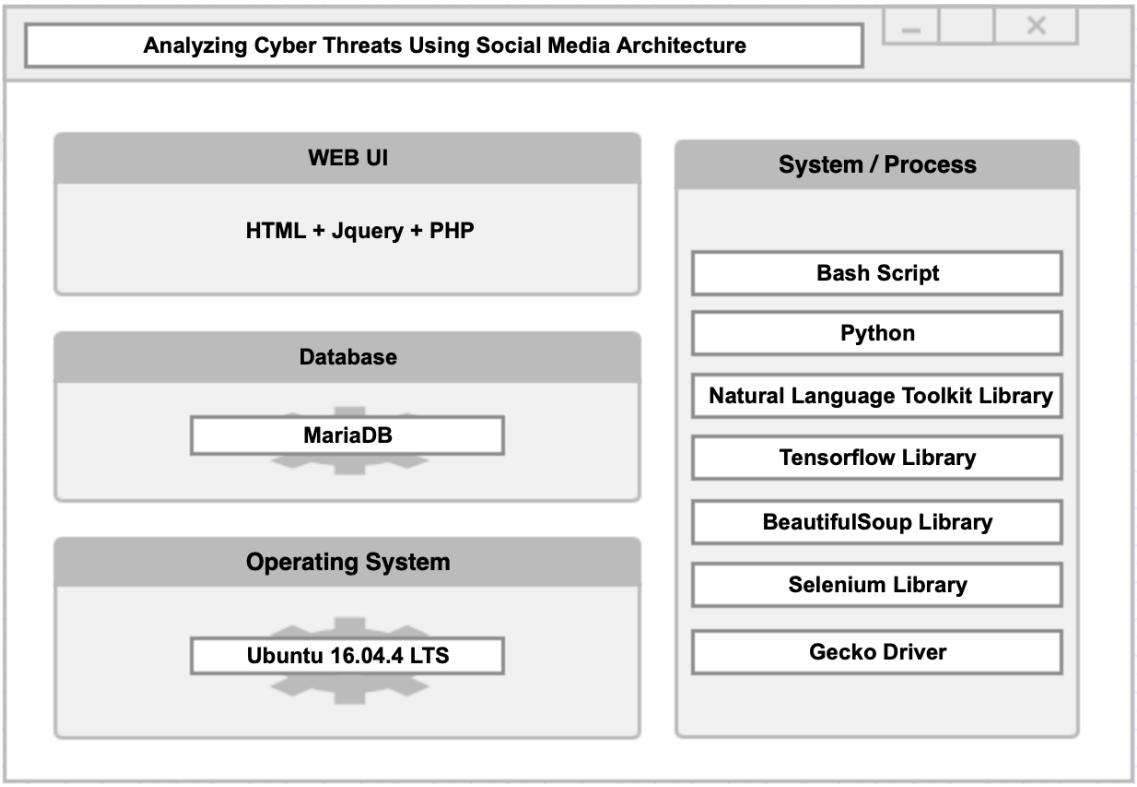


Figure 4.1 Architecture of the Study

The study has Web UI for easy application for users because the system has different scripts and many of them need to work in orchestration. Web UI takes a parameter from the input box and then starts interpretation with serialization with this parameter, such as figures and codes. First of all, the user enters a word, such as zero-day, and then clicks a search button. The Web UI call system procedures work with PHP and Python codes. The codes can obtain some tweets and store them in MariaDB, working on the Ubuntu Operating System. Other system and process tools include Python and Bash Script, other libraries, and the driver.

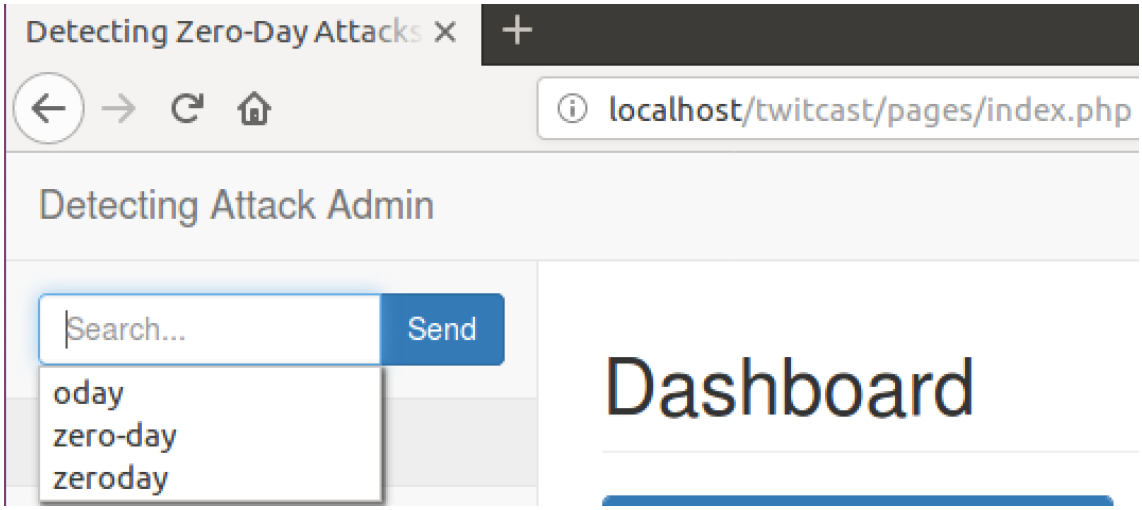


Figure 4.2 Input Parameter

```
<div class="navbar-default sidebar" role="navigation">
      <div class="sidebar-nav navbar-collapse">


          <ul class="nav" id="side-menu">


              <li class="sidebar-search">
              <form class="form-horizontal" role="form" method="post" action="searchword.php">
                  <div class="input-group custom-search-form">
                      <input type="text" class="form-control" name="formcontrol" placeholder="Search...">
                      <span class="input-group-btn">
                      <input id="submit" name="submit" type="submit" value="Send" class="btn btn-primary">
                      <!--
                      <button class="btn btn-default" type="button" id="submit"  value="Send">
                          <i class="fa fa-search"></i>
                      </button>
                      -->
                  </span>
                  </div>
              </form>
                  <!-- /input-group -->
```

Figure 4.3 Input Parameter HTML & PHP Form Code

```
root@ubuntu: /var/www/html/twitcast
root@ubuntu: /var/www/html/twitcast 170x54
<?php

$formcontrol = $_POST["formcontrol"];

$old_path = getcwd();
chdir('/mnt/hgfs/Shared/twitter2/');
//$command = escapeshellcmd('python tSearchAndInsert.py $formcontrol 2 > log.txt 2>&1');
//$output = shell_exec($command);

$cmd = "python tSearchAndInsert.py ".$formcontrol." 1 > log.txt 2>&1";
shell_exec($cmd);

chdir($old_path);



header("Location: index.php?id=$formcontrol");
?>
```

Figure 4.4 Search Word Parameter HTML & PHP Form Code

4.2 Technical Architecture

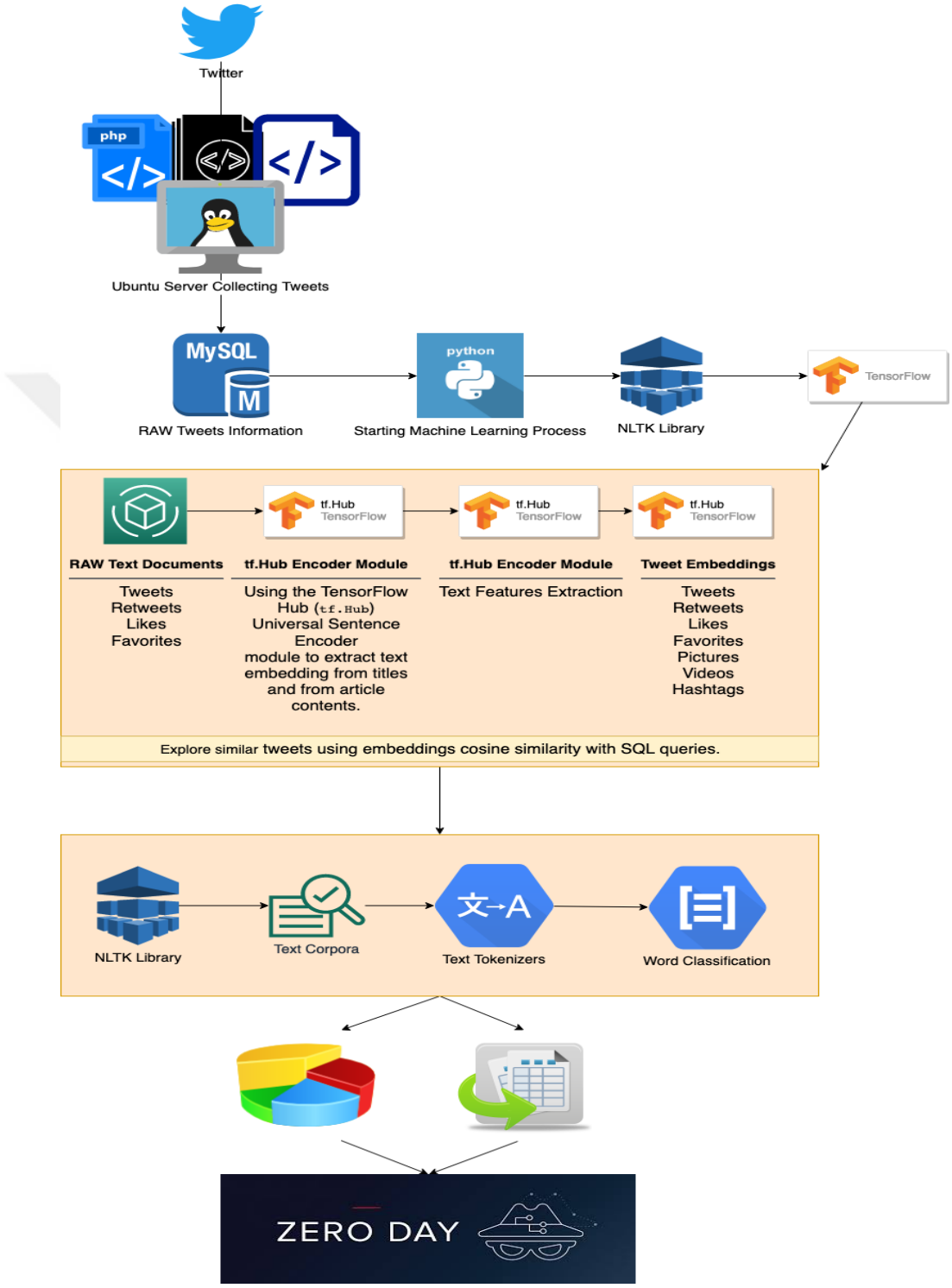


Figure 4.5 Technical Architecture Flow Diagram

4.3 TensorFlow Machine Learning Library

TensorFlow can be described as a library that is used for researching and producing and it should be noted that it is an open-source machine learning system. It offers APIs for both beginners and professionals for developing on desktop, mobile, web, and cloud.

TensorFlow systems were created by the Google Brain Team and constitute a library for numerical computation and large-scale machine learning. TensorFlow bundles together a slew of machine learning and deep learning (aka neural networking) models and algorithms and makes them useful by way of a common metaphor. It uses Python to provide a convenient frontend API for building applications with the framework, while executing those applications in high-performance C++ (TensorFlow, 2019).

In this work, the TensorFlow libraries read and parse Twitter's raw text tweets. It uses simplicity and extensibility functions using the tf.Hub module, the text embedding module, to parse raw Twitter data. However, in tf.Transform, the preprocess_fn function runs in a hidden TensorFlow context where you can call all TensorFlow operations (including calling a tf.Hub module) without performing all the detailed steps.

TensorFlow works on vectors, converting all the tweets it examines into vectors for learning and comparing tweets. For raw data from Twitter such as object or speech recognition like tweets, we know that all the information needed to successfully perform the task is encoded in the data (because people can perform these tasks from raw data). However, natural language processing systems traditionally see words as separate atomic symbols and they can therefore be represented as "cat", Id537, and "dog", Id143. These encodings are optional and do not provide useful information to the system about the relationships that may exist between individual symbols. This means that the model can barely benefit from what it has learned about "cats" when processing data about "dogs" (both animals, four legs, pets, etc.). Showing words as unique, discrete identities also leads to a lack of data, and it often means that we may

need more data to successfully train statistical models. Using vector representations can overcome some of these obstacles.

TensorFlow neural probabilistic language models are generally trained using the maximum likelihood (ML) principle to find maximum similarity with the next word.

We will designate historic words with “H” and target words with “Wt”.

$$P(w_t|h) = \text{softmax}(\text{score}(w_t, h)) = \frac{\exp\{\text{score}(w_t, h)\}}{\sum_{\text{Word w' in Vocab}} \exp\{\text{score}(w', h)\}}$$

Figure 4.6 Equation of Softmax From Tensorflow Library

This provides a suitably normalized probabilistic model for language modeling.

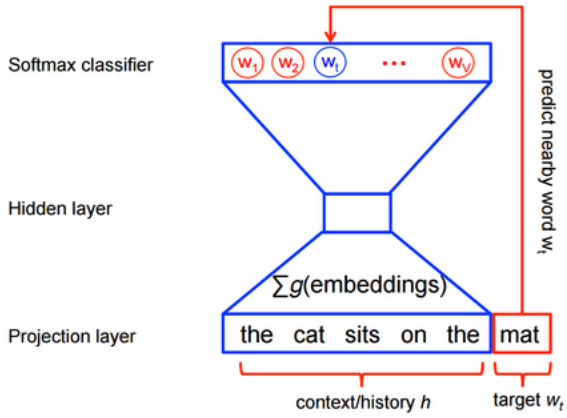


Figure 4.7 Softmax Classifier Logical Algorithm Schema

However, this is very expensive because we need to calculate and normalize each probability using the score for other words in the current context at each training step.

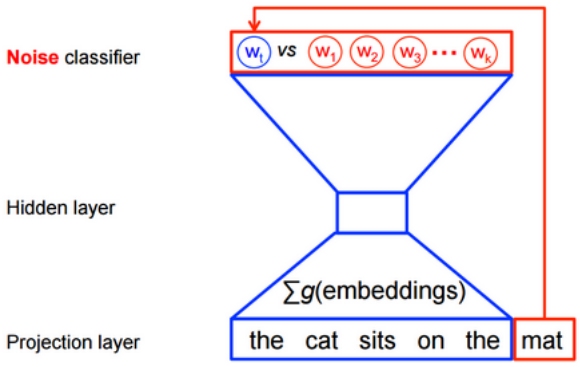


Figure 4.8 Noise Classifier Logical Algorithm Schema

A skip-gram model is faster than the SoftMax classifier, and a skip-gram model works like this:

Example Tweet: "Security researchers have found a zero-day vulnerability in a popular building on KDE Desktop"

Normalization Context: ([Security, have], researchers), ([researchers, found], have), ([have, found], zero-day), ...

New Dataset Becomes: (researchers, security), (researchers, have), (have, researchers), (have, found), (zero-day, have), (zero-day, found), ...

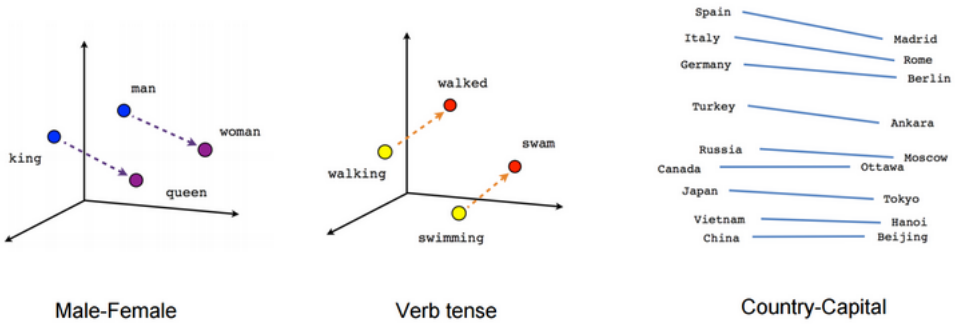


Figure 4.9 Example of Tensorflow Successful Result

Examples of TensorFlow vector dimensionality include male-female, verb-tense, and country-capital. In this study, vector dimensionality is as follows: ZeroDay-Vulnerability, 0day-Vulnerability, Zero-Day-Vulnerability.

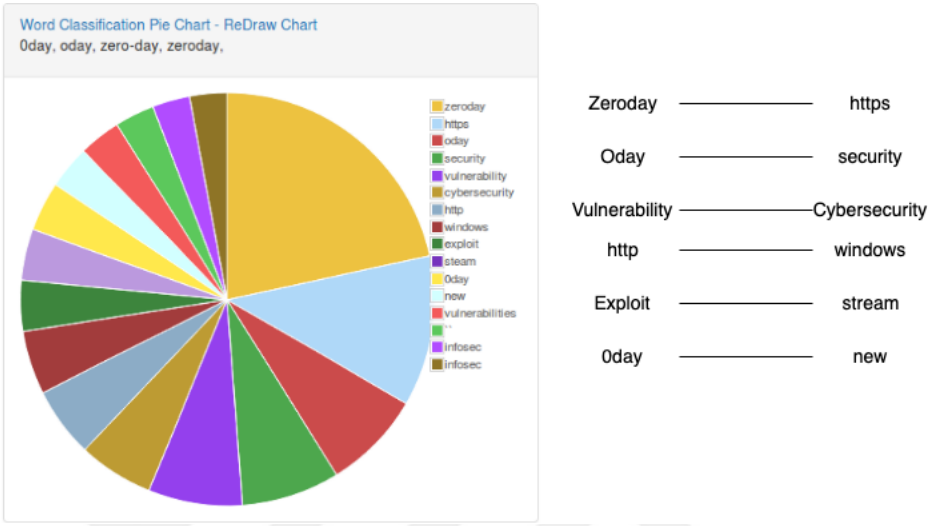


Figure 4.10 TensorFlow Vector Dimensionality for Zero-Day

An example is given of a tweet that is the most valuable tweet found by the program. TensorFlow creates vectors such as these:

id	Search Word	User Name	Tweet	Date	Reply	ReTweet	Favori	wc	assurance
19	ZeroDay	SilentStormSec	"The popular #Steam game client for #Windows has a #zeroday privilege escalation vulnerability that can allow an attacker with limited permissions to run a program as an administrator." #cybersecurity #infosec #cyberthreats #cyberdefense #cybersecurity https://www.bleepingcomp	Aug 8	0	2	1	41	3

Figure 4.11 Most Valuable Tweet Found from Program

Sentence:

"The popular #Steam game client for #Windows has a #zeroday privilege escalation vulnerability that can allow an attacker with limited permissions to run a program as an administrator." #cybersecurity #infosec #cyberthreats #cyberdefense #cybersecurity https://www.bleepingcomp.com

Vector:

[['"the', 'popular', '#steam', 'game', 'client', 'for', '#windows', 'has', 'a', '#zeroday', 'privilege', 'escalation', 'vulnerability', 'that', 'can', 'allow', 'an', 'attacker', 'with', 'limited', 'permissions', 'to', 'run', 'a', 'program', 'as', 'an', 'administrator'], ['"', '#cybersecurity', '#infosec', '#cyberthreats', '#cyberdefense', '#cybersecurity', 'https://www'], ['bleepingcomp']]

[['"the', 'popular'], ['"the', '#steam'], ['popular', '"the'], ['popular', '#steam'], ['popular', 'game'], ['#steam', '"the'], ['#steam', 'popular'], ['#steam', 'game'], ['#steam', 'client'], ['game', 'popular'], ['game', '#steam'], ['game', 'client'], ['game', 'for'], ['client', '#steam'], ['client', 'game'], ['client', 'for'], ['client', '#windows'], ['for', 'game'], ['for', 'client'], ['for', '#windows'], ['for', 'has'], ['#windows', 'client'], ['#windows', 'for'], ['#windows', 'has'], ['#windows', 'a'], ['has', 'for'], ['has', '#windows'], ['has', 'a'], ['has', '#zeroday'], ['a', '#windows'], ['a', 'has'], ['a', '#zeroday'], ['a', 'privilege'], ['#zeroday', 'has'], ['#zeroday', 'a'], ['#zeroday', 'privilege'], ['#zeroday', 'escalation'], ['privilege', 'a'], ['privilege', '#zeroday'], ['privilege', 'escalation'], ['privilege', 'vulnerability'], ['escalation', '#zeroday'], ['escalation', 'privilege'], ['escalation', 'vulnerability'], ['escalation', 'that'], ['vulnerability', 'privilege'], ['vulnerability', 'escalation'], ['vulnerability', 'that'], ['vulnerability', 'can'], ['that', 'escalation'], ['that', 'vulnerability'], ['that', 'can'], ['that', 'allow'], ['can', 'vulnerability'], ['can', 'that'], ['can', 'allow'], ['can', 'an'], ['allow', 'that'], ['allow', 'can'], ['allow', 'an'], ['allow', 'attacker'], ['an', 'can'], ['an', 'allow'], ['an', 'attacker'], ['an', 'with'], ['attacker', 'allow'], ['attacker', 'an'], ['attacker', 'with'], ['attacker', 'limited'], ['with', 'an'], ['with', 'attacker'], ['with', 'limited'], ['with', 'permissions'], ['limited', 'attacker'], ['limited', 'with'], ['limited', 'permissions'], ['limited', 'to'], ['permissions', 'with'], ['permissions', 'limited'],

['permissions', 'to'], ['permissions', 'run'], ['to', 'limited'], ['to', 'permissions'], ['to', 'run'], ['to', 'a'], ['run', 'permissions'], ['run', 'to'], ['run', 'a'], ['run', 'program'], ['a', 'to'], ['a', 'run'], ['a', 'program'], ['a', 'as'], ['program', 'run'], ['program', 'a'], ['program', 'as'], ['program', 'an'], ['as', 'a'], ['as', 'program'], ['as', 'an'], ['as', 'administrator'], ['an', 'program'], ['an', 'as'], ['an', 'administrator'], ['administrator', 'as'], ['administrator', 'an'], ["", '#cybersecurity'], ["", '#infosec'], ['#cybersecurity', ""], ['#cybersecurity', '#infosec'], ['#cybersecurity', '#cyberthreats'], ['#infosec', ""], ['#infosec', '#cybersecurity'], ['#infosec', '#cyberthreats'], ['#infosec', '#cyberdefense'], ['#cyberthreats', '#cybersecurity'], ['#cyberthreats', '#infosec'], ['#cyberthreats', '#cyberdefense'], ['#cyberthreats', '#cybersecurity'], ['#cyberdefense', '#infosec'], ['#cyberdefense', '#cyberthreats'], ['#cyberdefense', '#cybersecurity'], ['#cyberdefense', 'https://www'], ['#cybersecurity', '#cyberthreats'], ['#cybersecurity', '#cyberdefense'], ['#cybersecurity', 'https://www'], ['https://www', '#cyberdefense'], ['https://www', '#cybersecurity']]

From the command line screenshot:



Figure 4.12 TensorFlow Vector Dimensionality Debug Example

4.4 NLTK Natural Language Toolkit

NLTK can be defined as a leading platform for building Python programs to work with human language information. It provides easy-to-use interfaces to over 50 corpora and lexical resources such as WordNet, along with a suite of text processing libraries for classification, tokenization, stemming, tagging, parsing, and semantic reasoning, with wrappers for industrial-strength NLP libraries and an active discussion forum.

NLTK is a powerful text analytics, NLP, and text mining library so we use the NLTK library for text analysis operations, providing a set of diverse natural language algorithms.

It is open-source and easy to use. NLTK consists of the most common algorithms, such as tokenizing, part-of-speech tagging, stemming, sentiment analysis, topic segmentation, and named entity recognition. This library processes tweets to analyze, preprocess, and understand the written text from raw Twitter data.

To give a real NLTK example for tweet processing, first all the raw data contain things like different languages and different symbols. After the raw data have been processed, the NLTK Tokenizer module translates them into English and they can be processed. As a final step, classification is performed using word classification.

Raw Tweet example:

Zoom users on Macs: please take steps at the bottom of the article to mitigate this gnarly zero-day exploit.

#ZyXEL P660HN-T1A 7.3.15.0 CVE-2017-18374 - Default Credentials Weak Authenticated\n\nhttps://0day.city/0day/CVE-2017-18374.html …\n\n#0day #Zeroday

احلى اغنية لالك هي وندم

الحب للشجعان ياصديقي اما البسكلتات تزوجهم امهاتهم

2القاهرة_حريق#الاورام _معهد#n\ونعمه بطيب جنتك n\اللهم ارحم كل من مات حريقا

@AssalaOfficial @oday_official\n\n#أيمن على اغنية _عدي#تعليق الاصالة الجديدة

حياته روتينيه جداً وخلاص يا اخو

طبيب سعودي يجهز عيادة متنقلة ويقودها شخصياً من جازان إلى المشاعر المقدسةn\النا_شرف_الحجاج_خدمة#

نسأل الله لنا ولكم الصحة والعافية والبركة في العمر n\لا يقدر الله شرًا لا خير فيه فإن حصل لنا أمر مما لا نتمناه فلنقل لعله خير ترجع بسلامه ونعم الأخت n\وإنشاء الله يكون غيابكم خير لكم وانتمن لكم السعادة وراحة البالn\والسعادة في الدنيا والآخرة

السعادة لقلبكn\ما تعودنا منكم علي كل هالحزان

من (أسوأ)ليس :؟ قال ..واكتشفت أنه ليس هناك حساب ولا رب بعد كل ما عملت (مت)ما هو شعورك لو :ملحد يحدث متدين حكي_طخ#n\شعورك إذا كان هناك رب و حساب

وأمتنا علي طاعتك وحسن n\وحقق أمانينا اللهم زذنا قربا الليك n\يتمني تحقيقها فاللهم أستجب لنا n\ يارب في قلب كل منا أمنية صباح معطر بذكر الله n\تطمئن القلوب n\صباح جميل عامر بذكر اللهn\عبادتك يارب

今日はZERODAYを聴きにARTHOUSEへ！\n\nガッツリパワーアップしてる！！\nまとまりつつもそれぞれの特色が出てきて聴き応えが増してるなー。\n\nやっぱスゲーわ！！！

旅立つ前のラストZERODAY観に...\n\n今まで彼らの音楽に救われて、いっぱい助けられて来ました。\n最後って思うとライブに向かう電車の中で、わくわくより寂しさが勝って、着きたくないなって思ったりした。\n\nでも、本当に忘れられない特別過ぎる夜で、今までで一番かっこいいライブでした。\n\nありがとう

明日です。\n\n8/7(水)ARTHOUSE\nLegecko\nTAMIW\nLightning Swells Forever\nクロロカンナ\nZERODAY\nstomachs

本日7日は、奈良からLegeckoを迎え、TAMIW / Lightning Swells Forever / クロロカンナ / ZERODAY / stomachsの超濃厚な注目メンツ全6組が出演！是非お越しくださいませ！開演18時

死ぬほど何と無くですけどわかるような気がしますよろしくお願いします！

知らんバンドやったけど「一番のファンの子が遠くに行くのでラストはその子のために歌います！」ってゆってるのどちゃくそにエモすぎたし一緒に写ってる動画久美やったら絶対欲しいから撮ってあげたくなって勝手に撮りましたm(__)mファンの子に届け！\nホーリーナイトて曲かっこよかった！\n#ZERODAY

```
ecamalan@ubuntu: /mnt/hgfs/Shared/twitter2 123x24
Who wants a Nike Mercurial Football Boot? UK size 11.\n\nI'm giving it out
WMNS NIKE AIR MAX 98 “PURPLE / RACER PINK” $95.00 https://sneakersteal.com/2019/08/18/wmns-nike-air-max-98-purple-racer-pin
k-95-00/ …
WMNS NIKE REACT ELEMENT 55 $62.38 FREE SHIPPING https://sneakersteal.com/2019/08/24/wmns-nike-react-element-55-62-38-free-s
hipping/ …
Working on those #chickenlegs #legday #gymmotivation #SundayMotivation #SundayMorning #workout #tattoo #adidas #freeballing
 #bulgegay #bulge #underwearbulge #vpl #fetish #gym #SocialistSunday #gayuk pic.twitter.com/zj0QBUwsiA
Wow. The adidas Ultra Boost 1.0 for the @UWAthletics is sick. Find out how to get these on 8/31 https://snkrne.ws/328s9cQ
Y’all ever realize how affective @Nike’s “Just Do It” can be?
Yeah, Jump Out boys, that's Nike boys, hoppin' out coupes\nThis shit way too big, when we pull up give me the loot\n(Gimme
the loot!) pic.twitter.com/oEC6LSUklH
Yeezy did It first.. Nike hold this L
Yes or No? Adidas Spezial x Liam Gallagher
Yess!!!  my uncle did that!  #Nike #Tonga #MMT
Yesterday a guy noticed my Adidas socks when I was having a piss. He asked me if they were used to which I reply that yes a
nd invited him to have a sniff. It was so hot.
yohan wearing adidas pants, and the saga continues \n\nhello @adidas , pls make him as your endorser  #김요한
You are now to @Nike Air Monarchs what @DelReid is to cargos. Where’s your endorsement deal?
#youareofficiallyoldif you wore these Nike classics as a kid…and also now
You got to earn your stripes or you just another dude wearing adidas
嬉しすぎて嬉しいww\nすごい嬉しいのが伝わってくるよw\n\nだってめちゃくちゃ好き！！\n綺麗だしちょっぴりえっちぃし、やばい！
 【話題記事】「ナイキ」 × 「サカイ」から全11型のコラボコレクション　キービジュアルに大坂なおみら起用\nhttps://www.wwdjapan.c
om/articles/912709  \n#NIKE #SACAI
ecamalan@ubuntu:/mnt/hgfs/Shared/twitter2$
```

Figure 4.13 Raw Twitter Data

```
ecamalan@ubuntu: /mnt/hgfs/Shared/twitter2 123x23
# -*- coding: utf-8 -*-
from __future__ import unicode_literals
from __future__ import print_function

import sys
import codecs
import nltk

nltk.data.path.append("/home/ecamalan/nltk_data/")

from nltk.corpus import stopwords

# USAGE: python freqDist.py result.txt
default_stopwords = set(nltk.corpus.stopwords.words('english'))

#stopwords_file = '/root/nltk_data/corpora/stopwords/english'
stopwords_file = '/home/ecamalan/nltk_data/corpora/stopwords/english'
custom_stopwords = set(codecs.open(stopwords_file, 'r', 'utf-8').read().splitlines())

all_stopwords = default_stopwords | custom_stopwords

input_file = sys.argv[1]
                                                                                1,1           Top
```

Figure 4.14 NLTK Tokenizer Codes

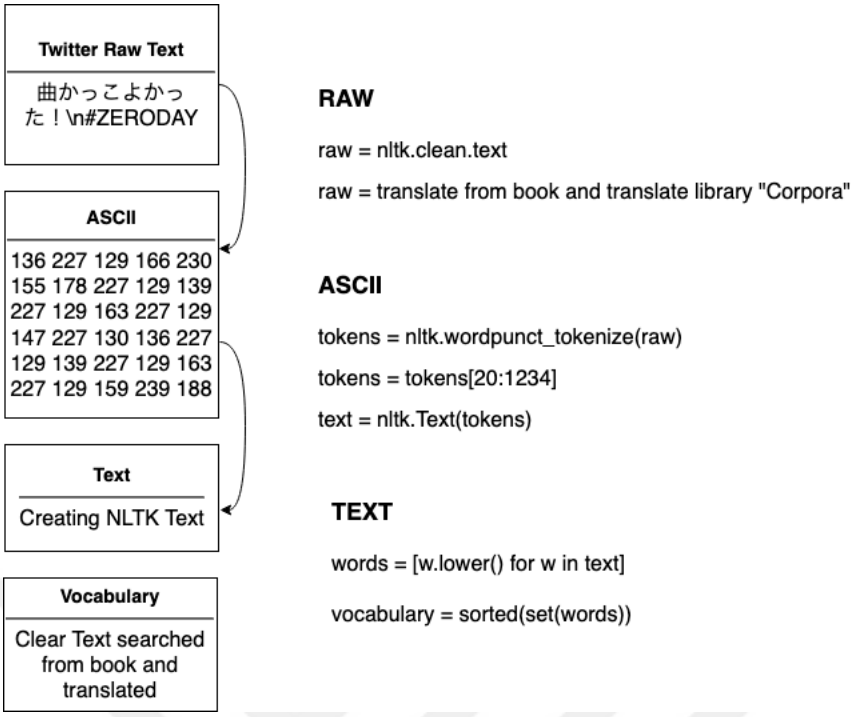


Figure 4.15 NLTK Clean Text Process

The next step involves word classification and frequency distance with NLTK modules. Tweet classification is one of the most important markers for zero-day vulnerability research tools because there are many tweets and most of them are alike, but a clever classification can change a lot and be more decisive.

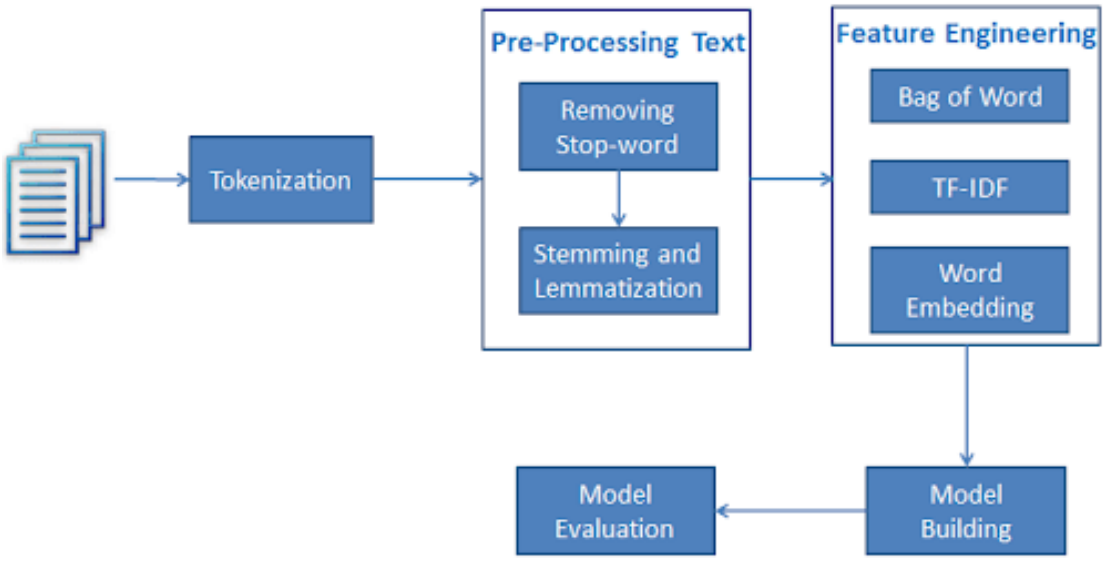


Figure 4.16 NLTK Word Classification Architecture

CHAPTER 5

AN APPLICATION ON TWITTER

5.1 Importance of the Study

The Internet is a very big world and every second data are being transferred from one user to another. It is not possible to follow this transfer of information by people watching and/or reading it. For this reason, there is continuous work performed on intelligence software all around the world to identify risky text and to prevent possible attacks. As seen from the literature review, there are software programs available for data collection and identification of threats, such as CyberTwitter. However, these programs use OSINT systems. In this study, codes have been written to search the information in data collected from Twitter, to check the vulnerabilities and also to become a source as OSINT. In the case of Turkey, it would be a domestic product and could be developed and sold.

5.2 Purpose of the Study

The purpose of the study is to determine threat risks and monitor the data of Twitter, pick the tweets shared that are about an attack such as zero-day, and prevent them. For this, codes are written and tested.

5.3 Hypotheses

The hypothesis of this study is that as soon as people find weaknesses and zero-day threats, they try to show them to others on social media via the Internet. This study seeks to ensure that measures are taken on social media by first identifying the weaknesses that people have found on the first day and informing them of their concerns. An application example of this study on Twitter is shown below in Figure 5.1.

5.4 Environment and Sample

Social media is a public information environment for this study, so this study uses one of the most popular platforms of social media: Twitter. This research aims to develop the collection of information from social media and engage in an inspection of it with neural language and word classification learning.

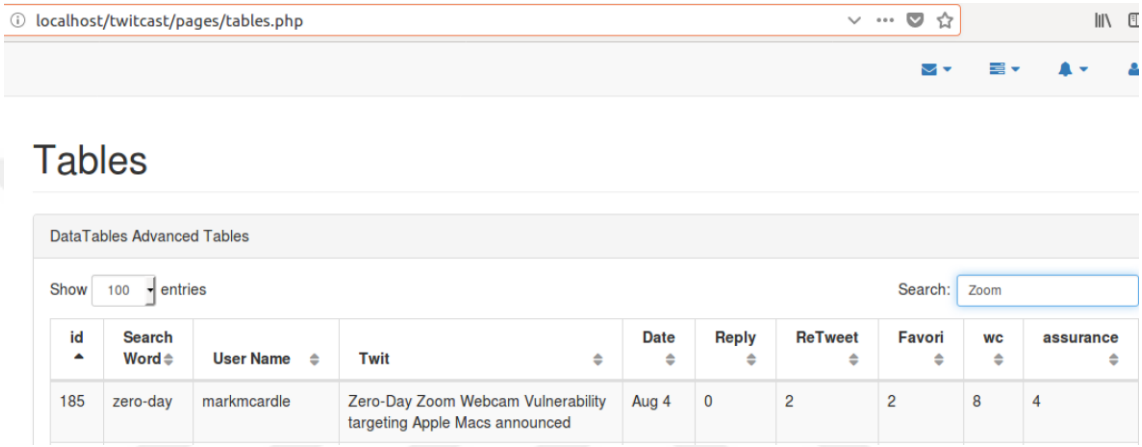


Figure 5.1 Tables Shown by the Software



Figure 5.2 Zero-Day Tweet Example (**Twitter, 2018**)

As seen in the above figures, Jonathan Leitschuh had written a tweet about finding a tweet that included word “zero-day” and he said that the tweet had existed for more than 90 days. However, as seen here, there was no address provided to the mentioned tweet. With the program presented here, though, the detected word and the account that shared that word can be detected.

These two figures show that if somebody says that he or she found a vulnerability on the Zoom application and this is still an open threat, then this vulnerability is also a zero-day vulnerability from the perspective of Twitter. This user shows that when a user finds any anomaly about technology, such as a zero-day threat, first of all he or she announces the information on social media. The figures also show that an Apple Mac vendor announced this vulnerability on 4 August 2019, but the Twitter user wrote that it had existed at least 90 days ago. This study will therefore search on social media for new zero-day threats.

5.4.1 Twitter

Twitter is the most popular text-based social media site on the Internet. Twitter’s text-based style is more suitable for this study than any other social platform. Users can send any personal information, news, meeting info, or related texts on Twitter easily. Thus, this platform can be checked for new zero-day threat information and this study uses Twitter as a social media platform. In addition, Twitter has some restrictions for collecting information. For example, any user can collect all Twitter users’ information with robots or crawlers. This restriction writes on “https://twitter.com/robots.txt”.

For this, the study obeys the Twitter rules with related information as follows:

```
# Every bot that might possibly read and respect this file.

User-agent: *

Allow: /*?lang=

Allow: /hashtag/*?src=

Allow: /search?q=%23

Disallow: /search/realtime
```

```
Disallow: /search/users

Disallow: /search/*/grid


Disallow: /*?

Disallow: /*/followers

Disallow: /*/following


Disallow: /account/not_my_account

Disallow: /account/deactivated

Disallow: /settings/deactivated


Disallow: /oauth

Disallow: /1/oauth


Disallow: /i/streams

Disallow: /i/hello


# Wait 1 second between successive requests. See ONBOARD-2698 for
details.

Crawl-delay: 1


# Independent of user agent. Links in the sitemap are full URLs
using https:// and need to match

# the protocol of the sitemap.

Sitemap: https://twitter.com/sitemap.xml
```

In this study, the crawlers cannot refresh faster than 1 second, cannot search in real time, and cannot search direct users and grids. This research's crawlers use the Twitter search form and search Twitter users and scroll down through such people.

Then information is collected with related search words and stored in MariaDB/MysqlDB.

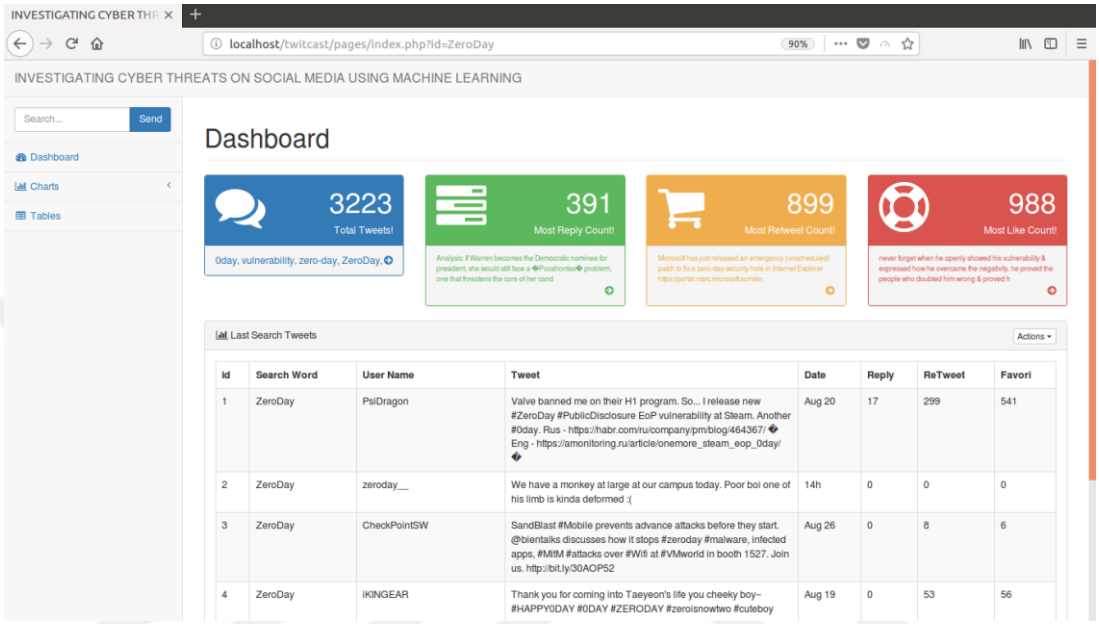


Figure 5.3 Dashboard of Applications for Web UI

5.4.2 Searched Words

The words 0-day, 0day, zero-day, and zeroday are searched words that are special words for investigating zero-day vulnerabilities and make sense within the TensorFlow machine learning framework.

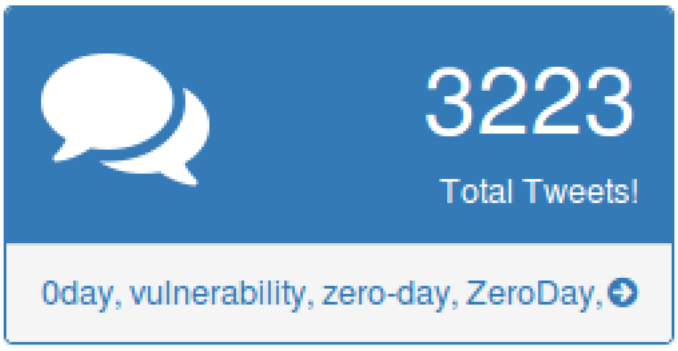


Figure 5.4 Searched Words List

Table 5.1 Pie Chart of Searched Words, Sorted

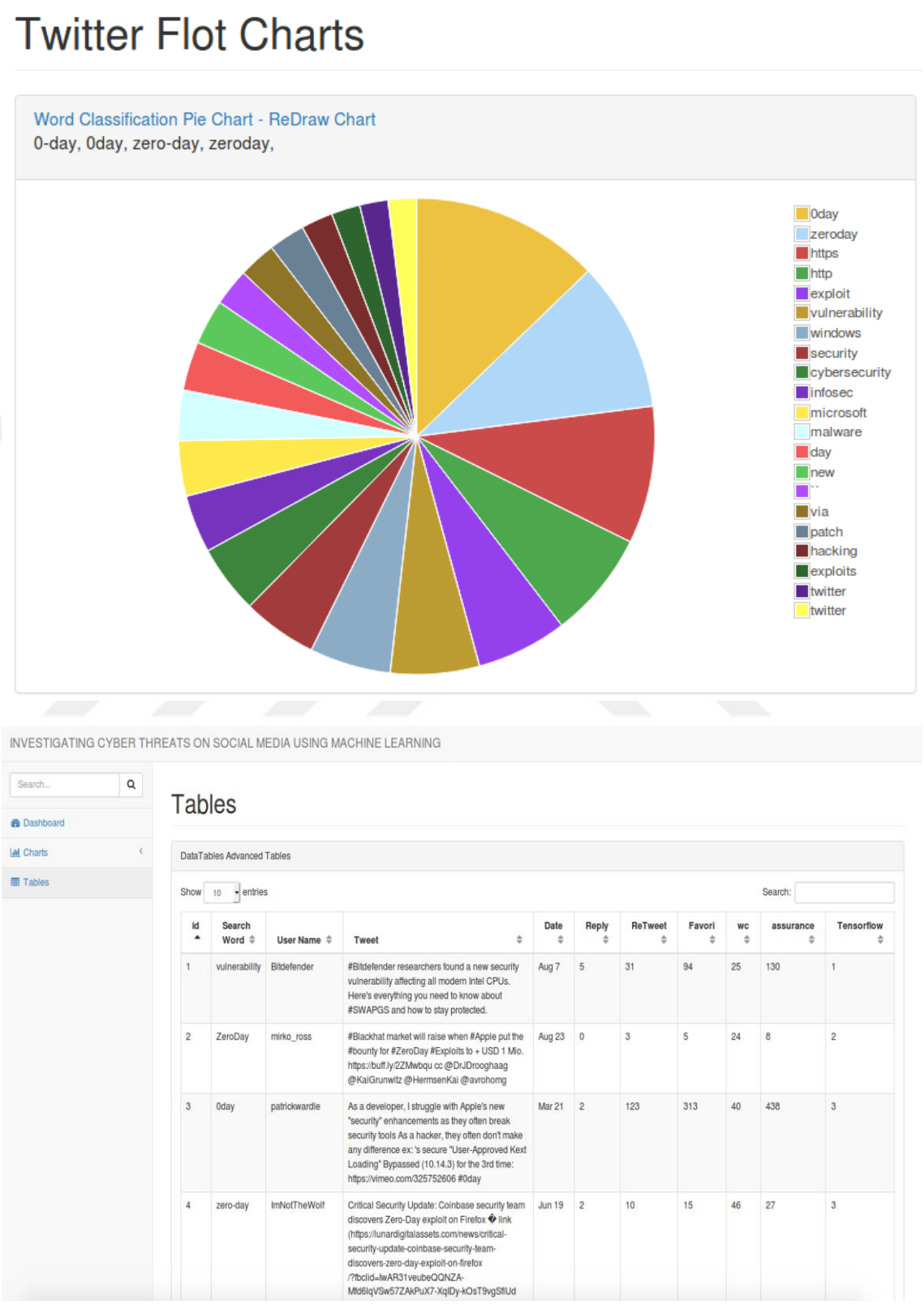


Figure 5.5 Table of Tweets with Details

5.5 Limitations

This project uses a virtualization system and basic laptop computer, and its hard disk is not enough for a large project.

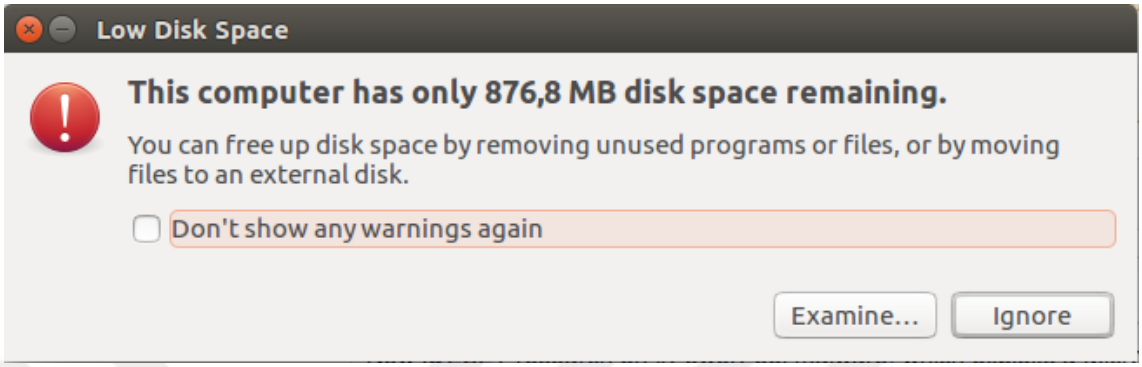


Figure 5.6 Limitations of HDD

```
# Every bot that might possibly read and respect this file.
User-agent: *
Allow: /*?lang=
Allow: /hashtag/*?src=
Allow: /search?q=%23
Disallow: /search/realtime
Disallow: /search/users
Disallow: /search/*/grid

Disallow: /*?
Disallow: /*/followers
Disallow: /*/following

Disallow: /account/not_my_account
Disallow: /account/deactivated
Disallow: /settings/deactivated

Disallow: /oauth
Disallow: /1/oauth

Disallow: /i/streams
Disallow: /i/hello

# Wait 1 second between successive requests. See ONBOARD-2698 for details.
Crawl-delay: 1

# Independent of user agent. Links in the sitemap are full URLs using https:// and need to match
# the protocol of the sitemap.
Sitemap: https://twitter.com/sitemap.xml
```

Figure 5.7 Limitations of Twitter Rules

As a result, this study's crawlers cannot refresh faster than 1 second, cannot search in real time, and cannot search direct users and grids. This research's crawlers use the Twitter search form and search Twitter users and scroll down through such people. Then information is collected with related search words and stored in MariaDB/MysqlDB.

5.6 Codes and Application

For a better understanding of the study, the codes will show the real working system, starting first of all with the frontend of Web UI.

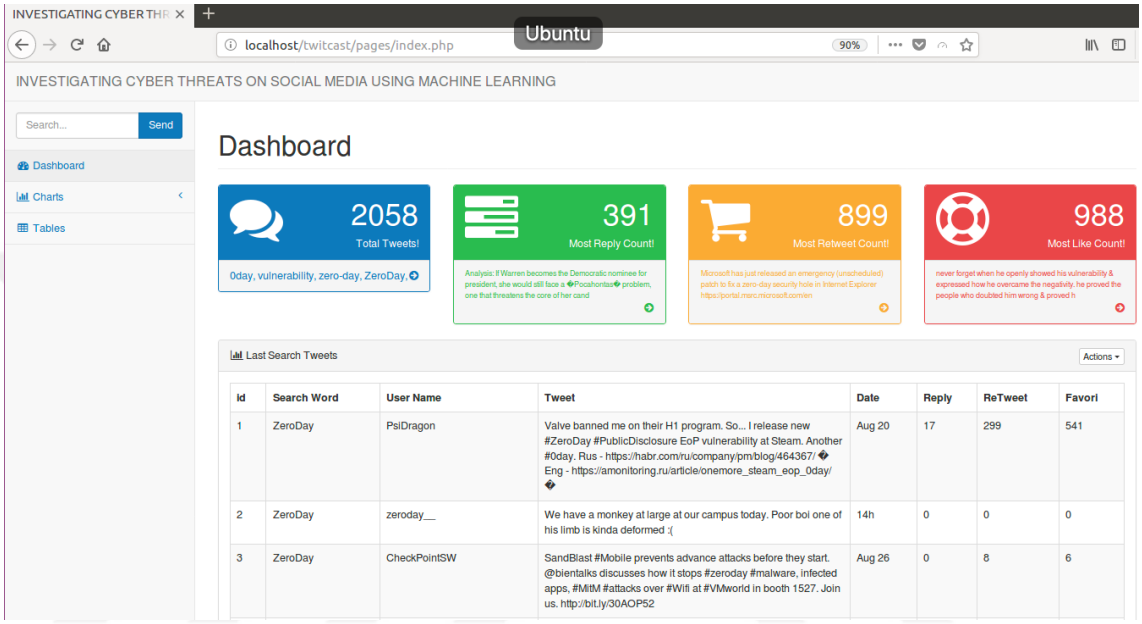


Figure 5.8 Frontend of Web UI

Users can use this research tool from any browser as it is compatible with many different types of browsers. In coding this the frontend of Web UI html, Php, Jquery, and Bootstrap technology was used. In addition, the compatibility part of the code was written for Internet Explorer and the Microsoft Edge browser.



Figure 5.9 Compatibility Part of Internet Explore and Edge

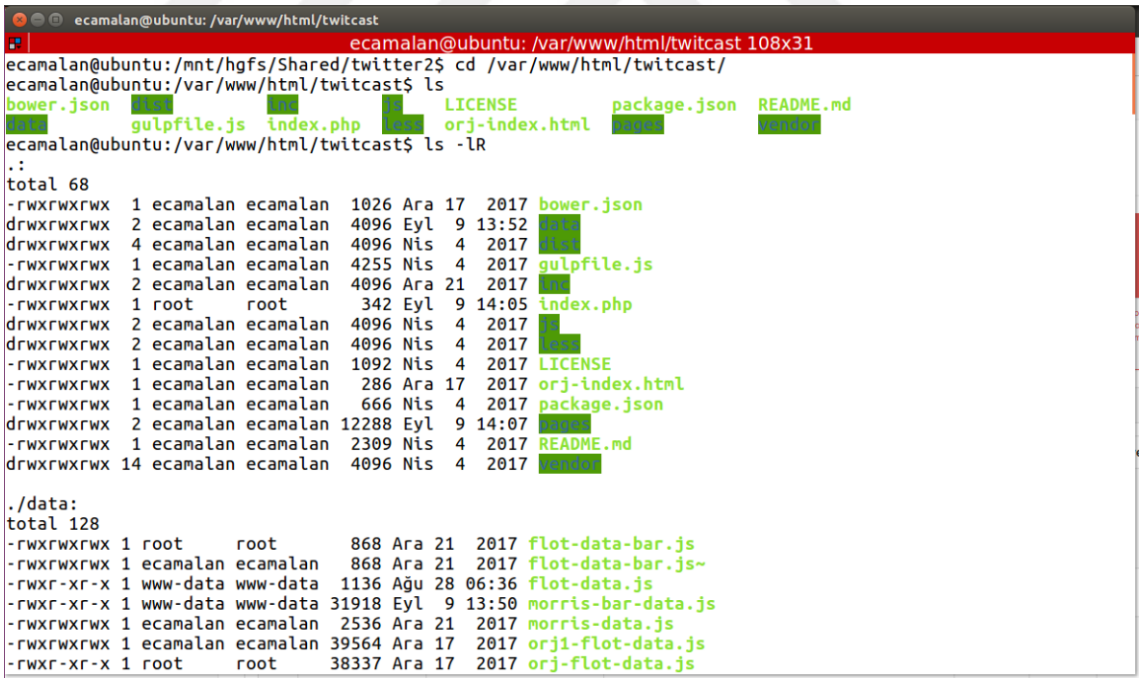


Figure 5.10 Code of Web UI

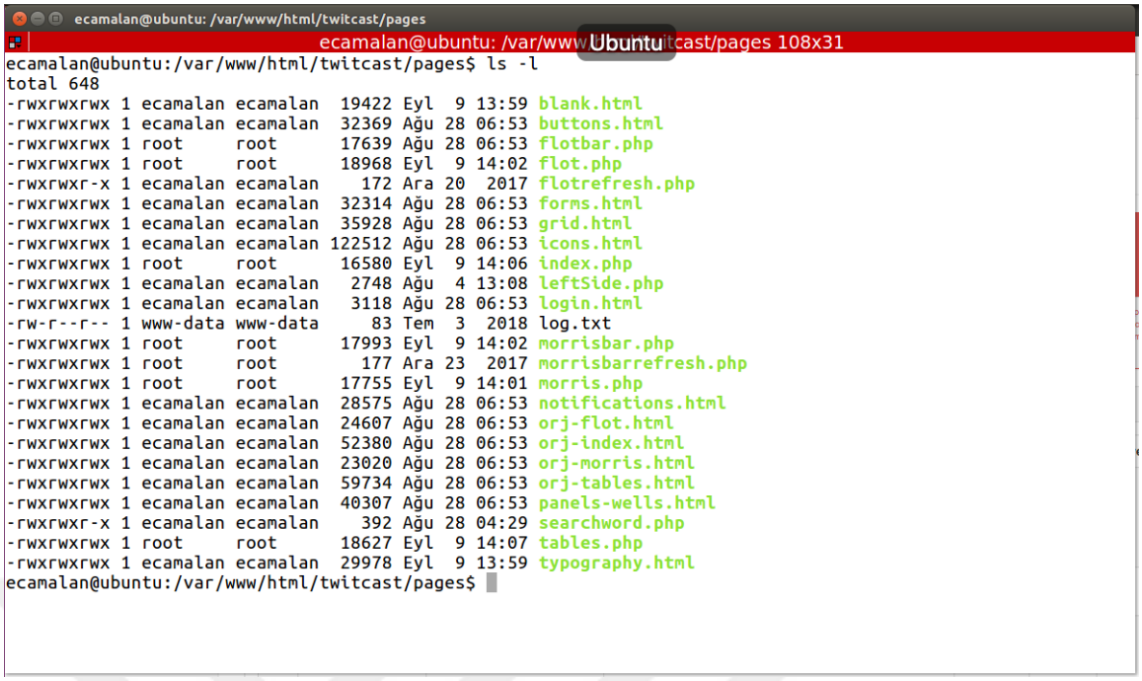


Figure 5.11 Code of Server Side PHP of Web UI



Figure 5.12 Code of Web UI

After showing the code of Web UI, the second important part of the system is the PHP, Bash script, and Python script. These scripts work together to search, collect, calculate, and find zero-day information on social media.

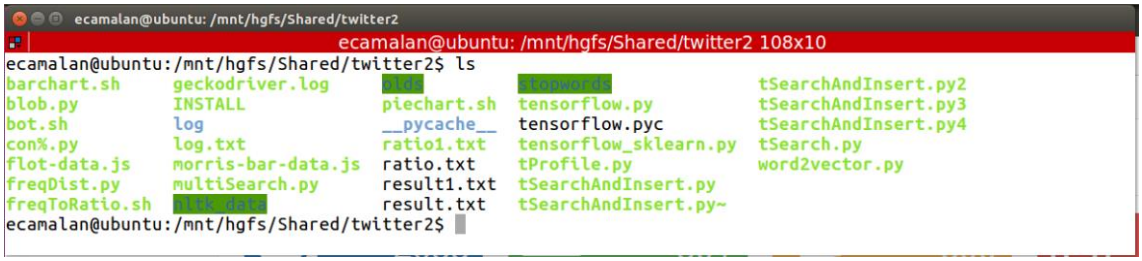


Figure 5.13 Code of Scripting

After using the search bar for searching for new words, as shown below, the crawler searches for the word with the Twitter search bar. When finding results, Twitter shows only 10 tweets, the best hashtag, pictures, and videos. However, we need more than 10 tweets. Therefore, our robots imitate people and scroll down after the page is opened. Robots doing this for 5 pages find all the necessary tweets and save them in the database.

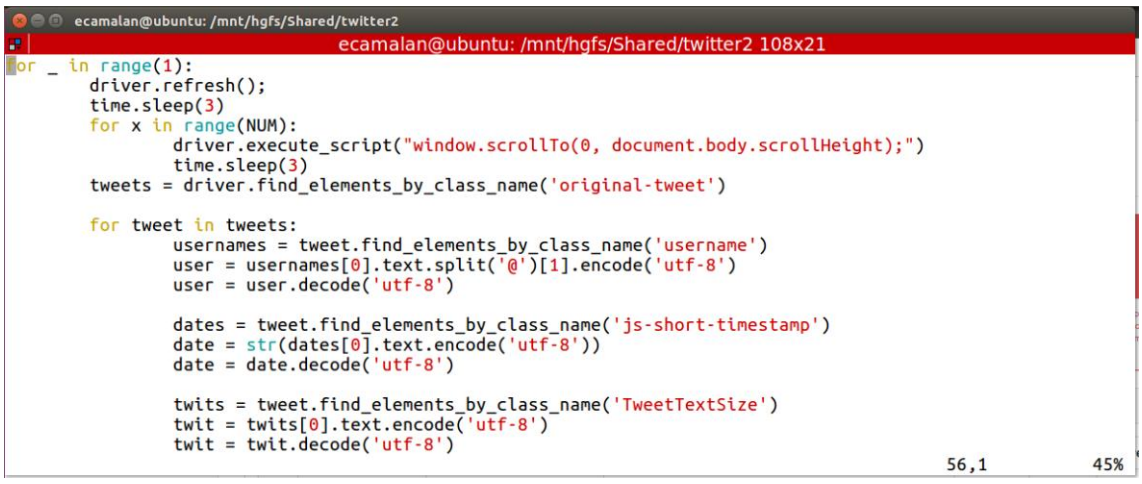


Figure 5.14 Code of Scrolling Page Imitating a Person

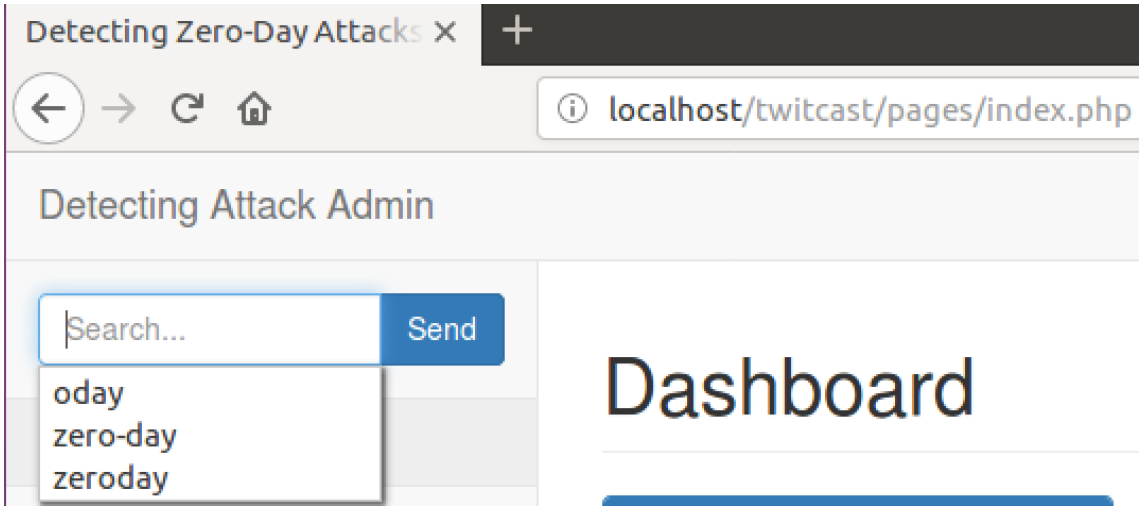


Figure 5.15 Input Parameter

```
ecamalan@ubuntu: /var/www/html/twitcast/pages
ecamalan@ubuntu: /var/www/html/twitcast/pages 121x28
        <div class="navbar-default sidebar" role="navigation">
            <div class="sidebar-nav navbar-collapse">


                <ul class="nav" id="side-menu">


                    <li class="sidebar-search">
                    <form class="form-horizontal" role="form" method="post" action="searchword.php">
                        <div class="input-group custom-search-form">
                            <input type="text" class="form-control" name="formcontrol" placeholder="Search...">
                            <span class="input-group-btn">
                            <input id="submit" name="submit" type="submit" value="Send" class="btn btn-primary">
                            <!--
                            <button class="btn btn-default" type="button" id="submit"  value="Send">
                                <i class="fa fa-search"></i>
                            </button>
                            -->
                        </span>
                        </div>
                     </form>
                        <!-- /input-group -->
                    </li>
                    <li>
                        <a href="index.php"><i class="fa fa-dashboard fa-fw"></i> Dashboard</a>
                    </li>
                    <li>
                                                                                95,89         17%
```

Figure 5.16 Input Parameter HTML & PHP Form Code

```
ecamalan@ubuntu: /var/www/html/twitcast/pages
ecamalan@ubuntu: /var/www/html/twitcast/pages 121x20
<?php

$formcontrol = $_POST["formcontrol"];

$old_path = getcwd();
chdir('/mnt/hgfs/Shared/twitter2/');
//$command = escapeshellcmd('python tSearchAndInsert.py $formcontrol 2 > log.txt 2>&1');
//$output = shell_exec($command);

$cmd = "python tSearchAndInsert.py ".$formcontrol." 50 > log.txt 2>&1";
shell_exec($cmd);

chdir($old_path);



header("Location: index.php?id=$formcontrol");
?>
                                                                    1,1           All
```

Figure 5.17 Search Word Parameter HTML & PHP Form Code

Collecting tweets and learning words about zero-day vulnerabilities is done with the NLTK Library and TensorFlow Library.

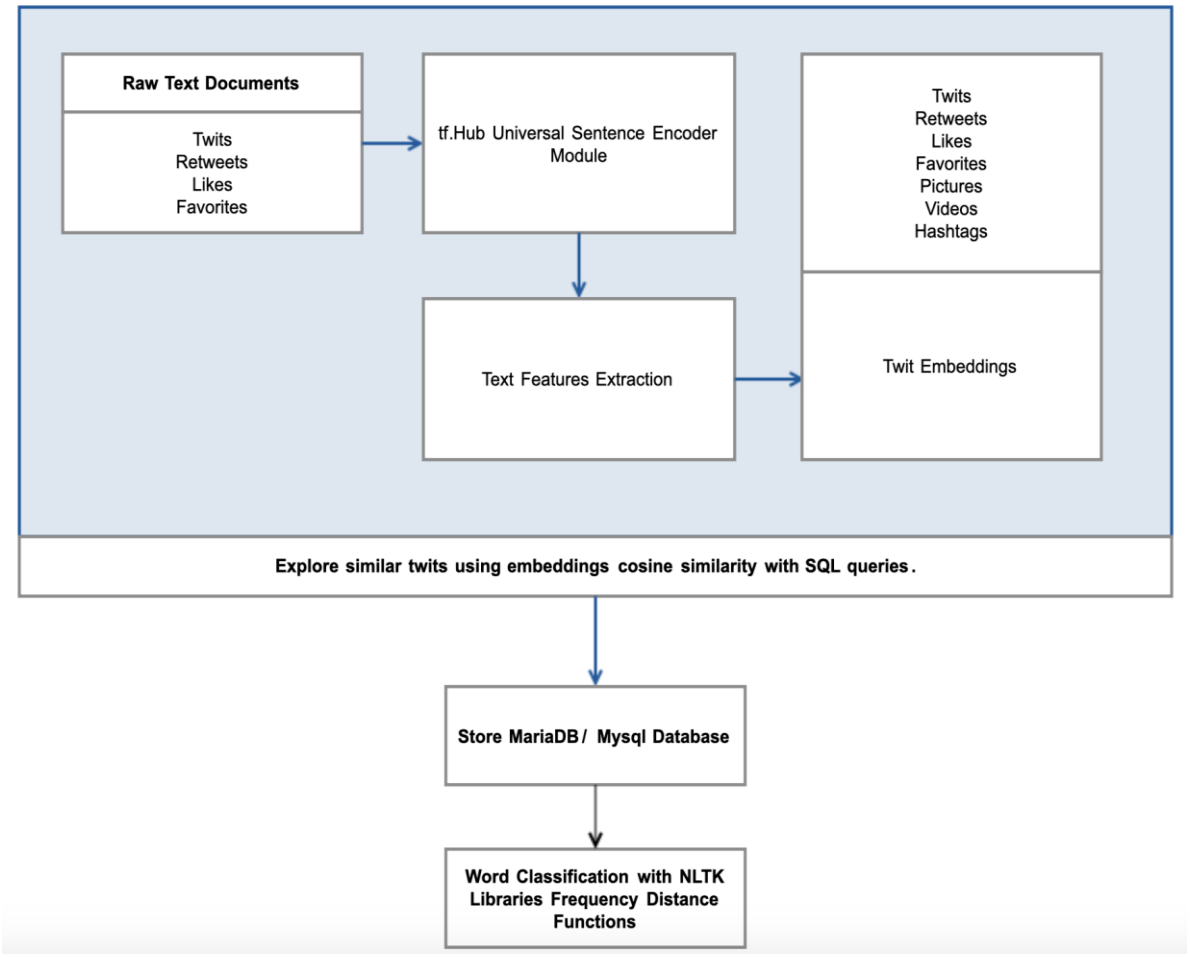


Figure 5.18 Architecture of NLTK and TensorFlow Libraries Working Together

CHAPTER 6

PERFORMANCE

6.1 Performance

This study has established a process for crawling Twitter, a social media platform, and collecting information. During this process the robots imitate people, so they open browsers in shadow mode surfing on Twitter, collect related information, and store it in a database. This process can change and may be limited by Twitter's scroll-down count. Surfing on Twitter, humans read and scroll down many times, so in this research we can scroll as much as we want.

The figures below show 4 performance criteria: for a 1-page scrolling, 5-page scrolling, 10-page scrolling, and 15-page scrolling.

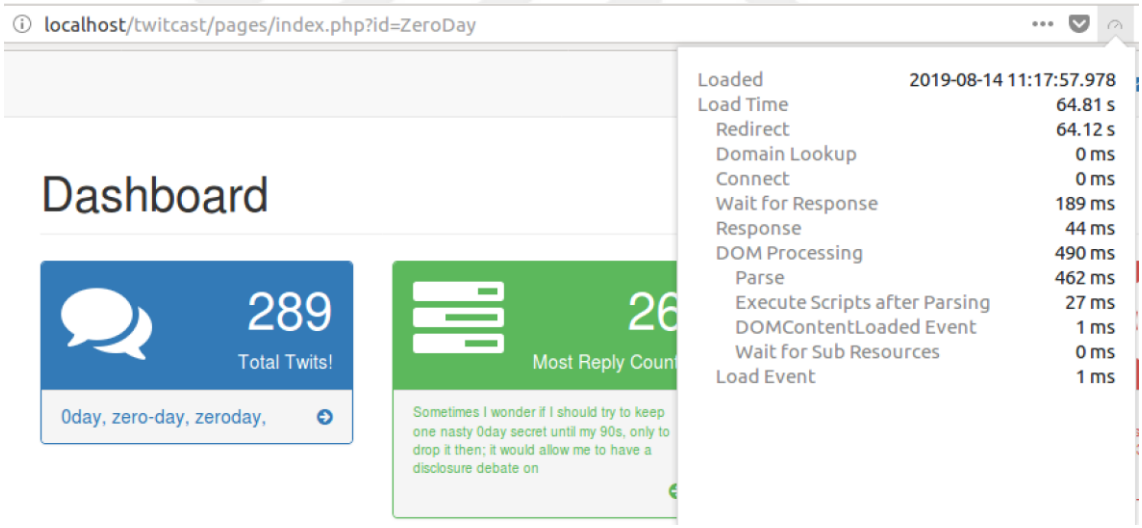


Figure 6.1 Performance of 1-Page Scrolling and Collection of Information from Twitter Page

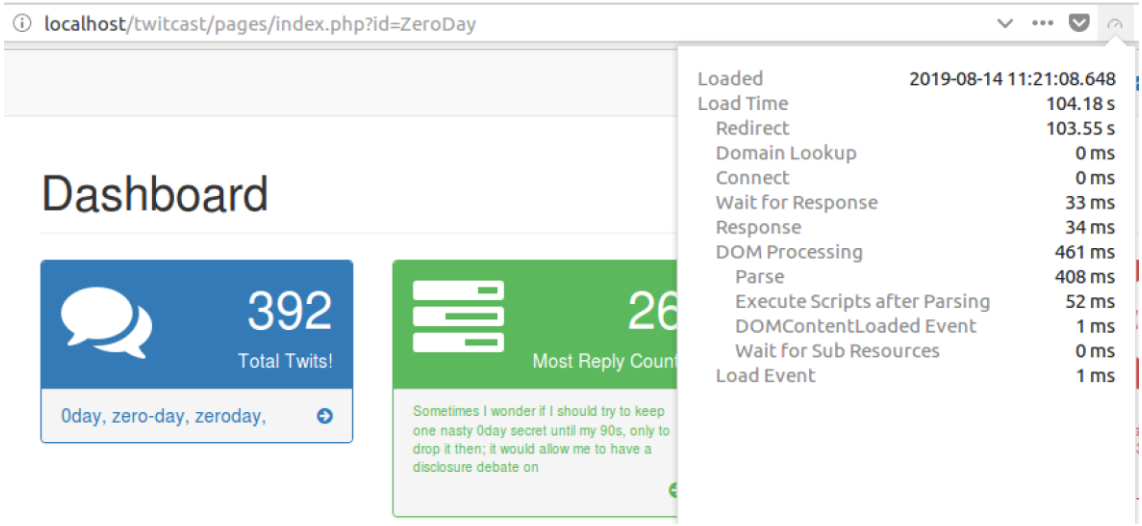


Figure 6.2 Performance of 5-Page Scrolling and Collection of Information from Twitter Page

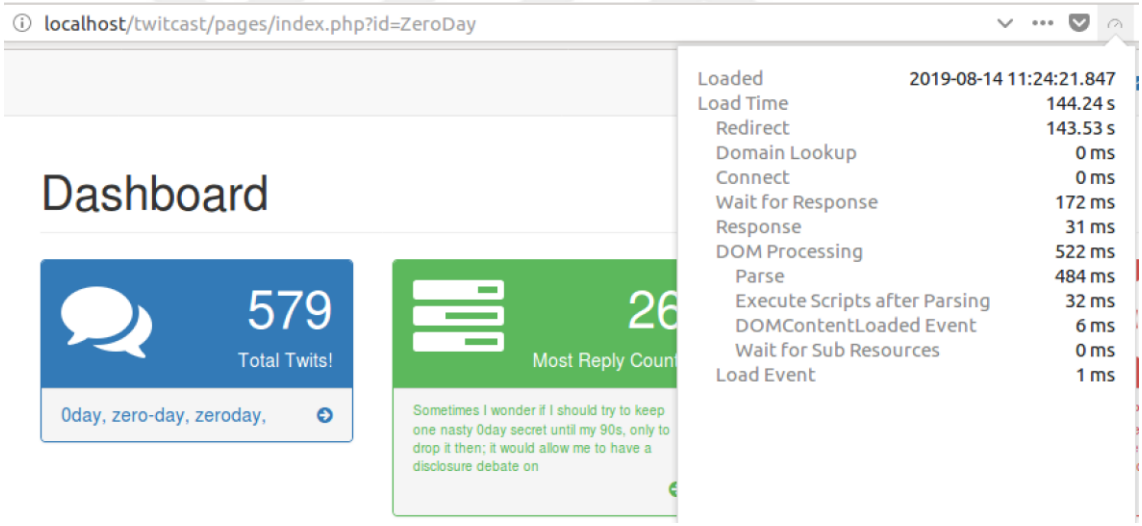


Figure 6.3 Performance of 10-Page Scrolling and Collection of Information from Twitter Page

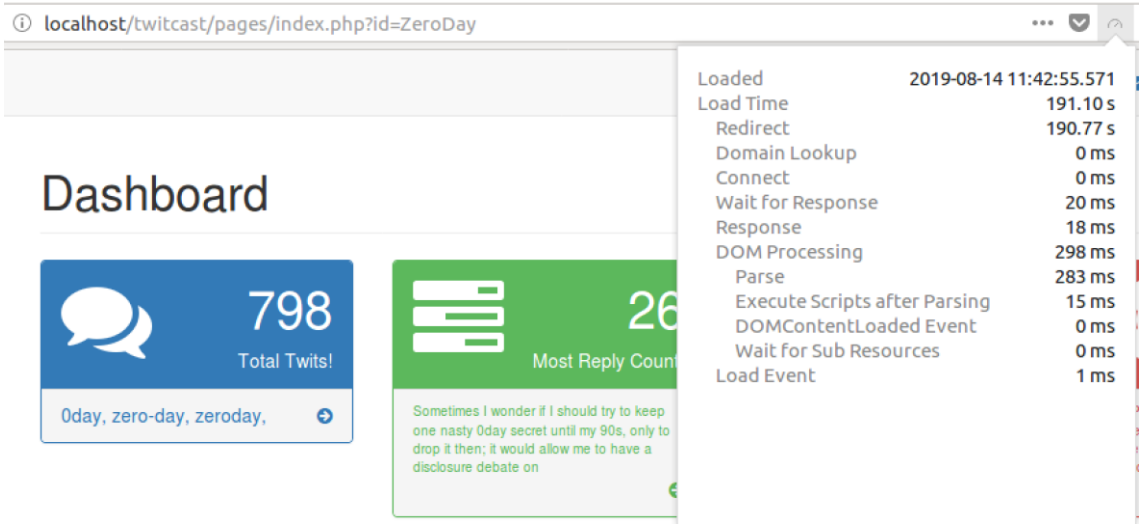


Figure 6.4 Performance of 15-Page Scrolling and Collection of Information from Twitter Page

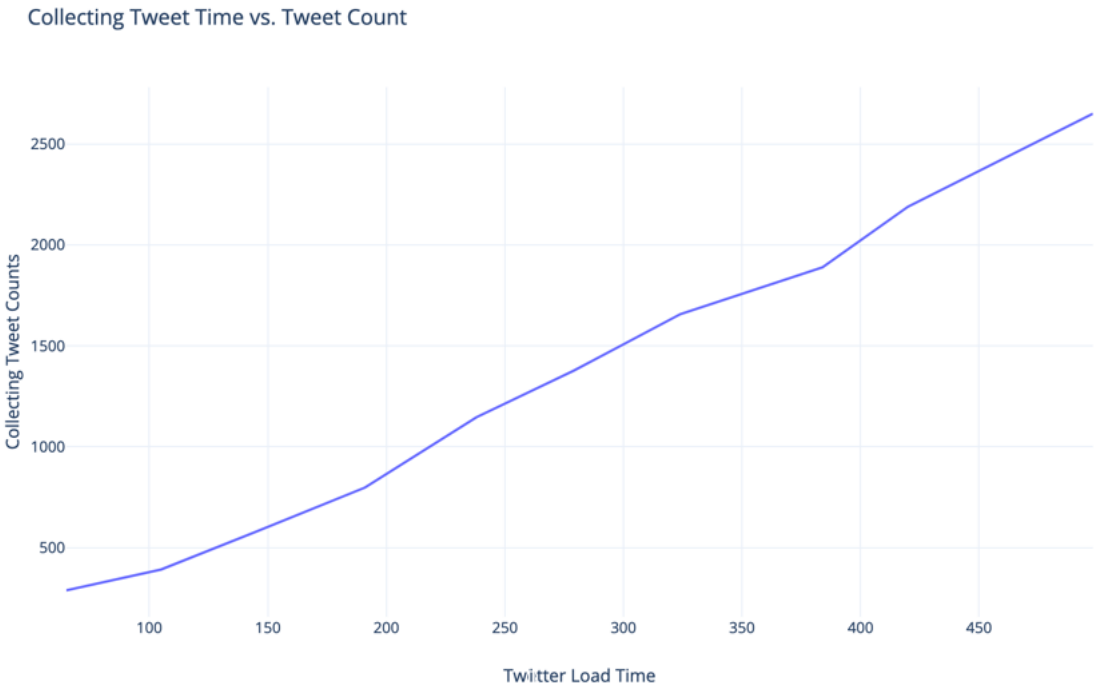


Figure 6.5 Collecting Tweet Time vs. Tweets

The graph in Figure 6.6 shows us that while the program collects tweets in the first place, it depends entirely on Twitter's response time.

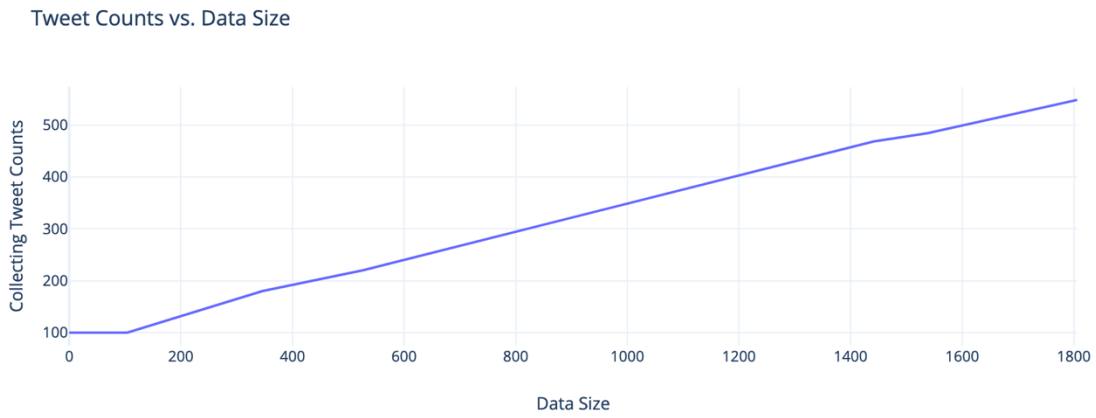


Figure 6.6 Data Size vs. Tweet Counts

Method	Tweet Counts	Time
BOT Collects Data	294 between 1000	5 minutes
API Collects Data	150	60 minutes

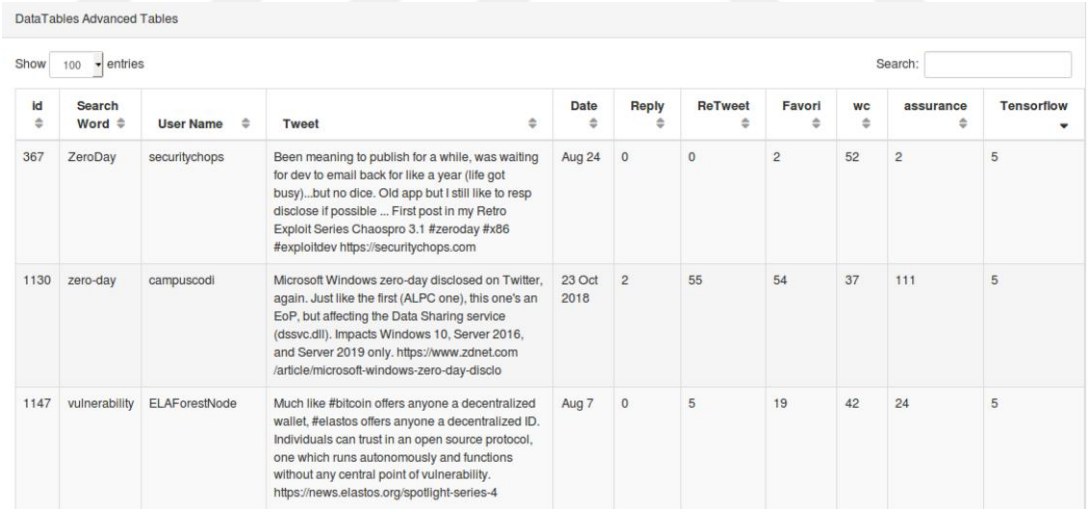
Figure 6.7 Comparison of Tweets Collection Performance with BOT vs. Twitter API

Table 5.3 shows us that Twitter API allows you to pull 150 tweets per hour, but the application in this study can collect between 294 and 1000 tweets in 5 minutes. Therefore, they who work on twitter projects could not measure instantaneous data extraction. This means that the research's application works in real time.

Table 6.1 Comparison of Finding Zero-Day Tweet Success Rate

Order By	Success Rate (Top 10)	Success Rate	Reply	Retweet	Favori	NLTK	TensorFlow
Reply	**10%**		**381**	**54**	**121**	**24**	**1**
Retweet	**60%**		**44**	**899**	**920**	**25**	**2**
Favorite	**20%**		**3**	**636**	**988**	**34**	**0**
NLTK	**60%**		**0**	**9**	**17**	**61**	**2**
TensorFlow	**80%**		**0**	**0**	**2**	**52**	**5**

Table 6.2 Research Application Table Interface


DataTables Advanced Tables

Show 100 entries Search:

id	Search Word	User Name	Tweet	Date	Reply	ReTweet	Favori	wc	assurance	Tensorflow
367	ZeroDay	securitychops	Been meaning to publish for a while, was waiting for dev to email back for like a year (life got busy)...but no dice. Old app but I still like to resp disclose if possible ... First post in my Retro Exploit Series Chaospro 3.1 #zeroday #x86 #exploitdev https://securitychops.com	Aug 24	0	0	2	52	2	5
1130	zero-day	campuscodi	Microsoft Windows zero-day disclosed on Twitter, again. Just like the first (ALPC one), this one's an EoP, but affecting the Data Sharing service (dssvc.dll). Impacts Windows 10, Server 2016, and Server 2019 only. https://www.zdnet.com /article/microsoft-windows-zero-day-disclo	23 Oct 2018	2	55	54	37	111	5
1147	vulnerability	ELAForestNode	Much like #bitcoin offers anyone a decentralized wallet, #elastos offers anyone a decentralized ID. Individuals can trust in an open source protocol, one which runs autonomously and functions without any central point of vulnerability. https://news.elastos.org/spotlight-series-4	Aug 7	0	5	19	42	24	5

Table 6.2 shows us a comparison of tweet rates sorted by different variables such as reply counts, retweet counts, favorite counts, NLTK libraries word classification counts, and TensorFlow libraries finding vector counts.

CHAPTER 7

RESULTS

At the end of the application process, it was seen that the program can find new information from tweets via word classifications by analyzing the true data if the working set has the given TensorFlow and NLTK libraries. The studies also showed that the system may require manual debugging. This is because 50 percent of the tweets were talking about new weaknesses. These are newly related; however, the program is also likely to select old words. Thus, the user can see both old and new (learned) keywords together and separate them. In the application part of this study, words like Zero Day, 0 Day, Zero-Day, and 0-Day were researched and the system collected tweets. However, the pie chart showed that there were more important keywords in the tweets than these words. Here we could thus see that the program can learn other related words and it shows and lists those tweets to the user, too. For example, the program can search for the words “terror, threat, terrorism, attack” and it can also find the word “bomb”, and this may help to prevent real-life terror attacks. Similarly, when “zeroday, 0day, and zero-day” are searched for simultaneously, the zero-day vulnerability, which is on the agenda at the same time, comes out of “windows, exploit, steam”. When tweets that include these word classifications are searched, the Table 7.3 shows that the application discovers a new zero-day opening. The table thus presents a zero-day exploit available to us.

When this research is used effectively by collecting data from many sources, it will gather the right data for us without any efforts to visit any news sites. It is also possible to make sure that these are up-to-date. The pie chart below shows that even if we search for the same words, as the search increases, more new keywords appear and these keywords are collected at a specific similar point, actually pivoting. The first graph (Table 6.1) shows 298 tweets and the last one (Table 6.2) shows 1295 tweets.

Table 7.1 Twitter Flot Chart 1

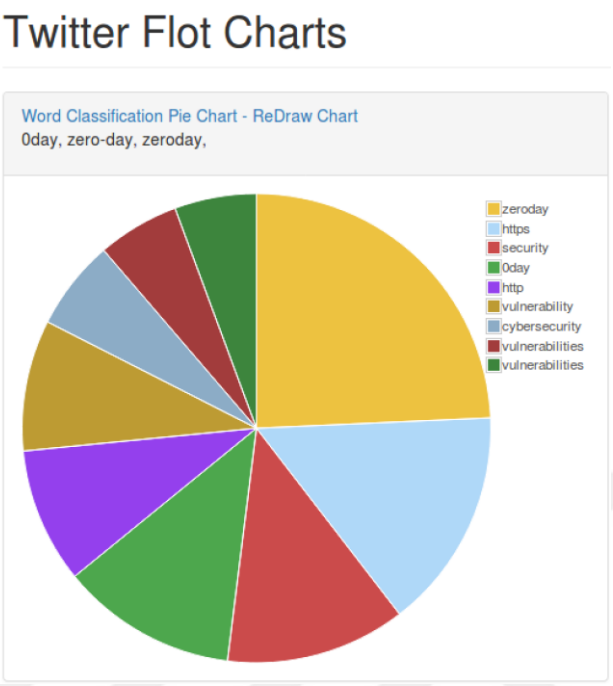
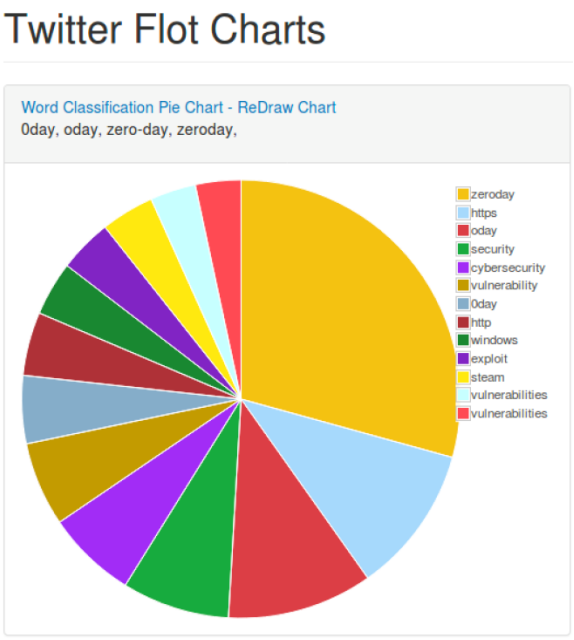


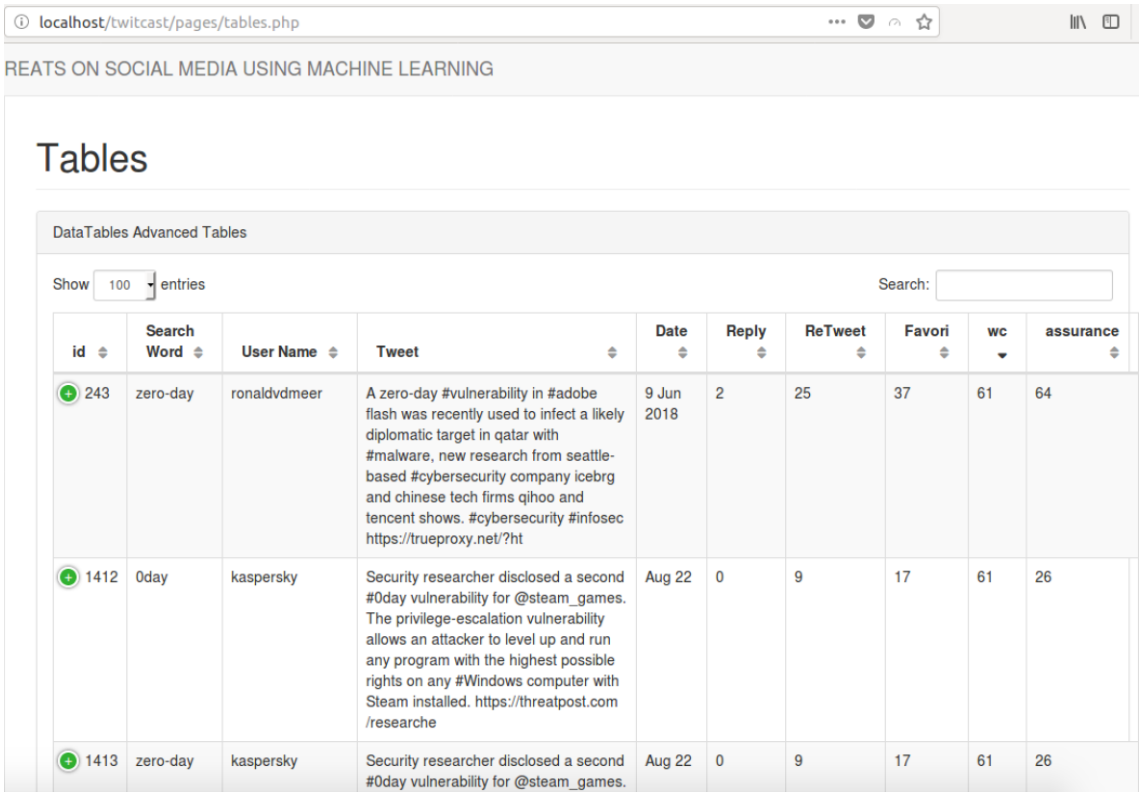
Table 7.2 Twitter Flot Chart 2



On the other hand, with this research, the following thoughts are sufficiently addressed: "If there is a weakness, the tweet that is talking about it would be popular and be top-ranked because the users who find and see the weakness would like it, favorite it, and

retweet it". This research proves to us that in fact people like to retweet only what they see as visually beautiful. They do not generally like or retweet a newly found weakness. Thus, a tweet about a weakness may not be popular. The table below shows this situation in more detail.

Table 7.3 Word Classification



id	Search Word	User Name	Tweet	Date	Reply	ReTweet	Favori	wc	assurance
243	zero-day	ronaldvdmeer	A zero-day #vulnerability in #adobe flash was recently used to infect a likely diplomatic target in qatar with #malware, new research from seattle-based #cybersecurity company icebrg and chinese tech firms qihoo and tencent shows. #cybersecurity #infosec https://trueproxy.net/?ht	9 Jun 2018	2	25	37	61	64
1412	0day	kaspersky	Security researcher disclosed a second #0day vulnerability for @steam_games. The privilege-escalation vulnerability allows an attacker to level up and run any program with the highest possible rights on any #Windows computer with Steam installed. https://threatpost.com /researche	Aug 22	0	9	17	61	26
1413	zero-day	kaspersky	Security researcher disclosed a second #0day vulnerability for @steam_games.	Aug 22	0	9	17	61	26

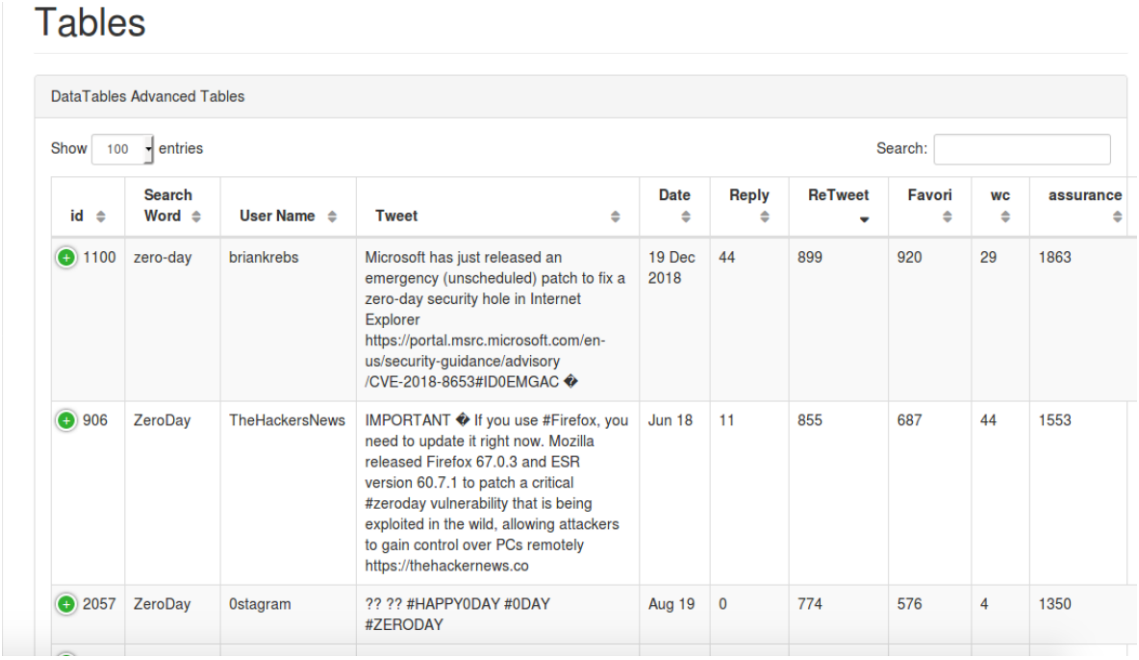
In this table, the word classification called WC is 60, and the arrow at the bottom indicates that it is ranked according to it, it is the highest, and it addresses the Linux KDE desktop vulnerability.

Table 7.4 Word Classification 2

1236	zero-day	GelosSnake	Project Zero has released a "0day "In the Wild" spreadsheet - "This spreadsheet is used to track cases of zero-day exploits that were detected "in the wild" https://www.securityweek.com /organizations-asia-targeted-inpage-zero-day Official blog: https://googleprojectzero.blogs	May 18	0	22	45	57	67

WC 57 and zero-day references were found here. There is a link in the table to the source where these were found, but this is a published site. Table 5.1 represents a site that has not yet been published. Therefore, discovery is possible even before publication.

Table 7.5 Retweet Count



Tables

DataTables Advanced Tables

Show 100 entries Search:

id	Search Word	User Name	Tweet	Date	Reply	ReTweet	Favori	wc	assurance
1100	zero-day	briankrebs	Microsoft has just released an emergency (unscheduled) patch to fix a zero-day security hole in Internet Explorer https://portal.msrc.microsoft.com/en-us/security-guidance/advisory /CVE-2018-8653#ID0EMGAC	19 Dec 2018	44	899	920	29	1863
906	ZeroDay	TheHackersNews	IMPORTANT If you use #Firefox, you need to update it right now. Mozilla released Firefox 67.0.3 and ESR version 60.7.1 to patch a critical #zeroday vulnerability that is being exploited in the wild, allowing attackers to gain control over PCs remotely https://thehackernews.co	Jun 18	11	855	687	44	1553
2057	ZeroDay	0stagram	?? ?? #HAPPY0DAY #0DAY #ZERODAY	Aug 19	0	774	576	4	1350

This table shows us that a tweet with 185 retweets ranked by retweets is just an advertisement. WC = 45, which means it is high but it still is not top-ranked.

CHAPTER 8

CONCLUSION

Terror is a violent activity that frightens people and reduces their quality of life. There is a threat that these actions may take place in either real life or in the virtual world created by the Internet. Since it is possible for people to communicate easily about the preparation of criminal acts, especially on social media platforms, continuous monitoring of these environments has become a necessity. In these environments, millions of data transfers take place within seconds. Therefore, these exchanges cannot be controlled by the human eye. Various programs must be created for such control. In particular, the presence of content containing various keywords should be monitored continuously. However, it must be noted that these keywords may change. Hence, there should be a word library of the control mechanism that learns, reconciles, and develops itself. If such a control mechanism is developed, it would be possible to know what people are talking about. Watching publicly published information may also provide commercial benefits in the future.

This study has aimed to provide a solution to the modern-day needs of monitoring the risks represented by cyber crime and cyber terrorism, specifically by designing a program that can monitor social media platforms for references to zero-day security loopholes that can allow potential cyber criminals or cyber terrorists to take advantage of security weaknesses and perpetuate criminal acts via the Internet. To address this need, the study began by exploring definitions of many key concepts in this field, from the idea of the Internet itself to the wide range of cyber threats that exist, with a special focus on the threats and attacks that may be relevant to social media platforms. The architecture of the new program presented here was then explained in detail, followed by an evaluation of the results. The new program relies on a TensorFlow machine learning framework based on principles such as word classification and maximum likelihood to identify threats in the cyber environment. The results demonstrated the program's success in an application designed to reveal zero-day vulnerabilities.

In conclusion, the program presented here is in its early stages of development, but if it is developed further, it can acquire more data from any social media platform with text

content. In addition to zero-day threats, it could also possibly find other keywords or tweets about unusual activities. This is because the program learns and lists other new words that are used together with the chosen keywords. For example, when “Nike” and “Adidas” are given to the program, it lists “New Balance” tweets as well. This shows that users were also significantly using “New Balance” while they were talking about Adidas or/and Nike. In other words, the new program presented here can learn, match, and list related words beyond the list of provided keywords. If this research is expanded in the future, more robots and browsers can be added and it can receive data from many websites. It can also find meaningful data much faster via neural networks using machine learning and processing. This is a valuable contribution to the literature on zero-day threat detection and cyber security in general, in light of the importance of these issues for personal, corporate, national, and even global peace and security. The work presented here has made it possible to quickly find new zero-day vulnerabilities, but this approach is still limited, as it is necessary to proceed manually and even stop sometimes. In future work, this approach could evolve into more advanced intelligence research.

CHAPTER 9

FUTURE WORK

The current data collected in this study were only obtained from Twitter, but it is necessary to gather information from many different social media platforms in order to perform better analysis and work more accurately. The size of the learning set used here was kept relatively low due to the machine's hard disk limitations, so expanding the size of the study with different social media sources and increasing the size of the data would also increase the consistency of the machine learning.

In addition, checking the zero-day vulnerabilities that are detected from different OSINT sources and checking whether these are actually zero-day or previously discovered weaknesses will increase the consistency of this study.

REFERENCES

[1] PWC Türkiye., "Küresel Bilgi Güvenliği Araştırması", 2017. https://www.pwc.com.tr/tr/hizmetlerimiz/risk-surec-teknoloji-hizmetleri/bilgi-guvenligi-ve-siber-guvenlik/bilgi-guvenligi-ve-siber-guvenlik-yayinlari/kuresel-bilgi-guvenligi-arastirmasi-2017/eglence-medya-ve-iletisim-sektoru.html (21.11.2018)

[2] Şenol, M., "Siber Güçle Caydırıcılık ama Nasıl?", Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(2), 10-17, 2016.

[3]Jeffrey, R.. "Sony Pictures Cyber-Attack Timeline", 2014. https://www.bankinfosecurity.com/sony-pictures-cyber-attack-timeline-a-7710

[4] DeSimone, A., & Horton, N., "Sony's Nightmare Before Christmas: The 2014 North Korean Cyber Attack on Sony and Lessons for US Government Actions in Cyberspace", The Johns Hopkins University Applied Physics Laboratory LLC. 2017.

[5] Alhassan, M.M., & Adjei-Quaye, A., "Information Security in an Organization", International Journal of Computer, 24(1), 110-116, 2017.

[6] Cavelty, M.D., "Cyber-Security, Contemporary Security Studies", Oxford University Press, Editors: Allan Collins, 362-378, 2012.

[7]Ocaklı, A., "Dijital Kapitalizm ve Yeni Medya Ekonomisi", 2017. http://ahmetocakli.blogspot.com.tr/2017/12/dijital-kapitalizm-ve-yeni-medya.html

[8] Gündüz, M.Z., & Daş R., "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri", ISCTURKEY 2016 - 9. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı, ODTÜ, 9(1), 11-18, 2016.

[9] Mouton F., Leenen, L., & Venter, H.S., "Social Engineering Attack Examples", Templates and Scenarios, Computers & Security Journal, 59, 186–209, 2016.

[10] Lunenburg, C.F., "Communication: The Process, Barriers, And Improving Effectiveness", Schooling Journal, 1(1), 1-11, 2010.

[11] Oxford English Dictionary. https://en.oxforddictionaries.com/definition/security, 2019.

[12] Kahn, E. R., & Cerf, G. V., "What Is The Internet (And What Makes It Work)", 1999. http://www.policyscience.net/cerf.pdf

[13] Pawar, V. M. & Anuradha J. "Network Security and Types of Attacks in Network", Procedia Computer Science, 48, 503 – 506, 2015.

[14] Sancak, K., "Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü", KTÜ Sosyal Bilimler Enstitüsü Dergisi, 6, 13-134, 2013.

[15] Degaut, M., "What is Security?", 2015. https://www.researchgate.net/publication/310495076

[16] Bachmann, S.D., & Gunneriusson, H., "Hybrid Wars: The 21st Century's New Threats to Global Peace and Security", 2015. https://www.researchgate.net/publication/268444446_HYBRID_WARS_The_21st_-_CENTURY'S_NEW_THREATS_TO_GLOBAL_PEACE_AND_SECURITY

[17] Altınbaşak, İ., & Karaca, E. S., "Internet Advertising and an Application on the Assessment of Internet Advertising", Ege Academic Review, 9(2), 463-487, 2009.

[18] Keefer A. & Baiget T., "How it all Began: a Brief History of the Internet", No Date. http://bd.ub.edu/pub/keefer/materials/Keefer01_How%20it%20began.pdf

[19] Solmaz, B., Tekin, G., Herzem, Z. & Demir, M., "İnternet ve Sosyal Medya Kullanımı Üzerine Bir Uygulama", Selçuk İletişim, 7(4), 23-32, 2013.

[20] Sade-Beck, L., "Internet Ethnography: Online and Offline", International Journal of Qualitative Methods, 3(2), 45-51, 2004.

[21] Agnihotri, R., Kothandaraman, P., Kashyap R., & Singh R., "Bringing "Social" Into Sales: The Impact of Salespeople'S Social Media Use on Service Behaviors and Value Creation", Journal of Personal Selling & Sales Management, 32(3), 333-348, 2013.

[22] Savaş S., & Topaloğlu, N. "Crime Intelligence From Social Media: A Case Study", 2017 IEEE 14th International Scientific Conference on Informatics, 2017. https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=8323137

[23] Sabah., "Assange: Facebook En Büyük Ajan", Sabah Teknoloji, 2011. https://www.sabah.com.tr/teknoloji/haber/2011/05/04/assange-facebook-dunyanin-en-buyuk-ajani-597582296690.

[24] Yavanoğlu, U., "Sosyal Ağlarda Bilgi Güvenliği Tehditleri ve Alınması Gereken Önlemler", Politeknik Dergisi, 15(1), 15-27, 2012.

[25] Bolton, D., "Anonymous "Declares War" on Turkey, Claims Responsibility for Recent Massive Cyberattacks", Independent, 2015. https://www.independent.co.uk/life-style/gadgets-and-tech/news/anonymous-declares-war-on-turkey-opsis-russia-cyberattack-erdogan-a6784026.html

[26] Zwart, R., "[dns-wg] RIPE NCC Authoritative and Secondary DNS services on Monday 14 December", 2015. https://www.ripe.net/ripe/mail/archives/dns-wg/2015-December/003184.html

[27] Darıcılı, A.B., & Özdal, B., “Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi”, İGÜ Sos. Bil. Dergisi, 4 (1),19-40, 2017.

[28] We Are Social., 2018. https://wearesocial.com/blog/2018/01/global-digital-report-2018

[29] Chip Online., “Atatürk Havalimanı'nda Conficker Paniği”, 2009. https://www.chip.com.tr/haber/ataturk-havalimani-nda-conficker-panigi_10740.html

[30] Solms, R.V., & Niekerk, J. V. “From Information Security to Cyber Security”, Computers& Security Journal, 38, 97-102, 2013

[31] Ermişoğlu, D., “Sosyal Paylaşım Sitelerinin Bilgi Güvenliği Açısından Karşılaştırılması”, Academia Journal of Social Sciences, 1(2), 40-47, 2016.

[32]Schmidt, A., “The Estonian Cyberattacks”, 2012. https://www.researchgate.net/publication/264418820

[33] Ada, M., “NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi”, T.C. Gazi Üniversitesi, Bilişim Enstitüsü, Adli Bilişim Anabilim Dalı, Yüksek Lisans Tezi, 2018.

[34] Ada, M., & Çakır, H., “Kuzey Atlantik Antlaşma Örgütü’nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi”, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5, 632-656, 2017.

[35] Özcan, M., “Siber Terörizm ve Ulusal Güvenlik:internet ve Hukuk”, Bilgi Üniversitesi Yayınları, İstanbul, 2002.

[36] European Comission, “Digital Agenda for Europe: key initiatives”, 2010. http://europa.eu/rapid/press-release_MEMO-10-200_en.htm

[37] NSA-CSS, “National Security Agency - Central Security Service”, 2016. https://www.nsa.gov/resources/students-educators/centers-academic-excellence/

[38] Stafford, B., "What is cybernetics?", Kybernetes, 31(2), 209-219, 2002.

[39] Özçoban, C., “21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü”, T.C. Harp Akademileri, Stratejik Araştırmalar Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi, 2014.

[40] Ustaoğlu, S., “Siber Savaş ve Uluslararası Hukuk”, T.C. Harp Akademileri Stratejik Araştırmalar Enstitüsü, Harp/Harekat Hukuku Anabilim Dalı, Yüksek Lisans Tezi, 2015.

[41] Karaman, M., & Çatalkaya, H., “Kurumsal Siber Güvenlik”, Açık Kaynak İstihbaratı ve Sosyal Medya Riski, 2014. https://www.researchgate.net/profile/Muhammer_Karaman/publication/273755222_Kur

umsal_Siber_Guvenlik/links/550a109d0cf26198a639e4d7/Kurumsal-Siber-Guevenlik.pdf

[42] Şimşek, M., "Terörizm: Kavramsal Bir Çalışma", Akademik Bakış, 54, 319-338, 2016.

[43]Aghatise, J., "Cybercrime Definition", 2006. https://www.researchgate.net/publication/265350281_Cybercrime_definition

[44] Aslay, F., (2017). "Siber Attack Methods and Current Situation Analysis of Turkey's Ciber Safety", International Journal of Multidisciplinary Studies and Innovative Technologies, 1(1), 24-28, 2017

[45] Brickey, J., "Defining Cyberterrorism: Capturing a Broad Range of Activities in Cyberspace", CTC Sentinel, 5(8), 4-5, 2012.

[46] Barry, C. "Future of Cyberterrorism: The Physical and Virtual Worlds Converge", Crime and Justice International, 13(2), 15-18, 1997.

[47] Qaisar, "Siber Terörizmle Mücadele ve Uluslararası Hukuk", T.C. Atatürk Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Anabilim Dalı, Yüksek Lisans Tezi, 2015.

[48] Miş, N., "Securitization Theory and Securitization of the Political", 2011. http://dergipark.gov.tr/download/article-file/17786

[49] Cambridge, 2018. www.dictionary.cambridge.org

[50] Secure Works, "Cyber Threat Basics, Types of Threats," Intelligence & Best Practices, 2018. https://www.secureworks.com/blog/cyber-threat-basics

[51] ACS- Australian Computer Society., "Cybersecurity, Threats, Challenges, Opportunities", 2016. https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cybersecurity_Guide.pdf

[52] Mauro, C., Dehghantanha A., & Dargahi T, "Cyberthreat Intelligence: Challenges and Opportunities", Cornell University, 2018. https://arxiv.org/abs/1808.01162

[53] Mittal S., Das Prajit K., Varish, M., Anupam J., & Finin T., "CyberTwitter: Using Twitter to generate alerts for Cybersecurity Threats and Vulnerabilities", 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), 2016.

[54] Tensorflow: https://cloud.google.com/solutions/machine-learning/analyzing-text-semantic-similarity-using-tensorflow-and-cloud-dataflow

[55] NLTK: https://www.nltk.org/

[56] Sanders, J., “Spectre and Meltdown Explained: A Comprehensive Guide for Professionals”, 2019. https://www.techrepublic.com/article/spectre-and-meltdown-explained-a-comprehensive-guide-for-professionals/

[57] Ribeiro, M., “How Open Source Intelligence Could Save Your Network”, Security Intelligence, 2018. https://securityintelligence.com/how-open-source-intelligence-could-save-your-network/

[58] Symantec, “How Symantec Endpoint Protection Technologies Protect Your Computers”, 2019. https://support.symantec.com/us/en/article.howto101774.html

[59] NLTK Library, “NLTK Word Classification”, 2019. https://www.nltk.org/book/ch06.html

[60] Tensorflow Library, “Tensorflow Machine Learning”, 2019. https://www.tensorflow.org/tutorials/keras

CURRICULUM VITAE

PERSONAL INFORMATION



Name Surname	**:**	Emre ÇAMALAN
Date of Birth	**:**	29.07.1986
Phone	**:**	+90 0530 238 04 03
Email	**:**	emre@camalan.net

EDUCATION

High School	**:**	Kalaba YDA
Bachelor	**:**	Atılım University
Master Degree	**:**	Ankara Yıldırım Beyazıt University

WORK EXPERIENCE

Security Consultancy Department Manager: I am employed by the Barikat Cyber Security Company as a Department Manager. Our aim is preventing hackers and ensuring better levels of cyber security by providing consultancy services to many institutions.

TOPICS OF INTEREST

- Security Analysis
- Forensics
- Software Development Security
- Linux Kernel Maintaining
- Hardening
- Information Systems Security
- Network and Communication Security

August 2019
ANKARA

Department of Computer Engineering

Emre ÇAMALAN

