



Kenzo Staelens

Jonathan van Caloen

Jonas Van den Berghe

Michaël Vasseur

Bachelor Elektronica-ICT Mentor: Tom Cordemans

2022-2023





Kenzo Staelens

Jonathan van Caloen

Jonas Van den Berghe

Michaël Vasseur

Bachelor Elektronica-ICT Mentor: Tom Cordemans

2022-2023

# Malicious Internet traffic interception

K. Staelens, J. van Caloen, J. Van den Berghe, M. Vasseur

This project investigates a way to intercept malicious internet traffic and how a solution can be provided, with an aim for ease of use. By usisng a webserver as a gateway and a firewall built on software developed in python. Emphasis is placed on the third and fourth network layers.

The first chapter regarding malware is given to understand how malware works. Types of attacks and what effect they have are discussed here. Understanding how it works is a baseline to prevent malicious software from infecting a system and helps develop a solution. Subsequently the existing solutions are described and compared. The next chapter discusses the criteria for efficient malware interception and blocking.

From all the known data, a firewall will be developed that will efficiently analyze the network traffic and throw up the necessary actions. The coming chapters cover the technical side of the solution, aiming to provide a look at the firewall coded in python with a user-friendly interface. Responding to the end user's demand for ease of use.

In the final chapter the evaluation of the project is described. The pros and cons of combining this solution with artificial intelligence for a possible sequel are also stated.

Keywords: Firewall, infrastructure, packet analyser, webserver, malware, artificial intelligence, user-friendly interface

# Inhoudsopgave

[tabellenlijst 4](#_Toc128231432)

[codefragmentenlijst 5](#_Toc128231433)

[begrippenlijst 6](#_Toc128231434)

[afkortingenlijst 7](#_Toc128231435)

[Inleiding 8](#_Toc128231436)

[1. malware 9](#_Toc128231437)

[1.1 types 9](#_Toc128231438)

[1.2 tekenen van infectie 9](#_Toc128231439)

[1.3 gebruik 9](#_Toc128231440)

[1.4 Type aanvallen 9](#_Toc128231441)

[2. firewalls en antivirussoftware 9](#_Toc128231442)

[1.1 Firewalls 9](#_Toc128231443)

[1.2 Antivirussoftware 9](#_Toc128231444)

[3. mogelijke oplossingen 9](#_Toc128231445)

[3.1 criteria voor malware detectie 9](#_Toc128231446)

[3.2 mogelijke oplossingen 9](#_Toc128231447)

[3.2.1 python 9](#_Toc128231448)

[3.2.2 c# 9](#_Toc128231449)

[3.3 vergelijking 9](#_Toc128231450)

[4. uiteindelijke oplossing 10](#_Toc128231451)

[4.1 laag drie: Netwerk 10](#_Toc128231452)

[4.2 laag vier: Transport 10](#_Toc128231453)

[4.3 user interface 10](#_Toc128231454)

[5. evaluatie 10](#_Toc128231455)

[Conclusie 11](#_Toc128231456)

[handleiding 12](#_Toc128231457)

[Literatuurlijst 13](#_Toc128231458)

[Bijlagen 14](#_Toc128231459)

[bijlage 1: kopieën van datasheets 15](#_Toc128231460)

[bijlage 2: vergaderverslagen 16](#_Toc128231461)

[bijlage 3: logboek rapporteren 17](#_Toc128231462)

# figurentenlijst

# tabellenlijst

# codefragmentenlijst

# begrippenlijst

# afkortingenlijst

DoS Denial of Service

# Inleiding

Voor dit project wordt er eerst een theoretisch onderzoek gedaan als voorstudie voor het ontwikkelen van een software firewall. De software wordt ontwikkeld in Python. Het project is bedoeld om een beter inzicht te verkrijgen in de werking van malware.   
  
Malware is een samentrekking van het Engelse woord malicious software en wordt vertaald als kwaadaardig en schadelijke software. Het vormt een dagelijkse dreiging voor het internetverkeer en kent vele vormen. Vanuit de vraag naar bescherming zal er worden gezocht naar een mogelijke oplossing vanuit het inzicht dat in de voorstudie werd verkregen. Dergelijke oplossingen bestaan reeds en worden door verschillende software bedrijven op de markt gebracht. Het is dan ook niet de kern van dit project om een betere oplossing te bekomen, maar om een ruimer inzicht in een deelaspect van computerbeveiliging te krijgen.   
  
In het eerste hoofdstuk wordt onderzocht wat malware is. In deze studie zal besproken worden welke types er bestaan en wat voor effecten deze hebben bij het geïnfecteerde toestel.  
  
Vervolgens worden de bestaande oplossingen besproken. Dit hoofdstuk behandeld firewalls en antivirussoftware.   
  
Uit al deze voorgaande kennis zal in het volgende hoofdstukken een mogelijke oplossing worden voorgesteld. Het behandeld de software firewall die ontwikkeld wordt in Python. Het filteren en analyseren van netwerk pakketten zal plaatsvinden op netwerk laag drie en netwerk laag vier. Netwerk pakketten uit landen die een verhoogd risico vormen kunnen door de ingebouwde geolocatie worden geblokkeerd. De software draait op een centrale server die samen fungeert met de firewall software. Hierdoor kan deze ook fungeren als een man in the middle. Dit is nodig om HTTPS-pakketten te decrypteren. De firewall zal ook vroegtijdig een Denial of Service aanval kunnen detecteren en stoppen. Er is interactie tussen de firewall en de eindgebruiker, zodat deze steeds op de hoogte wordt gesteld van mogelijke aanvallen. De gebruiksvriendelijke interface biedt een eenvoudig beheer. Ten slotte volgt een voorstel tot een mogelijk vervolg waar wordt besproken of artificiële intelligentie en rol zou kunnen spelen bij de behandeling van netwerk pakketten.   
  
De belangrijkste onderzoeksmethode is literatuurstudie van online bronnen. Het geeft inzicht in de werking van malware en hoe er zich tegen te beschermen. Ook geven de vele testen die worden uitgevoerd op de firewall bij de ontwikkeling ervan vele inzichten. De interface wordt geëvalueerd door middel van gebruikerstesten, ze worden op regelmatige tijdstippen in het proces voorgelegd.

# 1. malware

## 1.1 types

## 1.2 tekenen van infectie

## 1.3 gebruik

## 1.4 Type aanvallen

# 2. firewalls en antivirussoftware

## 1.1 Firewalls

## 1.2 Antivirussoftware

# 3. mogelijke oplossingen

## 3.1 criteria voor malware detectie

## 3.2 mogelijke oplossingen

### 3.2.1 python

### 3.2.2 c#

## 3.3 vergelijking

# 4. uiteindelijke oplossing

## 4.1 laag drie: Netwerk

## 4.2 laag vier: Transport

## 4.3 user interface

# 5. evaluatie

# Conclusie

# handleiding

# Literatuurlijst

# Bijlagen

# bijlage 1: kopieën van datasheets

# bijlage 2: vergaderverslagen

# bijlage 3: logboek rapporteren

|  |  |  |
| --- | --- | --- |
| Jonas Van den Berghe | Schrijven eerste file | Schrijven inleiding, abstract, toevoegen titels, maken inhoudstafel. |
| Vasseur Michaël | Aanpassingen aan Jonas eerste bestand. | Kaft voorzien van figuur met tittel en subtitel. Abstract en inleiding herschreven. |
|  |  |  |
|  |  |  |