Trojan

Hidden code

AP Hogeschool Antwerpen

Ethical Hacking

Contents

[What is a Trojan? 2](#_Toc123774784)

[Idee 1 De code verbergen als een video. 2](#_Toc123774785)

[Gebruikte code: 2](#_Toc123774786)

[De code compileren tot exe bestand. 2](#_Toc123774787)

[MP4 en code samenvoegen. 2](#_Toc123774788)

[Stappen: 2](#_Toc123774789)

[Bestand extra verbergen: 9](#_Toc123774790)

[Stappen: 10](#_Toc123774791)

[Uitvoering: 14](#_Toc123774792)

[Besluit: 14](#_Toc123774793)

[Idee 2 Code in images: 15](#_Toc123774794)

[Python code: 15](#_Toc123774795)

[Stappen: 16](#_Toc123774796)

[Steghide: 18](#_Toc123774797)

[Stappen: 18](#_Toc123774798)

[Threading: 19](#_Toc123774799)

[Mijn PythonCode: 20](#_Toc123774800)

[Wat te doen tegen trojans? 20](#_Toc123774801)

# What is a Trojan?

Volgens google is dit de definitie van een trojan:

A Trojan Horse (Trojan) is a type of malware that disguises itself as legitimate code or software.

Dit gaf me het idee, hoe kan ik code vermommen en verbergen voor een gebruiker.

# Idee 1 De code verbergen als een video.

Om dit de verkrijgen moet de mp4 gelijktijdig worden afgespeeld als de code en moet dit in 1 bestand zitten.

## Gebruikte code:

Omdat het hier voor mij echt gaat om een code voorbij de gebruiker gesmokkeld te krijgen heb ik deze zeer simpel gehouden. Ik heb gebruik gemaakt van de python libary tkinter om een boodschap te spelen op het scherm.

Text

Description automatically generated

## De code compileren tot exe bestand.

Door gebruik te maken van pyinstaller kan ik van deze code een exe bestand maken van deze code.

Deze code heb ik nodig voor het combineren met de mp4.

## MP4 en code samenvoegen.

Het antwoord hiervoor ligt in een programma waar je misschien niet echt direct aan denkt nl. Winrar.

### Stappen:

1. Selecteer beide files, de code die je wilt voorbij de gebruiker smokkelen en de mp4.
2. Rechts kilikken en onder winrar kiezen add to archiveA screenshot of a computer

   Description automatically generated with medium confidence
3. Kies een gepaste naam en selecteer create sfx archive. Graphical user interface, application

   Description automatically generated
4. Ga naar files en copier alles onder files to add: Graphical user interface, text, application, email

   Description automatically generated

We zullen deze nog nodig hebben.

1. Onder Advanced ga naar SFX options: Graphical user interface, application

   Description automatically generated
2. Onder general kies je een path to extract, vul hier in: Graphical user interface, text, application, email

   Description automatically generated
3. Onder Advanced kopieer je wat je van files gekopieerd had in stap 4. Graphical user interface, text, application, email

   Description automatically generated
4. Bij update kies je overwrite all files: Graphical user interface, text, application, email

   Description automatically generated
5. Vervolgens ga je naar setup en vul je in bij Ren after extraction: Graphical user interface, application

   Description automatically generated
6. We willen natuurlijk dat de gebruiker niets merkt of ziet dus in modes: Graphical user interface, text, application, email

   Description automatically generated
7. Men kan ook het icon hier aanpassen maar als je de naam aanpast verandert dit terug naar het winrar icon. Dus druk gewoon ok en nogmaals ok. Ik heb nu een file die movie.exe noemt. 

## Bestand extra verbergen:

Om te zorgen dat de icon van het bestand je niet weggeeft moeten we dit veranderen. Windows wil echter enkel icons veranderen van snelkoppeloingen en niet van de eigenlijke bestanden. Dit heb ik kunnen oplossen met het open source programa Resource Hacker. ([http://www.angusj.com/resourcehacker](http://www.angusj.com/resourcehacker/))

### Stappen:

1. Open het bestand dat je verkregen hebt in het vorige hoofdstuk in resource hacker. Graphical user interface, text, application, email

   Description automatically generated
2. Klik op de icon add binary ResourceGraphical user interface, text, application

   Description automatically generated
3. Selecteer een meer geschikt icon voor je programma.

Graphical user interface, text, application, chat or text message

Description automatically generated

1. Door dit te doen worden de icons vervangen door iets dat meer filmpje schreewt. Graphical user interface, text, application

   Description automatically generated
2. Verwijder de Icons sie niet mogen gebruikt worden. Graphical user interface, application

   Description automatically generated
3. Kies opslagen als en maak een nieuw bestand aan pauzeer en lees verder als we de naam gaan kiezen. A screenshot of a computer

   Description automatically generated with medium confidence
4. Zoals je kan zien hebben we nog altijd een exe extensie. Windows verbergt dit standaard dus een icon van mp4 kan voldoende zijn maar we kunnen nog 1 stap verder gaan. Ik kies een naam die ik goed vind en voeg hier 4pm aan toe (mp4 achterwaards). Plaats je cursor tussen de 4 en de p en rechts klik. Graphical user interface

   Description automatically generated
5. Door hier RLO te kiezen worden de exe en de 4pm omgedraaid weergegeven door windows. Ik heb dus nu voor de onvoorzichtige gebruiker de extensie mp4 aan mijn bestand al zal het nog altijd zich gedragen als een exe. Druk save.



Het enige dat nog weggeeft dat dit een exe bestand is en geen mp4 is dat windows dit nog altijd als application weergeeft.

## Uitvoering:

Bij het dubbelklikken ziet de gebruiker dit => A person speaking into a microphone

Description automatically generated with medium confidence

Bij het afsluiten krijgt hij echter door onze code ook dit te zien : Graphical user interface, text, application

Description automatically generated

## Besluit:

Dankzij deze techniek kan men code door hetzelfde bestand laten uitvoeren. Ik heb hier nu een zeer eenvoudige code laten zien maar alles is mogelijk.

# Idee 2 Code in images:

Dingen verstoppen in images en zo voorbij iemand smokkelen.

## Python code:

De basis code die ik gebruikt heb is van [Indently](https://www.youtube.com/@Indently). Dankzij deze code kan je tekst toevoegen aan jpg bestanden.

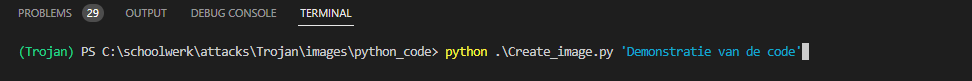
Text

Description automatically generated

De code voegt de boodschap aan de achterkant van de file toe.

### Stappen:

1. Kies een jpg die je wilt gebruiken: A picture containing text, cat, sitting, screen

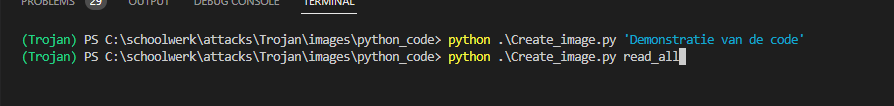
   Description automatically generated
2. Run het script met een string als argument. 

Hierdoor wordt er een nieuwe jpg aangemaakt met een boodschap op het einde toegevoegd. (Output.jpg)

A picture containing text, cat, screen, screenshot

Description automatically generated

1. Om te demonstreren dat er wel degelijk een boodschap in deze file zit neem ik er even een online hex editor bij: Graphical user interface, text

   Description automatically generatedHelemaal op het einde kan je de boodschap zien.
2. Ik heb ook functionaliteit ingebouwd in mijn code voor het bekijken van de boodschap. Als men ingeeft read\_all als argument dan zal je de voledige code van de jpg te zien krijgen: A picture containing text

   Description automatically generated

Je kan ook Read\_message als argument meegeven, Dan krijg je alleen de boodschap te zien. Text

Description automatically generatedText

Description automatically generated

## Steghide:

Steghide is een package die je kan downloaden op deze locatie: <https://sourceforge.net/projects/steghide/postdownload>

### Stappen:

1. Download the package en open de folder in een terminal:

Text

Description automatically generated

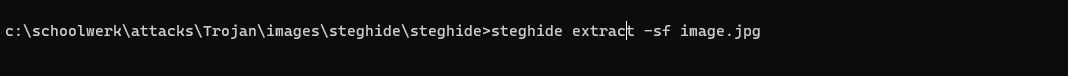
1. Zorg ervoor dat je een payload en een image in je folder hebt. Let wel je payload kan niet veel groter zijn dan de image. Bv zelfs mijn Trojancode (9429 kb) was te groot om te gebruiken met mijn image van 46 kb. Hierdoor heb ik een txt bestand gebruikt met de message.



Het programma vraagt om een passphrase, als je er 1 ingeeft heb je deze terug nodig om om de tekst de decrypteren.

Text

Description automatically generated

1. Voor het decrypteren van de image gebruik je: 

Text

Description automatically generated

Er bestaat malware die kleiner is dan ik bij macht ben nu te maken. En ik ben niet willig deze ongekende code los te laten op mijn pc maar als deze klein genoeg is kan je deze imbedden. Ook is het mogelijk om via een path images en payloads van elders op de pc te gebruiken.

# Threading:

Men kan 2 verschillende codes uitvoeren in hetzelfde programma.

## Mijn PythonCode:

Text

Description automatically generated

De file noemt game en de gebruiker krijgt inderdaad een spelletje. In de file zit echter ook bad code die simultaan wordt uitgevoerd. In dit geval krijgt de gebruiker een alert op het scherm maar dit kan natuurlijk alles zijn. Zo wordt het mogelijk om de gebruiker zelf zijn eigen systeem te laten infecteren zonder dat de gebruiker iets doorheeft.

# Wat te doen tegen trojans?

* Nooit software op je computer draaien die je niet vertrouwd!
* Open nooit een attachment van een email die je niet vertrouwd, ook geen filmpjes of images!
* Houd alle software up to date!
* Zorg dat je een up to date virusscanner hebt die trojans kan opsporen voor ze hun werk kunnen doen.