Análisis de Malware

Comprensión y Análisis de Código Malicioso

Uso de herramientas, búsqueda en logs, funcionalidad y propósito del malware.

SECCION 1
Conceptos y Definiciones

Clase 2
Procedimiento recomendado para análisis.

“Antes de analizar un malware, es necesario encontrarlo. Para poder identificarlo, es preciso recopilar diversa información en la máquina potencialmente infectada. Para realizar dicha recogida de información, es preferible desconectar el disco duro de la máquina infectada y conectarlo en una máquina sana para trabajar desde ella. No es conveniente trabajar en la máquina infectada; los malwares pueden alterar el funcionamiento de la máquina y ocultar información al analista.”

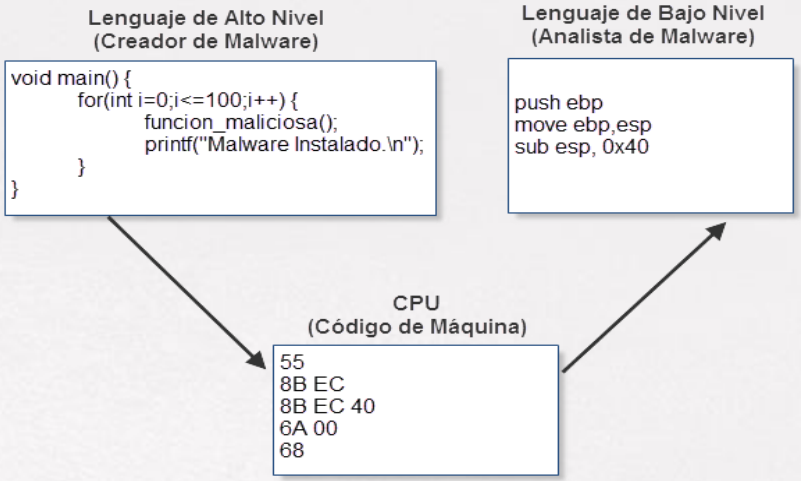
(Del libro “***Seguridad Informática y Malwares***”. Paul Rascagneres.)


require 'spec_helper'
require 'rspec/rails'
require 'capybara/rspec'
require 'capybara/rails'
Capybara.javascript_driver
Category.delete_all;
Shoulda::Matchers
config.integrate
with.test_framework
with.library :rails
end
end
Add additional
Requires supporting
spec/support/ and its
run as spec files by
in _spec.rb will

- **1) Desensamblado**

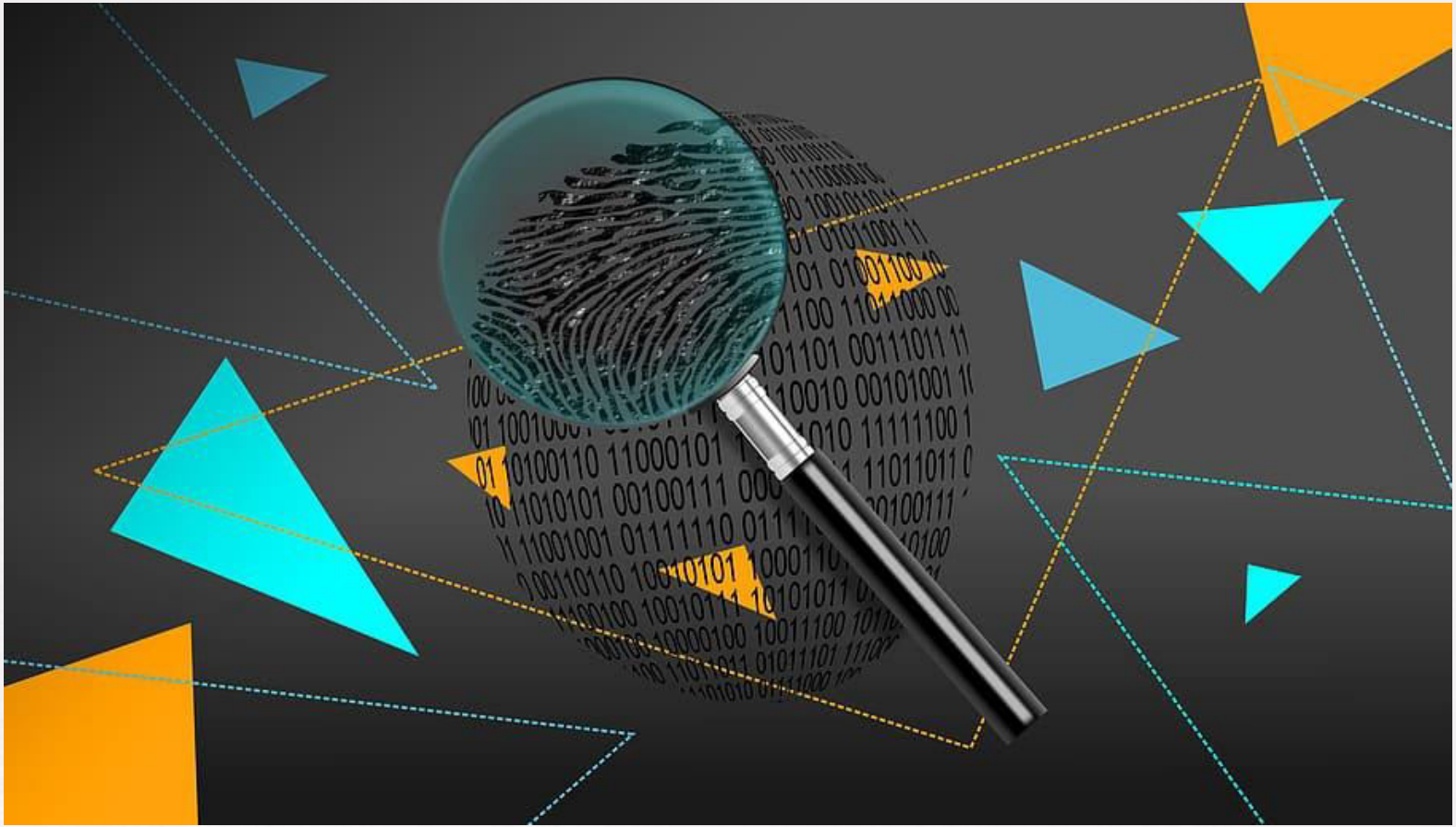
Esta técnica básica de análisis estático, nos permiten conocer desde afuera, información acerca del código malicioso.

Aprender a desensamblar códigos maliciosos a través del uso de técnicas de Ingeniería Inversa es una habilidad que lleva tiempo desarrollar y puede resultar complicada.



PASOS RECOMENDADOS

1) Reconocimiento.
2) Contención.
3) Identificación.
4) Comparación.
5) Extracción.
6) An. Estático.*
7) An. Dinámico.**
8) Informe.




CRACKS
DATA VIRUS
MALICIOUS SOFTWARE
THEFT
SOCIAL MEDIA ATTACKS
CYBERWARFARE
VIRUS
SOFTWARE FAILURE
NETWORK SNIFFING
YOUR DATA SAFETY
SPYWARE
HUMAN ERROR
SOFTWARE ERROR
STOLEN INFORMATION
TROJAN
CYBER ATTACKS
PASSWORD CRACKING
HACKING
FRAUD
CYBERCRIMINALS
TROJAN
ADWARE
SYSTEM PENETRATION
CYBERSTALKING

¡Nos vemos en la siguiente Clase!