Análisis de Malware

Comprensión y Análisis de Código Malicioso

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

SECCION 3
Laboratorio de Análisis.

Clase 1

Obtención de malware y análisis estático.

.

Obtención de malware:

Repositorios de malware:

-------- CUIDADO --------- MALWARE ACTIVO-------- CUIDADO ---

***p://www.offensivecomputing .net/
***p://www.textfiles .com/virus/
***ps://zeustracker.abuse .ch/
***p://contagiodump.blogspot .com/
***p://malware.dontneedcoffee .com/
***p://www.virusign .com/
***p://www.tekdefense .com/downloads/malware-samples/
***p://ytisf.github .io/theZoo/
***p://openmalware .org/
***p://secuboxlabs .fr/

-------- CUIDADO --------- MALWARE ACTIVO-------- CUIDADO ---

Se recomienda hacer descarga de malware directamente a maquinas virtuales “DESECHABLES”. Según el listado proporcionado o según sus propias búsquedas.

El análisis estático, se ejecutará directamente en la maquina virtual activando las herramientas descritas.

LABORATORIO


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!