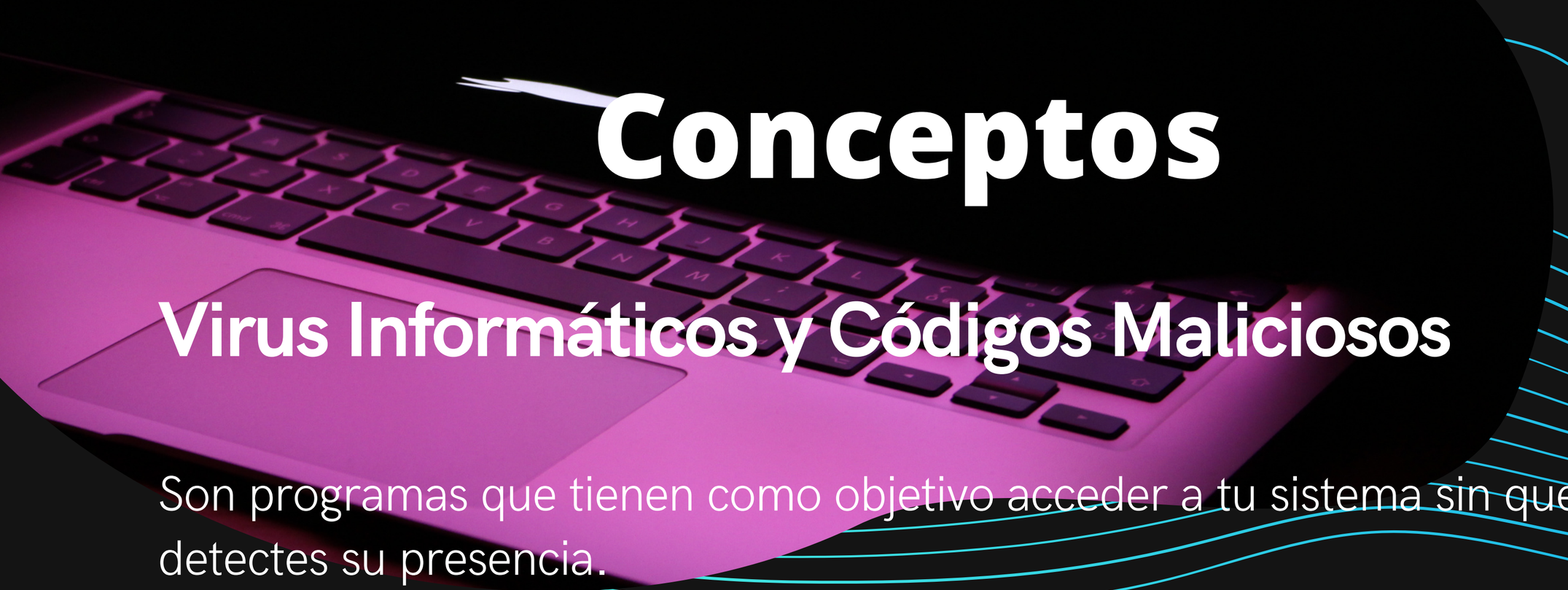
Virus Informáticos y Códigos Dañinos

GRUPO 1
ANGEL HERNÁNDEZ
CARLOS PINEDA
JESÉ HENRIQUEZ
HENRY ORTIZ
OSCAR VARELA



Conceptos

Virus Informáticos y Códigos Maliciosos

Son programas que tienen como objetivo acceder a tu sistema sin que detectes su presencia.

En función de la intención del Cracker, el programa podría:

- Robar credenciales, datos bancarios, información…
- Creación de redes con ordenadores botnet.
- Cifrado del contenido. Con esto se intenta que los usuarios paguen un rescate por sus datos.

Historia

El primer virus informático que se conoce fue desarrollado en 1971 por Robert Thomas, ingeniero de BBN Technologies. Conocido como el virus “Creeper”, este programa experimental infectó los mainframes en la red Arpanet, mostrando en el teletipo el mensaje: “Soy creeper: Atrápame si puedes”.

El primer virus informático verdadero que se descubrió de forma natural fue “Elk Cloner”, que infectaba el sistema operativo de Apple II a través de los disquetes, mostrando un mensaje humorístico en las computadoras anunciando que estaban infectadas.

Este virus desarrollado en 1982 por Richard Skrenta, de 15 años de edad, fue diseñado como una broma. Sin embargo, demostraba cómo se podía instalar un programa potencialmente malicioso en la memoria de una computadora Apple, evitando que los usuarios lo eliminaran.
El término “virus informático” no fue usado sino hasta un año después. Fred Cohen, un estudiante graduado de la Universidad de California, escribió un artículo académico titulado “Virus informáticos: teoría y experimentos”. En este artículo se acreditó a Leonard Adleman, su asesor académico y cofundador de RSA Security, por acuñar en 1983 el vocablo “virus informático”.

Características de los Virus Infomáticos

POLIMÓRFICOS

Algunos virus informáticos pueden tener muchas formas. Determinadas variedades se caracterizan por su capacidad para transformar su código, y precisamente al ser polimorfos (también llamados mutantes) son mucho más difíciles de detectar y eliminar

RESIDENTES Y NO RESIDENTES

Los virus informáticos pueden ser residentes o no residentes en la memoria del ordenador, o sea quedar o no de forma permanente en la memoria del equipo. Los virus no residentes se caracterizan porque el código del virus se ejecuta solamente cuando un archivo determinado es abierto

TRABAJO INTEGRADO

Determinados virus pueden atraer a otros, haciendo más letal su actividad. Incluso se ayudarán para esconderse y se asistirán al momento de contaminar una unidad específica del dispositivo.

ACTIVIDAD SILENCIOSA

Ciertos virus informáticos pueden llegar a ocultar los cambios que realizan dentro del ordenador, es decir que el sistema no mostrará signos de infiltración de virus. Esta característica puede hacer aún más dificultosa su detección.

Características de los Virus Infomáticos

RESISTENCIA AL FORMATEO

En unos pocos casos, los virus informáticos pueden permanecer en el sistema aunque el disco duro haya sido formateado. Este tipo de virus se caracteriza por tener la capacidad de infectar porciones muy específicas de la computadora, ya sea en el CMOS o albergarse en el MBR (registro de arranque principal).

MUTABILIDAD

Algunos virus informáticos modifican su propio código para evadir la acción de los antivirus, creando alteraciones de sí mismos en cada copia.

Tipos de Virus

- Virus
- Gusanos
- Troyanos
- Keyloggers
- Spyware
- Bots Maliciosos
- Virus de Macros

Tipos de Virus

- Pharming
- Virus de Archivo
- Secuestradores del Navegador
- Virus de Secuencia de Comandos (Scripting)
- Virus del Sector de Arranque
- Phishing

Tipos de Virus

Bombas Lógicas

Jockers

Ejemplos de Virus Infomáticos

MELISSA

fue un macro virus que se expandió a través de archivos adjuntos a emails y causó unas pérdidas de 80 millones de dólares.

YANKEE DOODLE

fue un virus de archivo no destructivo de origen búlgaro, que iniciaba la reproducción de la canción "Yankee Doodle" en los ordenadores infectados todos los días a las 17 horas.

SHAMOON

es un virus destructivo que borraba todos los datos de redes de ordenadores en cuestión de segundos.

KLEZ

ffue un macro virus que deshabilitaba el software antivirus en el ordenador infectado y enviaba correo no deseado (spam) a la bandeja de entrada de la víctima para impedir la recepción de nuevos mensajes.


Microaprendizaje: ¿Qué es un virus informático?
Share
Watch on YouTube