Seguridad Informática con Kali GNU/Linux

Clase 2: Malwares

UNIVERSIDAD TECNOLOGICA NACIONAL

Malware

Definición de Malware

UNIVERSIDAD TECNOLOGICA NACIONAL

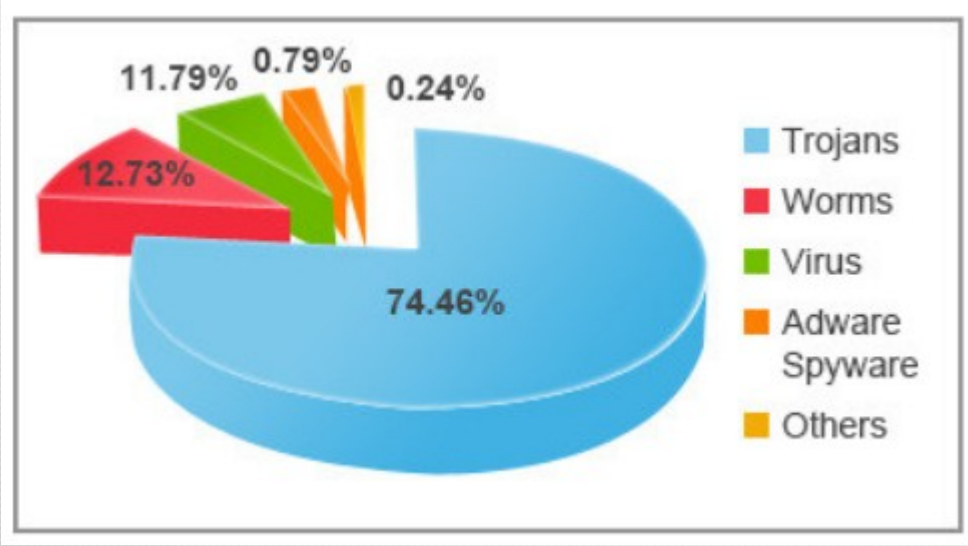
Malware significa Malicious Software (software malicioso).
Se denomina malware al software malicioso, diseñado para llevar cabo acciones no deseadas y sin el consentimiento explícito del usuario.
Es el término usado para referirnos a cualquier tipo de software cuya finalidad es causar algún daño, robar información, acceder a sistemas privados o mostrar publicidad no deseada.
Afectan todo tipo de sistema operativo y están escritos en distintos lenguajes.
Por lo tanto, el malware es el término principal que se utiliza para hablar de todas las amenazas informáticas.

Tipos de Malware

UNIVERSIDAD TECNOLOGICA NACIONAL

- Existen muchas clasificaciones en internet; cada autor enumera los tipos de malware a su manera.
- Los que vamos a enumerar nosotros son:

Dentro de esta categoría ya tenemos diferentes clasificaciones bastante más específicas de para las amenazas, como la de los troyanos, los gusanos, los virus informáticos, el adware, el spyware o ransomware entre otras.



Sin embargo no son malware todos los programas que pueden exponer tus datos. Tenemos que distinguirlo del software defectuoso, que son esos programas que no se han diseñado con malas intenciones, pero que tienen determinados errores dentro de su código por culpa de los cuales tu información puede quedar expuesta o tu sistema se hace vulnerable a determinados peligros.

Virus

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer virus:** Creeper (1971)
- **Características:** Se replican en los sistemas, reproduciéndose a si mismo o infectando otros programas y modificándolos.
- **Ejemplos:**
  - Elk Cloner (1982)
  - SCA virus (1987)
  - ILOVEYOU (2000)

Gusanos

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer gusano:** Morris (1988)
- **Características:** También se replican como los virus, pero no modifican otros programas. Pueden contener código malicioso para causar daños en el Sistema.
- **Propagación:** Emails, explotando vulnerabilidades en internet, etc.

- **Ejemplos:**
  - Wank (1989),
  - Slammer (2003)

Adware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer adware:** Es difícil de precisar ya que al principio se lo consideraba spyware. También es conocido como PUP (Potentially Unwanted Program), Malvertising y click-fraud.
- **Características:** Muestran o descargan publicidad no deseada al usuario para generar ganancias. Pueden recolectar información para saber los gustos del usuario y presentar publicidades acordes a esos gustos. También puede redireccionar las búsquedas del usuario a páginas publicitarias.
- **Propagación:**
  - Toolbars, browser extensions, etc.

Spyware

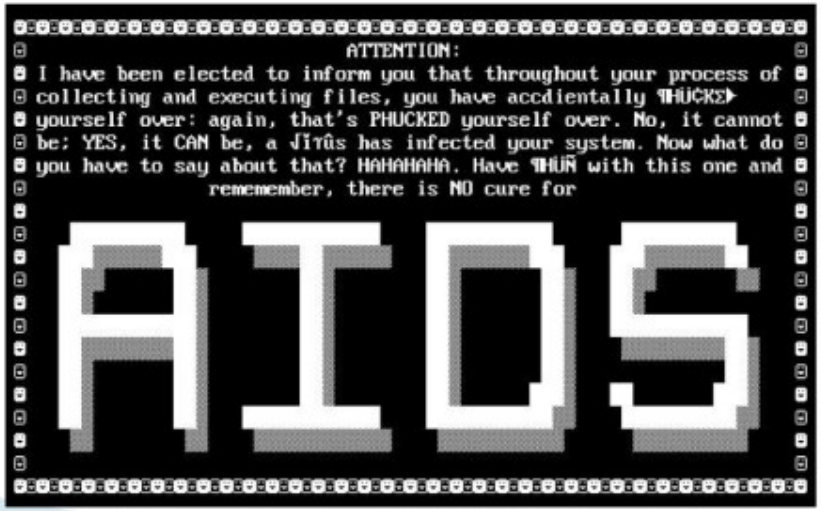
UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer spyware:** El termino surgió en 1995 en un post.
- **Características:** El objetivo es robar información y enviarla a un servidor externo sin el consentimiento de la victima. Muchos consideran a los adware y ciertos tipos de troyanos como spyware.
- **Empresa conocida que genera Spyware:** Hacking Team
- **Subtipos:**
  - Keyloggers (iSpy)

Ransomware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer ransomware:** AIDS (1989)
- **Características:** Pide un monto de dinero a la víctima a modo de "rescate" (ransom significa rescate) para que pueda volver a disponer de su información. Funcionan de forma online y offline.
- **Propagación:** Emails, downloaders, documentos de Office, sitios comprometidos, adware, exploit kits, etc.



Ransomware

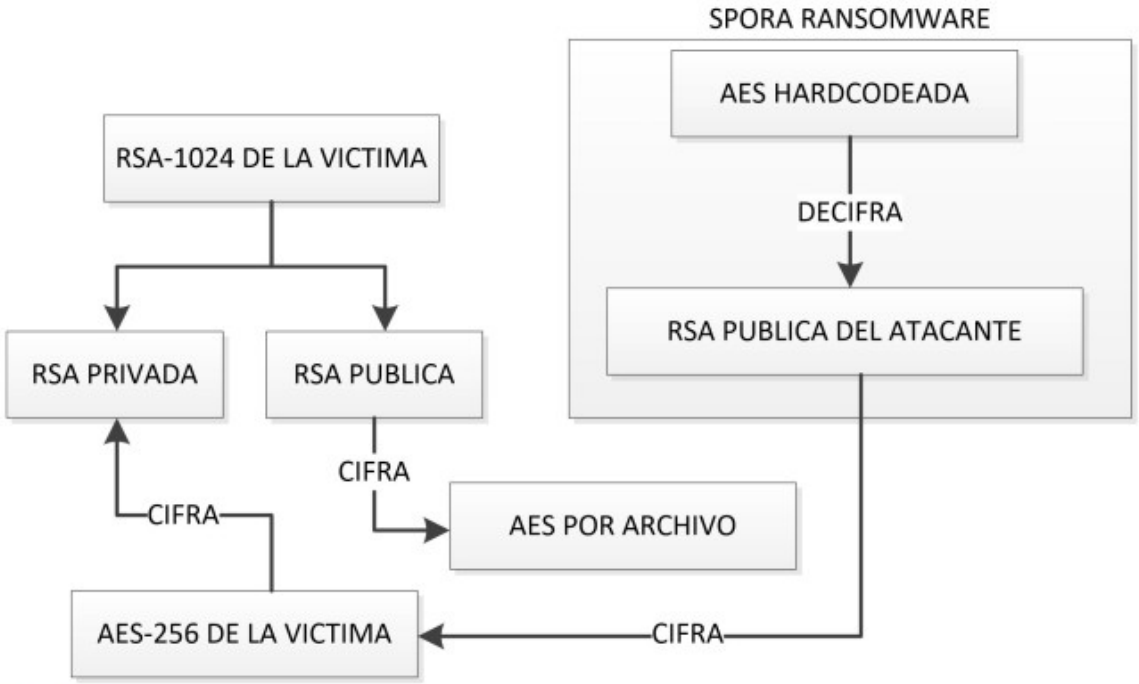
UNIVERSIDAD TECNOLOGICA NACIONAL

- **Subtipos:** Crypto, Locker, Ransom-as-a-service, Doxware, Cryptworm

Ransomware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **Spora offline**



Troyanos

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer troyano:** ANIMAL (1975)
- **Características:** El termino troyano se usa para todo malware que disfraza su verdadera intención.
- **Subtipos:**
  - **Downloaders:** Engañan al usuario para que los ejecuten y luego bajan otras amenazas. Ej: Fareit, Nemucod.
  - **Banking Trojans:** Se encargan de robar credenciales bancarias de los usuarios y números de tarjetas de crédito. Ej: Zeus, Tiny, Trickbot, Shifu.
  - **Backdoor:** Proporcionan una forma de acceder a un sistema sin ser detectado por programas de seguridad. Ej: Carbon, BlackEnergy.

Troyanos

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer troyano:** ANIMAL (1975)
- **Características:** El termino troyano se usa para todo malware que disfraza su verdadera intención.
- **Subtipos:**
  - **Rootkits:** Escalan privilegios para permitirle al atacante realizar acciones que requieren privilegios de administrador, ya sea explotando vulnerabilidades o usando credenciales. Ej: ZeroAccess
  - **Bootkit:** Infectan el MBR (Master Boot Record), con lo cual se ejecutan antes del SO. Ej: BOOTRASH
  - **RAT (Remote Access Trojan o Remote Administrator Tool):** Arquitectura cliente-servidor. Ej: Spyeye, DarkComet.
    - **Botnet:** Red de computadoras infectadas que son usadas para mandar spam, infectar con otras amenazas o hacer ataques DDoS. Ej: Mirai, Brickerbot.

Exploit Kits

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer Exploit Kit:** MPack (2006)
- **Características:** Diseñados para correr en web servers con el propósito de identificar vulnerabilidades en clientes y poder explotarlas para descargar y ejecutar otro malware. Generalmente disponen de una interfaz.
- **Ejemplos:**
  - RIGEK, SundownEK, AnglerEK

ATM & PoS malware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer ATM malware/ATM Skimmer:** Se cree que fue en 2008 que aparecieron los dispositivos.
- **Características:** Puede ser usado junto a dispositivos físicos, lo que se conoce como ATM Skimmers. Puede ser distribuido a través de CDs que se utilizan para instalar el malware en backoffice y luego una "mula" ingresa una clave especial en el cajero para acceder al panel del malware y obtener dinero.
- **Ejemplos:**
  - Alice, Ploutus, Tyupkin

ATM & PoS malware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer PoS malware: Rdasrv (2011)**
- **Características:** El objetivo es obtener información de tarjetas de crédito y/o debito a través de terminales de puntos de venta, leyendo su memoria. La información de las tarjetas que generalmente se cifra y se envía para ser autorizada, es interceptada y enviada al criminal.
- **Ejemplos:**
  - BlackPoS, PunkeyPoS, CenterPoS

“Fileless” malware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **El primer Fileless malware:** Poweliks (2014)
- **Características:** No generan archivos, sino que directamente corren en memoria, lo cual les da cierta capacidad para ser indetectables. Pueden ganar persistencia en el sistema. Generalmente esconden su código en registros de Windows, en el espacio de memoria de un archivo legitimo o en APIs (Application Programming Interface).
- **Ejemplos:**
  - Kovter, Phasebot, XswKit, DNSMessenger

Malware en distintos Sistemas Operativos

UNIVERSIDAD TECNOLOGICA NACIONAL

- **Android**
  - HummingWhale
  - Gooligan
  - Ghost Push
- **Linux**
  - Mirai
  - Amnesia
- **IOS**
  - AceDeceiver
  - XCodeGhost
- **OS X**
  - Pegasus
  - Fruitfly
  - Dok

Formas de propagación

UNIVERSIDAD TECNOLOGICA NACIONAL

- **Campañas de email**
  - URL
  - Adjuntos
    - Malware Payload
    - Downloader
    - Documentos de Office
    - PDF
- **Sitios comprometidos**
  - Adware
  - Campañas
    - ElTest
    - Pseudo Darkleech
    - Afraidgate

Clasificación: principales características (I)

- Virus: auto-réplica, infectan otros programas.
- Gusano: se replica mediante copias de sí mismo, pero no infecta a otros programas.
- Troyano: no se replica ni infecta a otros programas de forma automática e indiscriminada.
- Adware: presenta publicidad no deseada.
- Keylogger: captura pulsaciones en el teclado, espía lo que el usuario escribe.

Clasificación: principales características (II)

- Rootkit: usa técnicas para permanecer oculto en el sistema ante el usuario y las aplicaciones de seguridad.
- Backdoor: función de puerta trasera, permite al atacante conectarse y controlar la máquina infectada.
- Dialer: realiza llamadas de tarificación especial, incrementando la factura telefónica.
- Bot: los sistemas infectados son "zombies" que conforman una "botnet" o red de bots; esta red acepta órdenes de forma remota.

Clasificación: principales características (y III)

- Ransomware: cifra documentos y archivos, pide al usuario que pague un rescate si quiere la clave que permita acceder a los originales.
- Rogueware: falso antivirus, te hacen creer que el sistema está infectado y cobran para la supuesta desinfección.
- Crimeware: nueva denominación para el malware orientado al cibercrimen y fraude, con un claro interés de lucro.

Principales métodos de infección

- Descarga desde páginas webs.
- Adjuntos por email.
- Vulnerabilidades en software.
- Compartir dispositivos de almacenamiento.
- Otros protocolos y aplicaciones en Internet:
  - mensajería instantánea.
  - P2P.
  - redes sociales, etc.

Medidas para prevenir infecciones

- Usar antivirus actualizado.
- Actualización del sistema operativo, navegador y resto de aplicaciones.
- Uso de usuario restringido vs administrador.
- Sentido común y uso responsable:
  - Evitar abrir correo no deseado y enlaces llamativos en las redes sociales.
  - Evitar abrir documentos e instalar software de fuentes no confiables.

Análisis de Malware

UNIVERSIDAD TECNOLOGICA NACIONAL

- **Estático**
  - Recabar información sobre la amenaza, sin ejecutarla (fecha de compilación, ofuscador, strings resources).
    - Pestudio, Dependency Walker, PEiD, Resource Hacker
- **Dinámico**
  - Se ejecuta el malware y se realiza un seguimiento de las acciones que realiza. Relacionado con Debugging.
    - Process Monitor, Process Explorer, Fakenet, Wireshark, Regshot.
- **Ingeniería Inversa**
  - Obtener información de un archivo (generalmente cuyo código fuente no se dispone) para entender cómo funciona. Se lo vincula con el cracking.
    - IDA Pro, Ollydbg, ILSpy