Malware

José Galaviz

Definición

Cualquier tipo de programa diseñado para violar la seguridad de un sistema informático.

- Es intencional.

Virus

- Un programa oculto dentro de otro programa que sí es útil.
- Cuando se ejecuta es capaz de reproducirse copiándose en otros programas.
- Puede además llevar a cabo acciones como alterar o borrar datos, ralentizar el sistema o inutilizarlo.

Spyware

- Infiltran el sistema, permanecen ocultos.
- Recopilan datos del usuario u otros usuarios y la transmiten.
- Roban información confidencial.

Ransomware

- Secuestra datos del sistema.
- Los cifra o los envía a otro lado.
- amenaza con no descifrarlos o publicarlos a menos que se pague una suma.
- Típicamente en criptomonedas a monederos no rastreables.
- Mayo de 2013 a septiembre de 2014, CryptoLocker,

Caballo de troya

- Programa malicioso disfrazado de un programa útil.
- El propio usuario lo descarga y lo ejecuta.
- Normalmente establecen una puerta trasera en el sistema para que alguien pueda tener acceso no autorizado.
- Actúan como spyware, recolectando y transmitiendo información confidencial.
- Normalmente no se replican o transmiten a sí mismos.

Gusano (worm)

- Se replica y usa la conectividad del sistema infectado para propagarse a otros sistemas.
- Desde cada sistema infectado continúa propagándose.

Bomba lógica

- Fragmento de código inserto en otro programa útil.
- Cuando se cumple alguna condición se desata algún tipo de ataque.
- Julio de 2019 Siemens.

Rootkit

- Colección de programas maliciosos operando en colaboración.
- Gana privilegios de administración a través de alguna vulnerabilidad explotable (exploit).
- Programas del sistema que realizan acciones ocultas.
- Difícilmente detectables: alteración de listado de procesos, de loggers, de listado de archivos.
- En los peores casos, reemplazo del kernel.

Detección

La detección corre a cargo de software antivirus, aunque de funcionalidad extendida.

- Firma: buscando fragmentos de código conocidos.
- Heurística: Software que “muta” y cambia su código cada vez que infecta: buscando emparejamientos imperfectos.
- Caja de arena: ambiente virtual protegido y monitoreado para detectar comportamiento anómalo.
- Inteligente: data mining y reconocimiento de patrones para detectar comportamiento inusual.

Problemas

- Costo del software de protección.
- Alto costo en desempeño.
- Falsos positivos.
  - Remover software útil.
- Efectividad.
- Código polimórfico: cambios en el código que no restan funcionalidad.

Hay que protegerse

- Cualquier recurso de cómputo es un recurso valioso, no por lo que contiene, sino por lo que puede hacer.
- Para montar:
  - Envío de spam, phishing.
  - Acceder de allí a otros sistemas.
  - Negación de servicio distribuido.

Temas afines

- Phising. Robo de mecanismos de autenticación a través de engaño.
- SQL Injection. Servicios web basados en bases de datos, modificando el query se puede lograr obtener datos no autorizados