SEGURIDAD INFORMATICA

19	Adware
20	Control Remoto de Equipos (forma maliciosa)
21	Trashing

*Amenaza Adware (Thiago)

A: El adware es un tipo de software que muestra anuncios no deseados en la pantalla de tu dispositivo, ya sea una computadora o un móvil. A menudo, se instala junto con otros programas gratuitos o se obtiene a través de descargas sospechosas.

B: Su objetivo principal es generar ingresos para sus desarrolladores mostrando publicidad.

Tiene la capacidad de mostrar anuncios publicitarios de manera constante, incluso cuando el usuario no está navegando en internet.

Causar molestias: Estos programas tienden a generar anuncios de poca calidad, que resultan irritantes para el usuario.

C: El adware se ocasiona principalmente a través de descargas de software, tanto legítimo como fraudulento, que incluyen el adware como componente oculto.

D: Para evitar el adware, es crucial tomar medidas preventivas como utilizar software de seguridad confiable, mantener el software y el sistema operativo actualizados, descargar aplicaciones solo de fuentes oficiales, y ser cauteloso con los enlaces y archivos sospechosos.

https://www.google.com/search?q=como+evitar+el+ADWARE&num=12&sca_esv=284c23966837c08f&biw=1034&bih=613&ei=hcljaNKOGreJ5OUPxtaqsQ8&ved=0ahUKEwiS5eCNypuOAxW3BLkGHUarKvYQ4dUDCBA&uact=5&oq=como+evitar+el+ADWARE&gs_lp=Egxnd3Mtd2l6LXNlcnAiFWNvbW8gZXZpdGFyIGVsIEFEV0FSRTIEEAAYHjIGEAAYCBgeMgYQABgIGB4yCBAAGIAEGKIEMggQABiABBiiBDIFEAAY7wVIul9QyQlYhlhwB3gBkAEAmAF7oAGFD6oBBDIyLjG4AQPIAQD4AQGYAh6gAvwQwgIKEAAYsAMY1gQYR8ICBhAAGAcYHsICCBAAGAcYChgewgIIEAAYBxgIGB6YAwCIBgGQBgiSBwQyNi40oAfYdbIHBDE5LjS4B8cQwgcIMC43LjkuMTTIB9YB&sclient=gws-wiz-serp

https://youtu.be/3JJB6Jz2NlY?si=OesnBSblHcXUM6in

*Control Remoto de Equipos : (Joaquin)

(Forma maliciosa)

A: El control remoto malicioso de equipos se refiere a la capacidad no autorizada que tiene un atacante para acceder y manipular un dispositivo (como una computadora, servidor, smartphone, o cualquier otro equipo conectado a una red) a distancia, sin el consentimiento o

conocimiento de su propietario legítimo. El objetivo principal de este tipo de acceso es realizar actividades dañinas o ilegales.

B: Las características principales del control remoto malicioso de equipos se centran en cómo se logra y qué capacidades le otorga al atacante.

1. **Acceso no Autorizado**
2. **Persistencia**
3. **Ocultamiento y Evasión**

C: este control se logra mediante la instalación de software malicioso (malware) en el equipo de la víctima. Este malware puede incluir:

Troyanos de Acceso Remoto (RATs): Son programas diseñados específicamente para permitir el control total del equipo infectado desde una ubicación remota.

Backdoors (Puertas Traseras): Puntos de entrada ocultos en el software o hardware que permiten el acceso no autorizado.

Keyloggers: Software que registra cada pulsación de teclado, permitiendo al atacante capturar contraseñas y otra información sensible.

Spyware: Programas que monitorean y recopilan información sobre la actividad del usuario sin su conocimiento.

D: Evitar el control remoto malicioso de equipos es fundamental para proteger tu privacidad, tus datos y tu seguridad digital. La prevención se basa en una combinación de buenas prácticas, herramientas de seguridad y una actitud vigilante. Aquí te detallo las principales estrategias:

1. Mantener el Software Actualizado (Sistemas Operativos y Aplicaciones)

Importancia: Las actualizaciones suelen incluir parches de seguridad que corrigen vulnerabilidades conocidas que los atacantes podrían explotar

para obtener acceso remoto.

Acción: Habilita las actualizaciones automáticas para tu sistema operativo (Windows, macOS, Linux, Android, iOS) y para todas tus aplicaciones (navegadores web, programas de oficina, reproductores multimedia, etc.). Si no son automáticas, revísalas y aplícalas regularmente.

2. Utilizar Software de Seguridad Confiable

Antivirus/Antimalware: Instala y mantén actualizado un programa antivirus o antimalware de buena reputación. Realiza análisis completos del sistema periódicamente.

Firewall: Asegúrate de que tu firewall (el del sistema operativo y/o el de tu router) esté activado y configurado correctamente para bloquear conexiones no autorizadas entrantes y salientes.

E:https://gemini.google.com/app/7412f2e3fa935121?hl=es#:~:text=Evitar%20el%20control,entrantes%20y%20salientes.

Trashing (Ortiz Leonel)

- Trashing se refiere a la práctica de buscar información sensible o confidencial en la basura (basureros, papeleras, etc.), con el fin de obtener datos útiles, como contraseñas, documentos financieros, información personal, etc.
-
- Amenaza de tipo física y social
- Bajo nivel técnico requerido
- Acceso a información confidencial

- Difícil de detectar
- Puede ser el primer paso de un ataque mayor
- El trashing se da principalmente por una mala gestión de la memoria virtual, y suele ocurrir en los siguientes escenarios:

Demasiados procesos activos:

Cuando el sistema ejecuta más procesos de los que puede manejar con la RAM disponible, se ve obligado a intercambiar constantemente páginas de memoria entre RAM y disco.

Falta de memoria física:

Si la RAM es insuficiente, el sistema depende excesivamente de la memoria virtual (disco), lo que provoca intercambios frecuentes.

Poca localidad de referencia:

Si los procesos acceden a datos dispersos en la memoria (no siguen un patrón de acceso localizado), el sistema necesita traer muchas páginas distintas en poco tiempo, lo cual genera constantes fallos de página (page faults).

Algoritmos de reemplazo ineficientes:

Si el sistema operativo usa un mal algoritmo para decidir qué páginas sacar de la RAM (como un reemplazo FIFO sin control de localidad), puede expulsar páginas que se volverán a necesitar de inmediato.

Sobrecarga del scheduler:

Si muchos procesos compiten por la CPU y la memoria, el planificador del sistema puede hacer demasiados cambios de contexto, aumentando la necesidad de paginación.

d) ✅ 1. Aumentar la memoria física (RAM)

Si el sistema tiene muy poca RAM, usará con más frecuencia la memoria virtual (más lenta).

Solución directa: añadir más memoria física reduce la necesidad de paginación.

✅ 2. Controlar el grado de multiprogramación

Multiprogramación es la cantidad de procesos que se ejecutan simultáneamente.

Si hay demasiados procesos activos, compiten por la RAM, lo que genera page faults y lleva al trashing.

Solución: reducir el número de procesos concurrentes (por ejemplo, limitando el uso del sistema por parte de usuarios o servicios).

✅ 3. Usar algoritmos de reemplazo de páginas eficientes

Algoritmos como LRU (Least Recently Used) o Clock son mejores que FIFO para evitar reemplazar páginas que se necesitarán pronto.

Esto reduce los fallos de página innecesarios.

e)
https://www.tutorialspoint.com/operating_system/operating_systems_thrashing.htm?utm_source=chatgpt.com

https://www.geeksforgeeks.org/operating-systems/techniques-to-handle-thrashing/?utm_source=chatgpt.com

https://youtu.be/Uqel2_88oc8?si=I_Jx3F1YHOVCA7oH