Edición No. 6 – mayo 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

Ataques por Malware

Recordemos que los ataques por *malware* se sirven de programas maliciosos cuya funcionalidad ***consiste en llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad.*** Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico o tomar el control de su equipo. Con este boletín seguiremos aprendiendo sobre los diferentes ataques que existen por Malware, estemos atentos **¡la Seguridad es de todos!**

Keyloggers

Realizan un seguimiento y registran cada tecla que se pulsa en un equipo sin nuestro consentimiento. Pueden estar basados en un *software* o en un *hardware*, como por ejemplo un dispositivo USB.

Stealers

Este tipo de troyano ***accede a la información privada almacenada en el equipo.*** Al ejecutarse, analiza los programas instalados y las credenciales almacenadas para luego, compartirlas con el atacante.

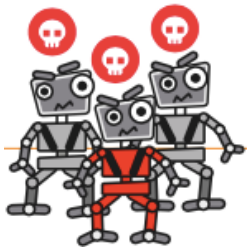
Gusano

Se trata de un tipo de malware que, una vez ejecutado en un sistema, ***puede modificar el código o las características de este***. Generalmente, pasan hasta que su proceso de reproducción se hace evidente, produciendo consecuencias en el rendimiento de nuestro equipo.

Rootkit

Es un ***conjunto de herramientas utilizadas por los ciberdelincuentes para acceder de forma ilícita a un sistema.*** Una vez dentro, se utilizaran para mantener al atacante con acceso al sistema y poder llevar a cabo otro tipo de ciberataques.

Botnets



Así́ se conoce a la ***red compuesta por diversos dispositivos infectados y controlados de forma remota por uno o varios ciberdelincuentes.***

Rogueware

Se trata de un ***software malicioso que simula ser un antivirus o herramienta de seguridad*** y que nos alerta de un problema con nuestros dispositivos.

Pueden alertar sobre la presencia de un malware, una amenaza o un problema que hay que corregir. Rápidamente, nos invitará a hacer clic en un botón o enlace para descargar un supuesto software con el que solucionar el problema.

Edición No. 6 – mayo 2021

Seguridad Informática en el sector Salud

¡Porque la seguridad es de todos!

Criptohacking

Es una práctica por medio de la cual, los ciberdelincuentes ***utilizan nuestros dispositivos sin nuestro consentimiento para llevar a cabo "extracciones" de criptomonedas.*** Durante el proceso, utilizan los recursos del sistema.

¿Cómo se propaga o infecta el malware? se propagan por medio de archivos adjuntos en correos electrónicos o desde paginas webs poco fiables, escondiéndose tras descargas de juegos, películas o aplicaciones no legitimas. Nosotros, confiados, no somos conscientes de que nuestros equipos han sido infectados hasta que es demasiado tarde. En ocasiones, vienen ocultos en dispositivos USB que conectamos a nuestros equipos sin ser conscientes del peligro.

¿Cuál es su objetivo? Su objetivo es monitorizar nuestra actividad y recoger datos que el atacante pueda utilizar para robar cuentas, información y perpetrar otro tipo de ataques.

Proponemos el siguiente ***listado de buenas prácticas en ciberseguridad para mejorar la protección de los dispositivos y la seguridad de la información frente a los ciberataques:***

- ✔ **Utiliza contraseñas robustas y diferentes** para proteger todas tus cuentas. Si es posible, utiliza la verificación en dos pasos u otro factor de autenticación.
- ✔ **Desconfía de los adjuntos sospechosos, enlaces o promociones demasiado atractivas.** La mayoría de los fraudes se basan en ataques de ingeniería social que pueden ser detectados aplicando el sentido común. En caso de recibirlo, se debe reportar de inmediato al correo de Seguridad de tu institución o al área de informática, adjuntando el correo sospechoso.
- ✔ **Ten cuidado por dónde navegas**. Utiliza solo webs seguras con https y certificado digital y utiliza el modo incógnito cuando no quieras dejar rastro.
- ✔ **Descarga solo de sitios oficiales** aplicaciones o software legitimo para evitar acabar infectado por malware. En el caso de las aplicaciones, recuerda dar solo los permisos imprescindibles para su funcionamiento.
- ✔ **Evita conectarte a redes wifi públicas o a conexiones inalámbricas desconocidas.** Especialmente cuando vayas a intercambiar información sensible, como los datos bancarios. Y, en caso de que tengas que conectarte por una emergencia, trata de utilizar una VPN.
- ✔ **No compartas tu información personal** con cualquier desconocido ni la publiques o guardes en páginas o servicios webs no fiables.
- ✔ **Haz copias de seguridad** para minimizar el impacto de un posible ciberataque.
- ✔ **No descargue contenido multimedia** por redes de intercambio tales como Ares.
- ✔ **Apagar el equipo de cómputo cuando termine su jornada laboral**, no solo previene que sea blanco de un ataque, sino que mejora el rendimiento, ahorra energía y previene el desgaste innecesario de este.

Fuente: INCIBE y la Oficina de Seguridad del Internauta (OSI).

Recuerda tratar tus contraseñas como a tu cepillo de dientes, no dejes que nadie más la use y cámbialas con frecuencia