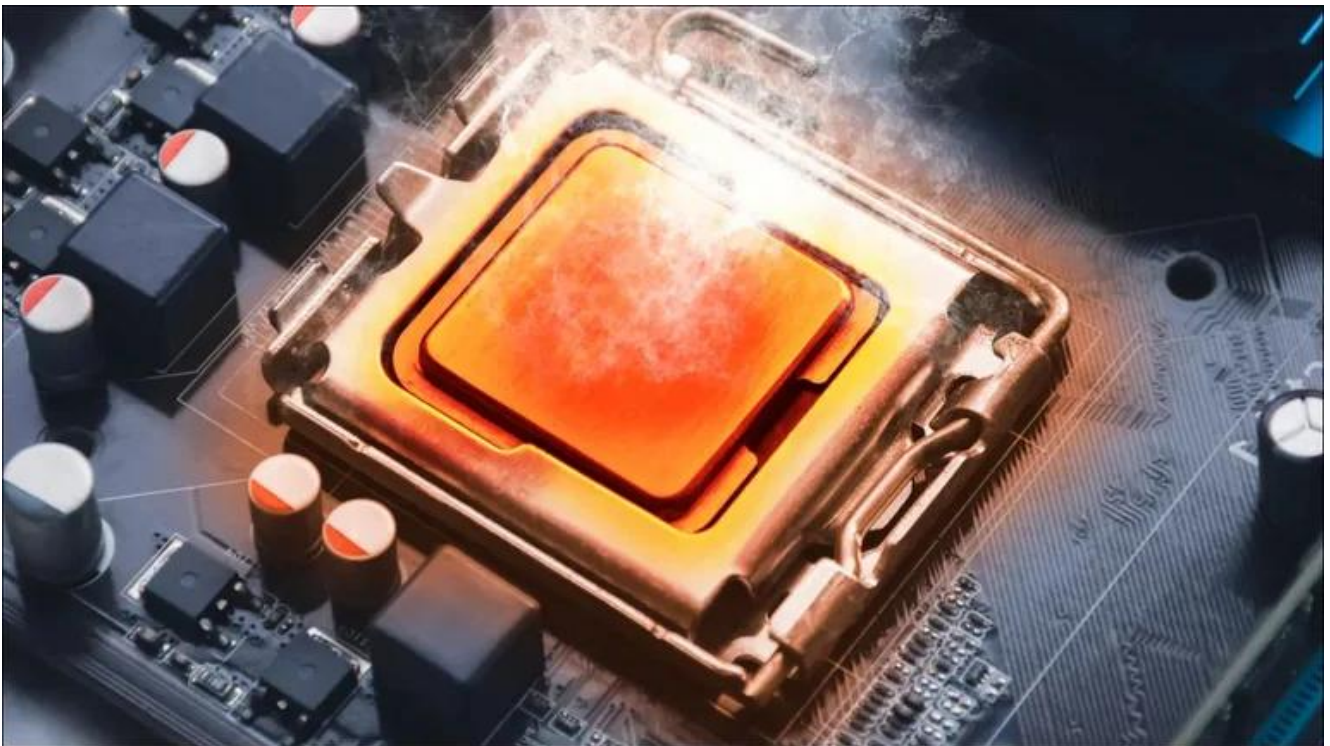


Estos virus ingresan al computador o laptop y queman su batería

02/01/2023



Los **virus** tienen diversas variantes y tipos que permiten a los **cibercriminales** ejecutar comandos dentro de una computadora ajena para robar **información**. Sin embargo también hay otros tipos que no solo afectan los sistemas de un dispositivo, sino que tienen la misión de dañar físicamente una **laptop** o una **PC**.

Si bien cada parte de los **dispositivos** tienen un periodo de prueba antes de salir al mercado en el que se determina el límite de sus capacidades de procesamiento de la **energía**, los **virus** de este tipo buscan superar los umbrales establecidos por especialistas.

Los “**virus de poder**” o “**virus de energía**”, como se les conoce a este tipo de **malware** se encargan de que el computador o dispositivo al que están afectando supere su **capacidad**

energética y se genere calor al interior del dispositivo hasta un punto en el que sea imposible de soportar para los componentes de la **computadora**.



Los virus de energía pueden causar daños irreparables a un dispositivo.

Una vez que un **malware** de este tipo se infiltra en un dispositivo y empieza a ejecutar sus comandos, las personas podrán experimentar un aumento progresivo en la **temperatura** de sus laptops o PCs de escritorio y “freír” la **CPU**, la **tarjeta gráfica** o en el peor de todos los casos, la **placa madre**, lo que implicaría la necesidad de todo un nuevo sistema de componentes en el dispositivo.

Para ganar tiempo y evitar daños directos por parte de este tipo de **virus** a las computadoras, los usuarios podrían incluir dentro de ellas un **sistema de enfriamiento** que tenga la capacidad de soportar un incremento en la **temperatura** de forma sostenida.

Utilizar un antivirus también es una forma de actuar para evitar que los **malware** como este lleguen a ejecutar sus sistemas dentro de una **laptop** o **computador** de escritorio, por lo que no son un problema que genere mayor preocupación entre los usuarios, que deberán diferenciar entre un aumento de la temperatura del dispositivo por efecto de un **virus** o porque está ejecutando programas o aplicaciones que exigen de forma excesiva a la **CPU** o a la **tarjeta gráfica**.



La temperatura de una tarjeta gráfica (GPU) debe estar controlada para no tener problemas de rendimiento.

Cómo evitar ser víctima de malware

Los **virus** ingresan a los dispositivos de distintas formas, pero la más común de todas es el **phishing**, que representa el **80 %** de los incidentes que se reportan antes las autoridades y es una de las más sofisticadas. En esta, un **cibercriminal** envía un correo electrónico a los usuarios pretendiendo ser una persona o entidad de confianza con la

finalidad de obtener **claves de acceso** o **información** bancaria de las personas para luego robar su **dinero** o usar esos datos para nuevos ataques.

Para no ser una víctima de **ciberdelincuentes**, los usuarios deberán evitar visitar sitios web dudosos o fraudulentos que soliciten la descarga de aplicaciones o programas como una “necesidad” para poder ingresar. Actualmente **Google Chrome** ofrece un sistema de **navegación** avanzada que advierte sobre este tipo de direcciones y las etiqueta como “no seguras”.

En el caso de que se reciban **correos electrónicos** ofreciendo descuentos, renovaciones de servicios, indicando fallas en el pago de alguna **suscripción**, “ofertas únicas” de tiempo limitado, entre otras que generen una sensación de urgencia, lo más probable es que se trate de una **estafa online** que busca que los usuarios ingresen datos bancarios.



El phishing es la modalidad de ciberataque más común en el mundo.

Observar los datos de quien envía el **correo** se puede

diferenciar los mensajes reales de los falsos. Si las direcciones de correo terminan en @gmail.com, @outlook.com, @hotmail.com, entre otras que no corresponden con **emails** institucionales, puede que se trate de una **estafa**.

Fuente: Infobae