LITORALPRESS

Fecha: 15-04-2023
Medio: Las Últimas Noticias
Supl. : Las Últimas Noticias
Tipo: Ciencia y Tecnología
Título: **Pendrives ultra seguros borran todos los archivos si le meten mal la contraseña**

Pág. : 21
Cm2: 686,5

Tiraje: 91.144
Lectoría: 224.906
Favorabilidad: No Definida

La línea IronKey, de Kingston, están fabricados con un estándar de seguridad que aún nadie ha violado

Pendrives ultra seguros borran todos los archivos si le meten mal la contraseña

Estos dispositivos funcionan con claves y varias otras capas de seguridad. La contraseña ni siquiera se pone en la misma memoria USB.

CEDIDA

Para mayor seguridad, el dispositivo despliega un teclado virtual en la pantalla del computador, que se acciona con el mouse, para que el usuario no tenga que escribir la clave con el teclado.

FRANCISCO NÚÑEZ

Nada hacía presagiar que el viejo y fiel pendrive, compañero de miles de estudiantes y trabajadores que allí almacenaron cientos de megabites de libros, informes, trabajos y juegos, tendría un renacimiento estelar.

El auge del almacenamiento en la nube, que permite rescatar cualquier archivo desde cualquier lugar, pareció amenazar la existencia de la memoria flash. El problema de la nube es que esos datos almacenados en algún servidor se vuelven vulnerables una vez que alguien con cierto conocimiento se apodere del computador, teléfono o tablet del usuario.

¿Será el pendrive más seguro? No el convencional, al menos. Es más, es potencialmente peligroso.

"Lo que ocurre es que al ser una conexión física, inician automáticamente una transferencia de datos al enchufarlos. Eso ocurre antes de que un antivirus pueda revisarlo. Y hay un tiempo en el cual se puede meter, por ejemplo, un randomware que te encripta el disco duro, apaga el antivirus y te cobra en bitcoins por recuperar tus cosas", explica Jonathan Frez, doctor en Computación y académico de la Escuela de Informática y Telecomunicaciones de la Universidad Diego Portales.

Conscientes de esta problemática y pensando en la protección empresarial de datos, fabricantes de memorias USB le dieron una vuelta de tuerca al dispositivo y lo hicieron más seguro. Kingston, por ejemplo, lanzó al mercado la línea IronKey (disponible en Spdigital.cl, https://bit.ly/41tNprX), que cifran los datos y archivos que se guardan dentro.

"Nuestros productos hoy son fabricados con el estándar AES 256Bits, que hasta el día de hoy no ha sido superado. Son, por lo tanto, productos con el más alto estándar de seguridad. No hay un porcentaje de inviolabilidad bajo los estándares que hoy estamos fabricando los productos. Por otro lado los productos tienen una serie de características que hacen todavía más compleja la opción de violar el acceso seguro. Toda la operación de cifrado y acceso a la zona segura se hace en la misma unidad externa, no dejando rastros que puedan abrir un espacio para un hacker", destaca Francisco Silva, country manager Chile-Perú de Kingston Technology.

Fuerza bruta

Los modelos IronKey están protegidos contra ataques y fuerza bruta, lo que bloquea las contraseñas del usuario tras completar diez intentos consecutivos fallidos con passwords inválidos. Para más seguridad, la unidad borra los datos cuando la contraseña del administrador se introduce de manera errónea también luego de diez intentos.

"Es importante destacar que nuestros productos seguros realizan el proceso de encriptación sin necesidad de cargar software o alguna aplicación que necesite ser instalada en el computador, todo se realiza en el USB o SSD ya que cuenta con su propio chip controlador que genera el proceso de encriptado y es el encargado de dar acceso a la información, leer o escribir datos en la unidad segura", dice el ejecutivo.

Para que no queden rastros de la contraseña en el teclado o pantalla táctil una vez que se inserta el pendrive en el puerto USB, en el monitor se despliega un teclado virtual donde, efectivamente, se introduce la clave.

¿Qué es la encriptación?

La encriptación –responde Silva– es el proceso técnico por el cual la información se convierte en un código secreto que permite ocultar los datos que envías, recibes o almacenas. Básicamente, se usa un algoritmo para codificar los datos antes de que la parte receptora decodifique los datos mediante una clave de desencriptado.

La familia IronKey también está compuesta por el producto estrella de esta línea, un disco duro externo (en Falabella.com, https://bit.ly/43BBrOK) de hasta 1 TB de capacidad. Y aunque en un principio estaban orientados hacia el uso en empresas, cuenta Francisco Silva, hoy son cada vez más los usuarios particulares que los compran.

Por cierto, no son los únicos que tienen productos de este tipo. Sandisk vende en Chile sus pendrive Extreme Pro (disponible en Tecnosistec.cl, https://bit.ly/41yEOVb), que cuenta con cifrado de archivos y protección de contraseña, lo que sen hace gracias al software SanDisk SecureAccess, que viene dentro del dispositivo.

Crudos y cocinados

En una época en que la protección de datos personales se ha vuelto clave, nunca hay suficiente protección contra los amigos de lo ajeno. Por eso Jonathan Frez, doctor en Computación, recomienda tomar ciertos resguardos.

"Es lo mismo que sucede con la comida, no hay que mezclar los alimentos cocinados con los crudos. En este caso, hay que tener cuidado con que los pendrives de uso personal se usen en el trabajo, porque podrían tener ya algún virus. Hay que considerarlos como infectados y, por supuesto, si se tiene antivirus, escanearlos de vez en cuando", precisa.

"Por esta misma razón algunas empresas incluso apagan los enchufes USB de los computadores que utilizan sus trabajadores", añade.