¡CUIDADO! UN KEYLOGGER PODRÍA ESTAR REGISTRANDO TUS CONTRASEÑAS

En los últimos años, el número de ciberataques ha aumentado considerablemente, en especial a pymes, y conforme aumentaban, también lo hacían las estrategias empleadas por los ciberdelincuentes para aprovecharse de las vulnerabilidades de las empresas. Los *keyloggers* son un ejemplo de ello.

Aunque la tecnología en sí no es novedosa, la manera en que se distribuye o infecta nuestros sistemas sí ha cambiado. En este post explicamos qué es un *keylogger* y cómo protegernos.

¿QUÉ ES UN *KEYLOGGER*?

Esta herramienta tiene como objetivo principal el registro de las teclas de dispositivos sin que el usuario se percate, ya que dicha acción se lleva a cabo en segundo plano. La información registrada se almacena en un fichero al que una tercera persona puede acceder. De esta manera, un ciberdelincuente podría tener acceso a datos confidenciales, como podrían ser las credenciales bancarias.

Se pueden clasificar en dos tipos diferentes, dependiendo de la manera en la que se integran en el dispositivo:

- ***KEYLOGGER* COMO DISPOSITIVO HARDWARE**. Consiste en un dispositivo que se conecta al teclado. Puede encontrarse entre el conector del teclado y el del equipo, quedando a la vista u oculto en el interior del teclado. Por lo general, almacena la información en el propio dispositivo, por lo que recuperar los datos registrados requiere su extracción física.
- ***KEYLOGGER* BASADO EN SOFTWARE**. Es un *malware* que puede infectar el equipo, por ejemplo, a través de un enlace malicioso, al descargar un programa de una página no fiable o al conectar un dispositivo USB. La información registrada se envía en remoto a un tercero, lo que lo convierte en el tipo de *keylogger* más utilizado por los ciberdelincuentes.

Como comentábamos, los *keyloggers* basados en *software* se pueden distribuir de distintas maneras. De hecho, se han detectado algunas campañas de tipo *phishing* dirigidas directamente a empresas. Los mensajes distribuidos en estas campañas suelen incluir un archivo adjunto que, al descargarlo, infecta el dispositivo con

un *keylogger* para robar las credenciales personales y otra información sensible.

También existe el riesgo de que nuestro equipo se infecte con este *malware* al instalar programas o descargar archivos desde fuentes no fiables o al utilizar dispositivos USB de origen desconocido.

¿Y SI MI DISPOSITIVO SE INFECTA POR UN *KEYLOGGER*?

Ahora que conocemos su funcionamiento, pongamos un supuesto de lo que podría suceder si fuéramos víctimas de un *keylogger* y las implicaciones que tendría tanto en nuestra información personal como en la de nuestra empresa.

Se está buscando desde un computador una aplicación de edición para crear carteles y otro contenido para su empresa. En el buscador aparece una web publicitando una herramienta con toda clase de características incluidas y completamente gratuitas. Si se da cuenta de que la URL de la web no comienza por HTTPS y tampoco dispone de un apartado de aviso legal. Aunque estos detalles le hacen sospechar de su fiabilidad, acaba descargando la aplicación en su computador.

Una vez instalada la aplicación, observa que la aplicación no funciona y finalmente la borra, pero todavía no sabe que un *keylogger* ha infectado su equipo. Afortunadamente, no utiliza este computador para acceder a servicios que puedan guardar información sensible, pero utiliza las mismas contraseñas para todas sus cuentas, incluidas las de su empresa.

De esta manera, al darse de alta en otra plataforma de edición, ha facilitado las credenciales de sus redes sociales y correo personal y los accesos a los sistemas de su empresa. En consecuencia, un ciberdelincuente podría aprovechar esta información para ejecutar un ataque a su empresa o a sus colaboradores, comprometiendo su seguridad y dañando así su imagen de confianza y reputación.

Como se puede observar, los riesgos asociados a los *keyloggers* son significativos, pero se pueden limitar e incluso evitar aplicando de manera rigurosa algunas prácticas sencillas, entre las que destacan:

- Descargar aplicaciones únicamente de fuentes fiables. En el ámbito de la empresa es importante determinar las aplicaciones que se permiten descargar en los dispositivos. Para ello, contar con una política de seguridad que contemple este apartado y asegurarse de que es conocida en nuestra organización puede ser útil para cumplir con esta práctica.
- Descargar archivos adjuntos o acceder a enlaces enviados por mensaje únicamente cuando podamos garantizar la legitimidad del remitente.
- Revisar que nuestro teclado no tenga conectado ningún elemento sospechoso. Puesto que este tipo de *keyloggers* podrían encontrarse dentro del dispositivo, conviene utilizar aquellos que hemos adquirido directamente de un proveedor.
- Actualizar nuestro equipo y mantener activadas medidas de protección como el antivirus o el cortafuego.
- Además, como medida preventiva ante una infección de un *keylogger* o cualquier otra amenaza, es importante utilizar contraseñas robustas y distintas para cada servicio y tener activada la autenticación de doble factor. De este modo, limitaremos las posibilidades de que un ciberdelincuente pueda acceder a nuestras diferentes cuentas.

- De nuevo, este tipo de ataques nos sirve para recordar la importancia de mantenernos alerta ante los riesgos cibernéticos. Conviene tener presente que la primera barrera de defensa es el propio usuario, motivo por el que una notable parte de las amenazas están basadas en la ingeniería social. Es por ello que la formación y concienciación en ciberseguridad de los miembros de nuestra organización, tanto en el ámbito profesional como en el personal, son las mejores herramientas para proteger nuestros sistemas.

AUTOR:

INCIBE (INSTITUTO NACIONAL DE CIBERSEGURIDAD)

ENLACE:

https://www.incibe.es/protege-tu-empresa/blog/cuidado-keylogger-podria-estar-registrando-tus-contrasenas