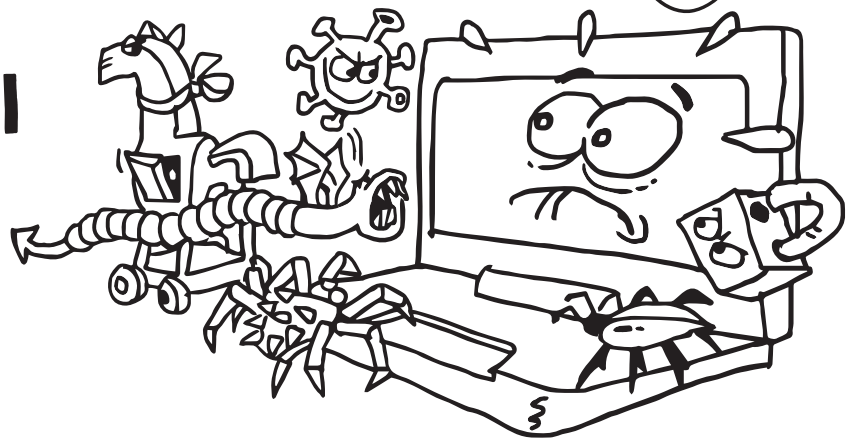
Milpa Digital

Cuidado con el malware y el phishing



No importa lo que estemos haciendo en la red, ya sea hablar con nuestros seres queridos, ver una película, elaborar un programa de radio, o documentar violaciones de los derechos humanos, nuestra seguridad y la de la gente que nos rodea depende en gran medida de la “salud” de los dispositivos con los que trabajamos.

Hay dos reglas fundamentales para evitar ataques de malware y phishing: tener cuidado con el origen del software que instalamos en nuestros dispositivos, y desconfiar siempre que alguien nos pida entrar en una página o abrir un archivo adjunto.

Qué es el software malicioso o malware

En general, llamamos **malware a cualquier programa que realiza acciones maliciosas en el dispositivo** en el que se ejecuta. Por ejemplo: tener acceso a contraseñas u otro tipo de información personal como fotos que tengamos guardadas, usar la capacidad de cómputo de nuestra computadora para generar criptomonedas o para lanzar ataques a páginas web, etc. Puede que tengamos malware si hemos instalado programas de fuentes no confiables, o si hemos hecho clic en un enlace o descargado un archivo sospechoso.

Un ejemplo famoso de malware es el **ransomware**, que cifra sin nuestro permiso los archivos en nuestro dispositivo, y luego las personas que lo ejecutaron nos exigen un pago para recuperarlos. Podemos protegernos frente a este ataque si tenemos una estrategia de **copias de respaldo** de nuestros archivos.

Malware generalizado y malware dirigido

Los ejemplos que hemos comentado antes son **malware generalizado**, que busca **infectar a la mayoría de dispositivos** que tengan alguna vulnerabilidad.

El **malware dirigido**, por el contrario, se usa para **infectar a una persona en particular**.

Dependiendo del adversario (una expareja violenta, un jefe en el trabajo, un delincuente o un servicio militar o de inteligencia), para lanzar un ataque dirigido, el malware específico es comprado en el mal llamado “mercado negro” o desarrollado por empresas cibermercenarias como NSO Gruop para infectarnos.

Es más difícil defenderse contra este malware dirigido, debido a su sutileza y la persistencia del posible adversario, pero casi siempre usará una vulnerabilidad en los programas o sistema operativo que usemos: por esto, **mantener nuestro sistema siempre al día con las últimas actualizaciones** puede ayudarnos a tener mayor protección.

Suscríbete a ResistenciaDigital en Telegram @CanalResistenciaDigital

Qué es el phishing (y cómo evitarlo).

El phishing es una técnica que consiste en engañar a la persona usuaria para robarle información confidencial, o para infectarle con alguna de las variedades de malware que mencionamos antes.

El phishing suele ser la estrategia de engaño para que la persona usuaria sea la vía de infección hacia su propio dispositivo. Puede ser también generalizado (pidiendo que cambies tu contraseña de correo, y redirigiéndote a una página falsa), o dirigido específicamente al dispositivo que estamos usando o al círculo de afinidad con un mensaje más personalizado.

Es mejor **evitar abrir archivos de fuentes desconocidas** (o incluso una fuente conocida puede enviarnos un mensaje si ha sido infectada). Si es muy importante, mejor preguntar por otro medio diferente (como una llamada de teléfono), o abrirlos en un entorno seguro (usando **Tails***, por ejemplo).

***Tails** es un **sistema operativo** que arranca desde un USB y que no deja rastros en nuestra computadora después de usarlo.

Para profundizar más, recomendamos esta ficha de la caja de herramientas de seguridad disponible en Español:

https://securityinabox.org/es/guide/malware/

¡No olvides que puedes imprimir tu propia MilpaDigital y compartirla!

CódigoSur EDICIONES