TIC INFORMA:
TE CONTAMOS 7 MANERAS EN LAS QUE TUS DISPOSITIVOS SE PUEDEN INFECTAR CON MALWARE

Sabemos que el malware constituye una de las amenazas más comunes que enfrentamos diariamente, como usuarios de internet. Por ello, desde el Departamento de Tecnologías de la Información y Telecomunicaciones (TIC) informamos a la Comunidad Minsal no sólo sobre los tipos de malware que existen: también queremos que conozcas cómo es que estos programas maliciosos son capaces de infectar tus dispositivos.

1 Phishing y correos de spam

Pese a que usualmente el principal objetivo de los correos de phishing es obtener información sensible de los usuarios, los correos de phishing también pueden incluir archivos o enlaces que pueden llevar al compromiso de tu dispositivo con malware. Te recomendamos siempre leer tus correos con detenimiento y probablemente caigas en la cuenta de que estás lidiando con alguna estafa. Las señales suelen ser errores de ortografía, que todo deba hacerse rápido, la solicitud de información personal o correos enviados desde un dominio sospechoso.

2 Sitios web fraudulentos

Para engañar a las víctimas llevándolas a descargar aplicaciones maliciosas, los cibercriminales buscan copiar los sitios web de marcas famosas u organizaciones conocidas. Los estafadores crean sitios fraudulentos disfrazándose del sitio oficial con un dominio similar, pero agregando una letra o símbolo que lo hace distinto. Los sitios web estarán ligados a un malware y tratarán de hacer que la víctima haga clic en estos enlaces que descargarán algún código malicioso en sus dispositivos.

3 Memorias USB

Los conocidos como "pendrive" son una forma popular de almacenar y transferir archivos; sin embargo, conllevan una serie de riesgos. Por ejemplo, a quienes no tienen buenas intenciones les gusta utilizar la estrategia de ingeniería social de memorias USB "perdidas" para que buenos samaritanos conecten alguna de estas memorias USB comprometidas con malware en sus computadoras. Una vez que una unidad afectada está conectada al equipo y es abierta, su dispositivo puede infectarse con un algún tipo de código malicioso, como un keylogger o un ransomware.

4 Torrents e intercambio de archivos P2P

Durante años las redes P2P y los torrents se ha ganado la reputación de ser herramientas para la descarga ilegal de software, juegos y archivos multimedia, también han sido utilizadas por desarrolladores como una forma simple de distribuir programas de código abierto o para músicos que buscan compartir sus canciones. Sin embargo, también son utilizados muchas veces por criminales que inyectan códigos maliciosos en esos archivos compartidos.

5 Software comprometido

Esta vulnerabilidad no es tan común, aunque tampoco es algo raro que criminales comprometan software legítimo en lo que se conoce comúnmente como ataques de cadena de distribución. Un ejemplo de esto fue el caso del software CCleaner. En estos ataques, los cibercriminales inyectan el malware directamente en la aplicación, que luego utilizan para propagar el malware cuando los usuarios desprevenidos la descargan.

6 Adware

Algunos sitios web están llenos de anuncios que aparecen cada vez que haces clic en cualquier sección de la página web o incluso pueden aparecer inmediatamente cada vez que accedes a ciertos sitios web. Si bien el objetivo de estos anuncios es, en general, generar ingresos para estos sitios, a veces contienen varios tipos de malware y, al hacer clic en estos anuncios o adware, puedes descargarlos involuntariamente en su dispositivo. Algunos anuncios incluso usan como táctica generar temor al indicar al usuario que su dispositivo ha sido comprometido y que solo la solución de seguridad que ofrece el anuncio puede limpiar su equipo.

7 Aplicaciones falsas

El último ítem de esta lista tiene que ver con falsas aplicaciones móviles. Estas aplicaciones suelen hacerse pasar por verdaderas y tratan de engañar a los usuarios para que las descarguen en sus dispositivos y de esa forma comprometerlos. Pueden disfrazarse de cualquier cosa, haciéndose pasar por herramientas para el seguimiento del estado físico, aplicaciones de criptomonedas o incluso por apps de rastreo de contactos de COVID-19. Sin embargo, la realidad indica que, en lugar de recibir los servicios prometidos, los dispositivos se infectarán con varios tipos de malware, como ransomware, spyware o keyloggers.

Como pueden ver, la lista de estrategias utilizadas por cibercriminales para apuntar a usuarios desprevenidos es larga y puede ser aún más extensa, ya que los cibercriminales siguen desarrollando nuevas tácticas maliciosas. Comprendiendo mejor estas amenazas, puedes estar más tranquilo, asegurándote de que hay formas de mantener tus datos seguros y dispositivos protegidos.

Bienvenidas las consultas al correo **seguridadtic@minsal.cl**

"Ciberconsejos para evitar Malware": te invitamos a revisar la nota anterior que preparamos por este tema. Clic aquí.