Hola mis estimados lectores, hoy nos adentramos en el apasionante mundo de la [ciberseguridad] para hablarles acerca de un programa maligno en específico que se encarga de registrar, en secreto, lo que hace un usuario para que los cibercriminales puedan hacer uso de esta información, similar a lo que hiciera un espía en el mundo real. En la era digital, nuestra vida privada y profesional se encuentran en constante interacción con la tecnología. **Sin embargo, esta integración trae consigo una nueva amenaza invisible y omnipresente: los *spyware*.**

Esta amenaza no consiste en **ataques directos de los conocidos virus o piratas informáticos, sino en infiltraciones indirectas en forma de programas de vigilancia instalados subrepticiamente en nuestros dispositivos.** Estas aplicaciones de vigilancia se denominan programas espías y sirven para registrar y transmitir a terceros los usos y comportamientos informáticos de un usuario. En algunas ocasiones, estos han sido utilizados con frecuencia por los profesionales del marketing para recopilar datos de sus clientes con fines de segmentación y selección, o simplemente para dirigir publicidad selectiva a las computadoras de los usuarios. De esta forma pudiéramos decir que suelen utilizarse legalmente, ya que su instalación podría autorizarse como parte del acuerdo de licencia "*clickwrap*, aceptación

en línea" que los usuarios aceptan al descargar programas gratuitos de utilidades y de intercambio de archivos de Internet. De esta forma se instalarían como parte de aplicaciones informáticas legítimas proporcionadas por empresas a sus clientes, para ofrecer funciones de actualización y comunicación a los usuarios de las aplicaciones.

Sin embargo, parece que la posibilidad de vigilar a distancia y comunicarse con los dispositivos es una oportunidad lo suficientemente atractiva como para atraer la atención de terceros con intenciones no legales. De ahí que estos programas maliciosos, diseñados para infiltrarse en nuestros dispositivos sin consentimiento, son capaces de monitorear nuestras acciones, recopilar datos personales y de esta forma comprometer nuestra seguridad digital. Esta información puede incluir detalles personales, hábitos de navegación, credenciales de acceso y datos financieros. Es válido aclarar que los spyware pueden llegar a través de descargas engañosas, adjuntos de correo electrónico o incluso a través de anuncios en línea.

El impacto de estos en la privacidad y seguridad es profundo. **Al obtener acceso a información confidencial, los ciberdelincuentes pueden realizar fraudes, ejecutar ataques de suplantación de identidad y espionaje corporativo.** Lo que sí está claro que las personas malintencionadas empleen estos programas espías por muchas razones, y es probable que lo continúen haciendo con más frecuencia en el futuro. Algunos hackers pueden emplear troyanos como medio para crear una red de computadoras comprometidas que utilizarán para un ataque de denegación de servicio distribuido. Otros pueden usar los mismos medios para crear una red que envíe correos electrónicos no deseados en el futuro. También pueden desarrollar un software de registro de pulsaciones de teclas para capturar información personal, como contraseñas y tarjetas de crédito. Los propios hackers pueden vender o intercambiar la información obtenida con otros para que puedan cometer actos similares.

Por otra parte, el uso indebido de spyware por parte de las organizaciones y corporaciones para vigilancia y control de usuarios plantea serias preocupaciones éticas y legales. A continuación, algunos de los más destacados:

- **Invasión de la privacidad:** Al recopilar información personal sin el conocimiento ni el consentimiento del usuario. Esto viola la privacidad y puede afectar la confianza en la tecnología.
- **Conflictos legales y penales:** Puede dar lugar a demandas legales y sanciones penales. Las leyes varían según el país, pero en muchos lugares, el uso no autorizado de spyware es ilegal.
- **Daño a la reputación:** Si se descubre que alguien ha instalado spyware en un dispositivo, su reputación puede verse gravemente

afectada. Esto es especialmente cierto en entornos empresariales o relaciones personales.
- **Riesgo de robo de datos:** Por el hecho de que puede robar datos sensibles como contraseñas, información financiera o datos médicos. Esto puede llevar al robo de identidad o a la exposición de información confidencial.
- **Uso no autorizado:** Instalar estos programas en dispositivos ajenos sin permiso es ilegal. Puede utilizarse para espiar a cónyuges, empleados o cualquier persona sin su conocimiento.
- **Impacto en la seguridad informática:** En cierto sentido puede debilitar, la seguridad de un sistema, permitiendo que otros atacantes accedan a la información o realicen actividades maliciosas.

Algunos ejemplos notorios de spyware que han causado impacto en la ciberseguridad son:

- **Havex o Dragonfly:** Dirigido contra sistemas de control industrial, representó una amenaza significativa para las infraestructuras críticas, de las cuales hablaremos la próxima semana.
- **FinFisher o FinSpy:** Utilizado principalmente por corporaciones para la vigilancia, se infiltró en sistemas de 32 países.
- **DarkHotel:** Este spyware apuntaba a personas de alto perfil en hoteles de lujo a través de las redes Wi-Fi.
- **Regin:** Un malware sofisticado que infectó computadoras, principalmente en Rusia y Arabia Saudíta.
- **Pegasus:** Conocido por infectar teléfonos inteligentes, se utilizó contra periodistas, activistas y otras personas de alto perfil.

Detectar spyware en un dispositivo puede ser complicado, pero hay señales que pueden indicar una posible infección. Aquí tienes algunas pistas a tener en cuenta:

1. **Anuncios emergentes y redirecciones:** Si aparecen anuncios emergentes constantemente o te redirigen a sitios web desconocidos, podrías estar infectado.
2. **Aplicaciones desconocidas:** Si aparecen aplicaciones no reconocidas en tu dispositivo, verifica su origen. Algunas aplicaciones pueden ser spyware disfrazado.
3. **Rendimiento lento:** Si tu dispositivo se vuelve más lento de lo habitual, podría ser un indicio de spyware. Los programas malignos en general consumen recursos y afectan el rendimiento general de los sistemas oeprativos.
4. **Cambios en la configuración:** Si ves ajustes o configuraciones que no recuerdas haber cambiado, presta atención. El spyware

puede modificar la configuración sin tu conocimiento.

5. **Datos móviles o uso de datos inusual:** Si notas un aumento repentino en el uso de datos móviles o datos en tu dispositivo, podría ser una señal de actividad de spyware.
6. **Mensajes extraños o llamadas:** Si recibes mensajes extraños o llamadas de números desconocidos, podrían estar relacionados con spyware.
7. **Batería agotada rápidamente:** Si la batería se descarga más rápido de lo normal, podría deberse a aplicaciones maliciosas en segundo plano.
8. **Verificación regular:** Realiza análisis de seguridad con un buen antivirus y verifica regularmente la salud de tu dispositivo.
9. **Calentamiento excesivo:** Si tu dispositivo se calienta más de lo normal sin una razón aparente, podría ser un signo de actividad maliciosa.
10. **Comportamiento extraño:** Si experimentas bloqueos, reinicios inesperados o comportamientos extraños, investiga más a fondo.

Recuerda que estas señales no son definitivas, pero si observas varias de ellas, es importante investigar y tomar medidas para proteger tu dispositivo. Protegerse siempre requiere una combinación de prácticas de seguridad informática y conciencia digital. Mantener el software actualizado, utilizar programas antivirus y evitar acceder a enlaces sospechosos son pasos esenciales, hemos debatido mucho al respecto y no debe verse como un simple lema, hay que aplicarlo en la realidad. Además, es crucial estar informado sobre las últimas amenazas y comprender cómo operan los spyware para poder identificar y neutralizarlos eficazmente.

Los spyware sin dudas representan una amenaza significativa en nuestro mundo interconectado. Es responsabilidad de cada individuo tomar medidas proactivas para proteger su información personal y contribuir a un entorno digital más seguro. A medida que la tecnología avanza, también debe hacerlo nuestra diligencia en la protección contra estos invasores invisibles. Recuerda siempre que los programas malignos siempre están al acecho. Por hoy nos despedimos hasta la próxima semana, donde comentaremos acerca de la seguridad en infraestructuras críticas.

Cubadebate.