# INDUSTRIA SPYWARE

## ESPIONAJE INDUSTRIAL

Luisa Murillo Montoro, Felipe Ribeiro,
Marina Arjona Morales
02/11/2023

# Índice

# 1. INTRODUCCIÓN

La presencia y el impacto del spyware en el entorno digital actual generan una variedad de desafíos en el ámbito de la ciberseguridad. Desde su definición y evolución histórica hasta la diversidad de tipos de spyware y sus métodos de distribución, esta amenaza ha adquirido un papel crítico en la protección de la integridad de la información y las operaciones tanto de empresas como de individuos.

Este conjunto de temas profundiza en la naturaleza del spyware, su evolución a lo largo del tiempo, los distintos tipos existentes y las estrategias de propagación. Además, se examinan los indicadores de infección y se comprenden las graves consecuencias que derivan de los ataques de spyware, lo que resalta la importancia de la detección temprana. Asimismo, se exploran las medidas preventivas que incluyen tecnologías de seguridad, educación de usuarios y prácticas de ciberseguridad como elementos cruciales en la defensa contra el spyware.

Este conjunto de temas también abarca las técnicas para eliminar el spyware de dispositivos y las herramientas disponibles para llevar a cabo esta tarea con eficacia. Por último, se examinan las tendencias emergentes, los desafíos continuos y las nuevas amenazas que surgen en un entorno digital en constante evolución.

En su conjunto, estos temas ofrecen una comprensión integral de un desafío en constante evolución en el ámbito de la ciberseguridad, proporcionando las bases para enfrentar y protegerse eficazmente contra el spyware.

# 2. DEFINICIÓN DE SPYWARE

El spyware es un tipo de software malicioso que se instala en un dispositivo, ya sea un ordenador, navegador web o aplicación móvil, sin el consentimiento informado del usuario. Su función principal es recopilar información personal confidencial y comunicar a un atacante. Esta información puede abarcar desde los hábitos de navegación y compras en línea hasta la captura de pulsaciones

de teclado, datos de tarjetas de crédito, contraseñas y credenciales de inicio de sesión.

La forma en que el spyware se introduce en un dispositivo puede variar. A menudo, se adjunta a otros programas que el usuario descarga e instala de forma deliberada, a veces de manera discreta. Otras veces, el software deseado incluye información en el acuerdo de licencia que describe el spyware sin utilizar ese término, obligando al usuario a aceptar su instalación para acceder al programa deseado. Además, el spyware puede ingresar al dispositivo a través de medios utilizados por otros tipos de malware, como visitar sitios web vulnerables o abrir archivos adjuntos maliciosos en correos electrónicos.

Este tipo de software tiene la capacidad de recopilar información personal, como contraseñas, números de tarjetas de crédito, historiales de navegación, correos electrónicos y otros datos sensibles. Registra y rastrea la actividad en línea del usuario, incluyendo los sitios web visitados, las búsquedas en Internet y los clics en anuncios. Luego, envía los datos recopilados a servidores o entidades externas, que pueden utilizarlos con diversos fines, como publicidad dirigida o incluso actividades fraudulentas. El término "spyware" se deriva de la combinación de "spy" (espía) y "software" (programa informático), ya que su función es espiar y recopilar datos de forma encubierta.

## 2.1 Spyware y el espionaje industrial

El spyware y el espionaje industrial son dos conceptos diferentes, pero están relacionados con la recopilación de información, especialmente en el ámbito de la tecnología y los negocios. Tanto el spyware como el espionaje industrial involucran la recopilación de información, pero difieren en varios aspectos, incluyendo sus objetivos, métodos y actores involucrados.

Tanto el spyware como el espionaje industrial tienen como objetivo principal recopilar información. En ambos casos, se busca obtener datos confidenciales o estratégicos, como secretos comerciales, datos financieros, información personal o información sobre las operaciones de una entidad. En ambas prácticas, la recopilación de información se realiza sin el conocimiento ni el consentimiento de la víctima. Tanto las víctimas del spyware como las de

espionaje industrial pueden no ser conscientes de que su información está siendo recopilada.

Los principales aspectos que diferencian estos conceptos son los objetivos, métodos, alcance y legalidad. El spyware se enfoca en recopilar información personal o confidencial de individuos, como datos de navegación, contraseñas o información financiera, con el propósito de robar datos o cometer actividades ilegales, como el robo de identidad. Tiene un alcance más limitado y suele afectar a dispositivos individuales. Por otro lado, el espionaje industrial se dirige a empresas o entidades, buscando obtener información confidencial o estratégica, como secretos comerciales, planes de productos, estrategias de marketing o datos financieros. El alcance del espionaje industrial es más amplio y puede impactar a toda una organización.

El spyware suele ser perpetrado por ciberdelincuentes, como hackers, que buscan obtener ganancias financieras o cometer delitos cibernéticos. En contraste, el espionaje industrial puede ser llevado a cabo por competidores, gobiernos u otras organizaciones interesadas en obtener información estratégica o comercial, y sus objetivos pueden ser tanto legales como ilegales. El espionaje industrial, involucra una variedad de métodos, que pueden incluir vigilancia física, robo de documentos, ciberespionaje, ingeniería social o la colocación de dispositivos de escucha en las instalaciones de una empresa. Los métodos utilizados en el espionaje industrial son más diversos y se adaptan a las circunstancias específicas.

Por otro lado, el spyware implica la instalación de software malicioso en dispositivos sin el conocimiento del usuario, que luego registra sus actividades y envía los datos a un servidor controlado por el atacante. En algunos casos, ciertas formas de recopilación de información pueden ser legales, como la investigación de mercado ética. Sin embargo, cuando cruza la línea de la legalidad, el espionaje industrial puede tener graves consecuencias legales y financieras. Las diferencias en legalidad a menudo dependen de las leyes específicas de cada jurisdicción y del contexto en el que se llevan a cabo estas actividades.

El espionaje industrial se lleva a cabo a través de diversas técnicas y métodos, cada uno diseñado para obtener información confidencial o estratégica de una

empresa o entidad. La intrusión informática es una forma de espionaje, en la que los atacantes buscan obtener acceso no autorizado a los sistemas informáticos de una empresa. Esto puede lograrse mediante la introducción de software malicioso, como virus, troyanos o ransomware, en la red de la empresa. Una vez dentro, los atacantes pueden robar información, modificar datos o desactivar sistemas.

El robo de la propiedad intelectual se centra en la adquisición de información confidencial y valiosa de la empresa, como patentes, secretos comerciales, fórmulas, planos de productos o estrategias de marketing. Los atacantes pueden obtener estos datos a través de la infiltración informática, la interceptación de comunicaciones o el robo de documentos físicos. El espionaje industrial mediante engaños implica el uso de tácticas de ingeniería social para obtener información confidencial. Esto puede incluir el phishing, donde los atacantes envían correos electrónicos falsos que parecen legítimos para engañar a los empleados y hacer que revelen información confidencial, como contraseñas o datos de acceso.

Por último, el espionaje físico es un método en el que los atacantes ecopilan información confidencial a través de medios físicos. Esto puede incluir la colocación de dispositivos de escucha en las instalaciones de la empresa, el seguimiento y vigilancia de empleados, el robo de documentos o incluso la búsqueda de basura en busca de información descartada.

La protección contra el espionaje industrial constituye un elemento esencial para las empresas que desean mantener su información confidencial resguardada y su competitividad en el mercado. Para lograr esta protección integral, es necesario implementar una serie de medidas estratégicas. La implementación de una sólida infraestructura de seguridad informática es fundamental. Esto incluye la utilización de firewalls, software de detección de intrusiones, cifrado de datos y sistemas de gestión de acceso. Además, mantener los sistemas actualizados y parcheados es esencial para evitar posibles vulnerabilidades.

La formación y concienciación de los empleados son aspectos clave para identificar y prevenir el espionaje industrial. Los empleados deben estar al tanto

de las tácticas de ingeniería social, el phishing y otros métodos de ataque comunes. Esto les permitirá proteger su propia información y alertar sobre actividades sospechosas. El establecimiento de políticas y procedimientos de seguridad sólidos es esencial para proteger la información confidencial. Esto incluye la gestión de contraseñas, el acceso a áreas sensibles y la protección de datos. Es fundamental que los empleados comprendan y cumplan con estas políticas.

La implementación de sistemas de monitoreo y detección es vital para identificar actividades sospechosas en la red y en las instalaciones físicas de la empresa. La detección temprana es esencial para tomar medidas ante posibles amenazas antes de que causen daño. La limitación y el control del acceso a las instalaciones físicas de la empresa se logran a través de sistemas de control de acceso, cámaras de seguridad y seguimiento de visitantes. Además, la protección de documentos físicos importantes en cajas fuertes o salas seguras es fundamental.

La extensión de las políticas de seguridad a los proveedores y contratistas que trabajan con la empresa es clave. Es necesario asegurarse de que cumplan con los mismos estándares de seguridad que se aplican internamente. La realización de auditorías periódicas de seguridad es esencial para evaluar la efectividad de las medidas de seguridad implementadas y para identificar posibles debilidades o vulnerabilidades.

En ocasiones, la asesoría de expertos en seguridad puede ser beneficiosa para identificar y mitigar posibles riesgos de espionaje industrial. La registración y salvaguarda de la propiedad intelectual de la empresa, como patentes y secretos comerciales, dificultan su robo o uso no autorizado.La elaboración de un plan de respuesta a incidentes que defina cómo actuar en caso de un ataque o una brecha de seguridad es esencial. Esto incluye la notificación a las autoridades y a los afectados, así como la mitigación de daños. La protección contra el espionaje industrial constituye una tarea continua que exige vigilancia constante y adaptación a las amenazas en evolución. Las empresas deben estar preparadas para enfrentar posibles riesgos y actuar proactivamente para minimizar las oportunidades de espionaje industrial.

# 3. HISTORIA Y EVOLUCIÓN

A lo largo de su evolución, el spyware ha experimentado cambios en sus técnicas y objetivos a medida que la tecnología ha avanzado. En sus primeras etapas, el **spyware primitivo** surgió en la década de 1990 hasta principios de los 2000. Solía ser simple y generalmente se instalaba en ordenadores mediante programas de uso gratuito o shareware. Estos programas a menudo incluían componentes de seguimiento que recogían información sobre las actividades del usuario y la enviaban a servidores remotos. Esto se utilizaba para fines de marketing y publicidad y el caso más notable fue el Zango.

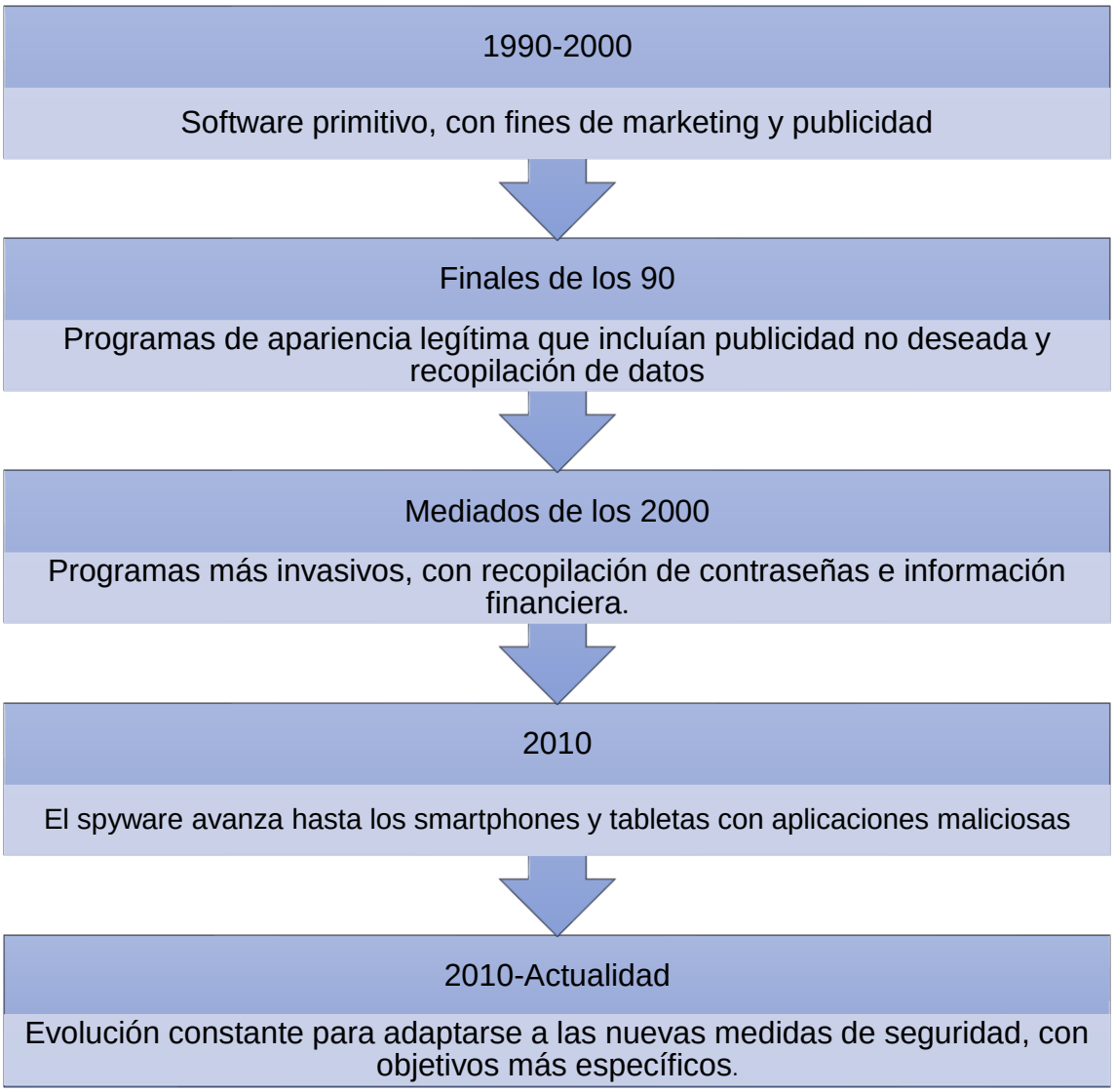
A finales de los 90, se convirtió en un método más común. A menudo, los usuarios instalaban programas aparentemente legítimos que también incluían publicidad no deseada y recopilación de datos. Los desarrolladores ganan dinero a través de anuncios mientras recopilaban información sobre el comportamiento de navegación de los usuarios.

A mediados de los 2000 los programas especializados eran más invasivos ya que registraban cada pulsación de tecla realizada por el usuario. Esto permitía a los atacantes robar contraseñas, información de tarjetas de crédito y otros datos confidenciales. En el 2010, con la popularización de los dispositivos móviles, el spyware se expandió para abordar smartphones y tabletas. Las aplicaciones maliciosas a menudo se disfrazaban como aplicaciones legítimas y se aprovechaban de los permisos de acceso para recopilar datos personales.

Desde el 2010 hasta la actualidad, a medida que las medidas de seguridad mejoraron y las empresas adoptaron técnicas de detección más avanzadas, el spyware también evolucionó. Los objetivos se volvieron más específicos, como gobiernos, empresas, activistas de derechos humanos, periodistas, individuos y dispositivos móviles y objetos conectados a Internet (IoT). Los casos más notables son Pegasus, **WannaCry, NotPetya y Stalkware.**

Se volvió más sigiloso, utilizando técnicas de evasión de detección y explotando vulnerabilidades de día cero. Los ataques de espionaje patrocinados por gobiernos y actores cibernéticos avanzados han desarrollado spyware altamente

sofisticado para llevar a cabo operaciones de ciberespionaje.En la actualidad, algunos tipos de spyware son parte de amenazas persistentes avanzadas (APTs), que son campañas de ciberespionaje de alto nivel que pueden operar durante largos períodos de tiempo. Utilizan técnicas avanzadas para eludir la detección y se alojan en la nube para dificultar su rastreo.




# 4. TIPOS DE SPYWARE

Existen varios tipos de malware que amenazan la seguridad en línea. El **adware,** por ejemplo, se manifiesta mostrando anuncios mientras navegas por internet. Cuando interactúas con estos anuncios, captura tus datos y rastrea tu actividad en la red, a menudo con el propósito de mostrarte publicidad no deseada o redirigirte a páginas fraudulentas en busca de obtener tus datos. Otro tipo de malware es el **keylogger,** que se dedica a registrar todas las pulsaciones de teclado. La información recopilada se almacena en un archivo, a menudo cifrado, lo que significa que cualquier cosa que escribas queda registrada.

Los **infostealers** son otro tipo de amenaza cibernética que recopila información de tu ordenador o dispositivo móvil, incluyendo datos de inicio de sesión, descargas y conversaciones de mensajería. Por otro lado, el Red Shell es un spyware que se instala en tu ordenador a través de descargas de videojuegos en línea, registrando tu actividad en estos juegos. Aunque inicialmente está destinado a mejorar la experiencia de juego, se instala sin previo consentimiento.

Además, **las cookies de seguimiento,** a pesar de ser comunes, también pueden considerarse un tipo de spyware, ya que registran y recopilan información de tu actividad en línea. Por último, los rootkits representan un tipo de spyware que permite a los delincuentes infiltrarse en lo más profundo de tu ordenador, a veces utilizando otros tipos de malware como troyanos. Estos rootkits pueden proporcionar a los atacantes un control significativo sobre tu sistema, lo que los convierte en una amenaza seria para la seguridad.

# 5. DISTRIBUCIÓN Y MÉTODOS DE INFECCIÓN

El spyware se propaga a través de diversos vectores de infección, lo que lo convierte en una amenaza persistente para la seguridad en línea. Uno de los principales métodos de propagación involucra descargas de software no seguras. Los usuarios pueden verse expuestos al spyware cuando descargan programas de fuentes no confiables o de sitios web no oficiales. En ocasiones, esta instalación se realiza de manera discreta, sin que el usuario tenga conocimiento de que está adquiriendo el software malicioso. Es importante tener

precaución al descargar aplicaciones y programas, asegurándose de que provengan de fuentes legítimas y verificadas.

Los correos electrónicos maliciosos también son un vehículo común para la propagación del spyware. Los correos de spam pueden contener adjuntos o enlaces maliciosos que, cuando se abren o hacen clic en ellos, instalan el spyware en el sistema del usuario. Estos correos a menudo intentan engañar al destinatario, haciéndo creer que se trata de mensajes legítimos o atractivos, lo que puede llevar a una instalación no deseada de malware.

Además, el uso de técnicas de ingeniería social es frecuente en la propagación del spyware. Los atacantes emplean tácticas engañosas para persuadir a las personas a descargar o ejecutar archivos maliciosos. Esto puede incluir suplantación de identidad en correos electrónicos, donde el remitente parece ser una entidad confiable o una persona conocida, o el uso de mensajes que parecen legítimos pero contienen enlaces o archivos maliciosos. La ingeniería social es una estrategia efectiva para engañar a las víctimas y lograr que instalen inadvertidamente el spyware. Por lo tanto, es fundamental que los usuarios sean cautelosos y estén al tanto de las posibles amenazas al interactuar en línea y al descargar software o abrir correos electrónicos sospechosos.

# 6. INDICADORES DE INFECCIÓN

Detectar una infección por spyware puede ser complicado, ya que a menudo opera en segundo plano de manera discreta. Sin embargo, hay indicadores que sugieren una posible infección por spyware: La detección de la presencia de spyware es esencial para garantizar la seguridad de los dispositivos y la privacidad en línea. Los indicadores de infección pueden variar, pero existen algunos síntomas y señales de advertencia clave a los que los usuarios deben prestar atención.

Uno de los indicadores más comunes es un rendimiento lento de la computadora o el dispositivo. Cuando el spyware se infiltra en un sistema, puede consumir

recursos y ralentizar significativamente el rendimiento. Las aplicaciones pueden tardar más en abrirse o responder, y la navegación en línea puede volverse frustrantemente lenta. Esta desaceleración no es necesariamente causada por el spyware por sí solo, pero puede ser un efecto secundario de su actividad continua de recopilación y transmisión de datos.

Otro indicio de infección por spyware son los cambios en la configuración del navegador. Los atacantes a menudo modifican la página de inicio, el motor de búsqueda predeterminado o agregan barras de herramientas no deseadas. Estos cambios pueden ser desconcertantes y pueden dificultar la navegación por la web de manera eficiente. Es importante prestar atención a cualquier ajuste inesperado en el navegador.

La presencia de anuncios emergentes intrusivos es un signo adicional a considerar. Los anuncios pueden aparecer de manera inoportuna y persistente, incluso cuando no se está navegando por la web. Estos anuncios a menudo están relacionados con las actividades de navegación del usuario y pueden ser indicativos de la recopilación de datos por parte del spyware.

Además de los síntomas relacionados con el dispositivo, la actividad inusual en las cuentas en línea del usuario puede ser una señal de advertencia. Esto puede incluir correos electrónicos enviados desde la cuenta sin consentimiento, publicaciones sospechosas en redes sociales o incluso intentos de acceso no autorizados a cuentas en línea. Cualquier actividad no reconocida o cambios en la seguridad de las cuentas deben ser investigados y tratados con seriedad.

# 7. CONSECUENCIAS DEL ATAQUE

Las consecuencias y los riesgos generados por un ataque spyware variarán en función del tipo de programa instalado y sus objetivos. No obstante, se pueden englobar en 3 bloques generales:

En primer lugar, el robo de información. La infiltración de un programa de spyware representa una amenaza a la privacidad y seguridad de los individuos y organizaciones. El robo de información a través de estos programas plantea graves preocupaciones, ya que las víctimas experimentan una pérdida de

privacidad y riesgos financieros debido al robo de datos de carácter personal y similares. Estos actos pueden derivar en un uso fraudulento de los datos recopilados, además de derivar en un daño significativo a la reputación y pérdidas económicas considerables.

En segundo lugar, la manipulación de resultados en motores de búsqueda a través de programas de spyware socava la fiabilidad de la información en línea. Esta consecuencia no sólo modifica los resultados de la búsqueda, sino que también puede propagar información no certera y desinformación, lo que puede influir en la percepción pública y llevar a decisiones erróneas basadas en datos incorrectos.

Esto presenta un desafío y expone la necesidad de una respuesta efectiva para proteger la integridad de la información en línea.

Por último, se encuentra el daño a los equipos. Estos programas acaban afectando negativamente al rendimiento de los dispositivos al consumir recursos del sistema, lo que puede ralentizar el funcionamiento de los ordenadores y dispositivos. Además, cabe destacar que en numerosas ocasiones el programa de spyware actúa como antecedente para, posteriormente, poder introducir en el sistema el malware adicional, lo que aumenta el riesgo de consecuencias más graves.

En el contexto del espionaje industrial, el daño a los equipos toma especial relevancia, ya que puede tener repercusiones económicas significativas. Con el daño a sus equipos, las empresas pueden sufrir la pérdida de información confidencial y estratégica, lo que afecta a su posición en el mercado. Además, puede dar lugar a una filtración de datos que afecten a la propiedad intelectual de terceros y generar pérdidas económicas significativas.

Por último, cabe destacar que mitigar los efectos de un ataque spyware en el ámbito empresarial supone un coste elevado en términos de tiempo y recursos financieros, además de conllevar daños en la reputación de la empresa.

# 8. PREVENCIÓN ANTE ATAQUES

La prevención y protección de los dispositivos son elementos clave en la defensa contra el espionaje industrial y las amenazas cibernéticas en general. Con la adopción de un enfoque integral que incluya tecnología de la seguridad, educación en los usuarios sobre esta problemática y prácticas sólidas y efectivas de ciberseguridad, se puede prevenir y proteger la información y la integridad de los sistemas.

## 8.1 Tecnologías de la seguridad

En la tarea de prevenir los ataques e infecciones por spyware, la seguridad a través de la tecnología se convierte en un aspecto esencial. El uso de programas de seguridad fiables como antivirus o antimalware con capacidad de detección y eliminación es un primer paso fundamental. Debido a que las amenazas evolucionan de manera constante, es relevante mantener este programa actualizado, para que se pueda adaptar a las nuevas amenazas.

Además, la previa instalación de programas o software denominados “corta fuegos” tanto en la red como en los dispositivos ayudarán a filtrar el tráfico no autorizado, creando una barra protectora para salvaguardar los sistemas y datos.

## 8.2 Educación a los usuarios

La educación y concienciación en los usuarios acerca de este fenómeno es un componente esencial para prevenir infecciones en los dispositivos. Este aspecto toma especial relevancia en el ámbito empresarial debido al auge del espionaje industrial por la competitividad de empresas en los mercados, ya muchos ataques se dirigen de manera directa a los empleados y sus dispositivos, como forma de acceder a la información empresarial.

Esto implica formar a los usuarios para que reconozcan ciertas señales de advertencia, como no abrir archivos adjuntos de dudosa procedencia o abrir enlaces que parezcan sospechosos. Sensibilizar a los usuarios sobre los riesgos asociados a estos ataques les permite identificar y prevenir posibles amenazas de ataques spyware.

Además, resulta imprescindible formar a los usuarios a acceder y navegar por Internet de forma segura, así como a comprender la importancia de autentificar los sitios que visitan y los riesgos de facilitar información personal o financiera.

### 8.3 Prácticas de ciberseguridad

En el plano empresarial, resulta imprescindible establecer unas políticas de seguridad cibernéticas comunes, que establezcan directrices claras para los empleados sobre cómo abordar la seguridad y prevención de amenazas spyware. Asimismo, también deberá contener los procedimientos en caso de un incidente de este tipo, ofreciendo así una respuesta rápida y minimizando los daños sufridos.

Por último, el monitoreo constante y permanente de la red en busca de patrones no comunes que puedan indicar una amenaza será esencial para detectar actividades o intrusiones en los sistemas cuanto antes. El monitoreo no sólo ayuda a prevenir, sin también a ofrecer una respuesta rápida si se produce un ataque, reduciendo el tiempo de inactividad en la empresa y por lo tanto el impacto financiero.

## 9. CÓMO ELIMINAR UN PROGRAMA SPYWARE DEL DISPOSITIVO

La presencia de un spyware en un dispositivo puede poner en riesgo la privacidad y seguridad en línea del usuario, por lo que mantener una buena metodología de prevención será relevante. No obstante, también será de suma importancia disponer de los pasos y las herramientas para poder eliminarlo de un dispositivo.

Si se ha identificado la presencia de un programa spyware, el primer paso para eliminarlo de forma manual será desconectar el dispositivo de Internet para evitar que la cantidad de información vulnerada aumente o que el mismo programa descargue otro spyware o malware adicional.

A continuación, se deberá detectar el programa o archivo asociado al spyware, con ayuda de un software antivirus o antimalware que realicen un escaneo del dispositivo y detecten la amenaza. Una vez detectados, se procederá a su eliminación tanto si se trata de un proceso en ejecución como si se trata de un programa o aplicación de apariencia legítima.

Para realizar este paso de forma manual sin la asistencia de un software antivirus, es recomendable arrancar el dispositivo en modo seguro o “safe mode” y se procederá a eliminar de forma permanente en primer lugar los denominados como archivos temporales, eliminándolos de igual forma de la papelera de reciclaje. A continuación, se analizarán los archivos y programas instalados en el dispositivo, detectando en la lista aquellos que no se reconozcan o que sean de dudosa procedencia, y se eliminarán de forma permanente.

Nuevamente mediante herramientas antimalware o antivirus se realizará un nuevo escaneo para asegurar que el dispositivo no contenga aún restos del programa spyware.

Una vez eliminado, se puede restaurar el dispositivo si ha sufrido daños significativos por el ataque, así como reforzar la seguridad mediante programas y antivirus actualizados.

Cabe destacar que estos pasos para eliminar el spyware variarán en función del dispositivo y del sistema operativo que se esté ejecutando, por lo que resulta recomendable revisar si existen algunas especificaciones por sus características.

## 9.1 Herramientas

Entre las herramientas más efectivas para su eliminación se destacan Malvarebytes (herramienta especializada en detectar y eliminar spyware y otros malware), Windows Defender (para usuarios Windows, es una herramienta de seguridad incorporada en el sistema operativo especializada en la eliminación de amenazas) o AdwCleaner (herramienta especializada en la eliminación de adware, usualmente asociado al spyware). Asimismo, se destacan compañías que ofrecen programas de seguridad que incluyen herramientas de eliminación de amenazas, incluido el spyware, como Avast, AVG, Bitdefender o Norton.

# 10. TENDENCIAS, DESAFÍOS Y NUEVAS AMENAZAS EN LA AMENAZA DE SPYWARE

El futuro de la amenaza spyware se presenta como un escenario en constante evolución, caracterizado por tendencias, desafíos y nuevas amenazas emergentes que plantean desafíos significativos para la ciberseguridad y la privacidad de los usuarios.

## 10.1 Nuevas tendencias

En el escenario a futuro de la amenaza del spyware, se observa una tendencia a seguir evolucionando y adaptándose a los nuevos tiempos. Esto, sumado a la dificultad de las autoridades para legislar este ámbito y la dificultad de combatirlos, insta a poner el enfoque en la prevención.

Como ejemplo de esta capacidad de adaptación, se observa una tendencia a una mayor atención como objetivo de ataque a los dispositivos móviles, ya que su ámbito de uso se ha ido expandiendo a lo largo de los años, sustituyendo en gran parte a los ordenadores en algunas funciones que anteriormente eran propias de este último.

Además, se almacena en ellos una gran cantidad de información personal y sensible, superior a la que se almacena en ordenadores, por lo que aumenta su atractivo. Asimismo, con la adopción cada vez mayor del trabajo remoto, los dispositivos móviles ya no sólo almacenan información de carácter privado, sino que, en muchas ocasiones y provocado por la falta de educación sobre ciberseguridad, también almacenan información y credenciales de la organización empresarial a la que el usuario pertenezca.

Al mismo tiempo, con el traslado de atención a los dispositivos móviles y la constante evolución del spyware, los encargados de realizar el ataque continuarán especializándose en las denominadas Técnicas de Ingeniería Social para lograr pasar más desapercibidos a ojos del usuario.

Por otro lado, se observa una tendencia en crecimiento de ataques de spyware basados en Inteligencia Artificial, que conllevan ataques más graves y frecuentes debido a su fácil repetición. Se basan en ataques del denominado como zero click, ya que no requieren de la intervención del usuario.

## 10. 2 Desafíos

Uno de los desafíos que se sigue planteando en el fenómeno del spyware continúa siendo la protección de la privacidad, sobre todo por el difícil equilibrio entre la obtención legítima de datos como las cookies para mejorar la experiencia del usuario y la protección de su intimidad. Este conlleva el siguiente desafío de crear una legislación pertinente que, como se ha nombrado ya en el presente informe, también supone una necesidad. Esta legislación debe tener en cuenta este equilibrio en un cálculo de coste-beneficio, y poder conseguir normativas y leyes sobre privacidad eficaces que contrarresten los programas spyware.

Por otro lado, casos pasados como Pegasus, han puesto de relieve el desafío de las Amenazas Persistentes Avanzadas, que ponen de relieve la necesidad de contar con sistemas de defensa fuerte y eficaces para desarmar estos programas que se caracterizan por, entre otras cosas, dificultar su detección.

Por último, el creciente uso de Inteligencia Artificial también presenta desafíos , ya que puede ser usada para automatizar los programas spyware y que puedan ser difundidos a gran escala, lo que pone de relieve la necesidad de contar con sistemas de detección eficaces.

En conclusión, el futuro del spyware será un escenario en evolución constante y desafíos permanentes que exigirán una adaptación constante de la ciberseguridad para contrarrestarlos.

# 11. CASO EXPLICATIVO

El caso del ataque ransomware a la empresa de externalización de productos y servicios IT Kaseya pone de relieve que la lucha contra estos ataques no se basa sólo en proteger y prevenir dentro de una empresa, sino que se trata de un

fenómeno que se debe acatar de manera global y estructural. El 2 de julio de 2021, la compañía de software especializada en soluciones y productos IT para empresas llamada Kaseya, publicó en su web un aviso en el que aseguraban estar investigando un ataque contra el servicio de la empresa, que únicamente afectaba a una pequeña parte de su cartera de clientes. Así, ofrecieron la solución de cerrar los servidores y notificar el problema a los clientes para que desconectaran los servidores de software asociados a la empresa.

Poco tiempo después, Kaseya informó que desplegado su equipo interno y contratado expertos externos para determinar el origen del problema. En aquel momento, la empresa estimaba que el ataque habría afectado a unos 40 clientes, a pesar de que en aquel momento contaba con una cartera de más de 36.000 clientes a los que externalizaba sus servicios.

Un día después, el 3 de julio, Kaseya finalmente confirmó que había sido víctima de un ciberataque, aunque continuaban insistiendo en que la cantidad de clientes afectados era mínima. Asimismo, informó de que estaba gestionando el desarrollo de una herramienta de detección para estos ataques y que se encontraba en proceso de corregir el código y replicar el vector del ataque.

El ataque se llevó a cabo mediante la explotación de una vulnerabilidad zero-day que se encontraba en reparación. A pesar de que desde la compañía no se confirmó la identidad del atacante, su autoría fue reclamada por REvil quien pidió un rescate a la compañía de 70 millones de dólares en Bitcoin.

Estos hackers, mediante una publicación en su web, afirmaron haber bloqueado más de un millón de sistemas y las redes de al menos mil empresas clientes en todo el mundo, incluido España.

# 12. CONCLUSIONES

El spyware, que afecta a la privacidad y seguridad de los usuarios y empresas, es una amenaza que evoluciona y se adapta a los nuevos tiempos. Su propagación y métodos de infección varían dependiendo de la tipología de spyware y de los objetivos que se quieran conseguir, aunque incluyen las descargas de software no seguras, correos electrónicos maliciosos y técnicas de ingeniería social. Los indicadores de infección pueden incluir un rendimiento

lento de la computadora, cambios en la configuración del navegador, anuncios emergentes intrusivos y actividad inusual en cuentas en línea.

Las consecuencias de un ataque de spyware pueden ser la pérdida de información personal, manipulación de resultados en motores de búsqueda y daño a los equipos. La prevención de ataques de spyware son esencial para combatirlos e implica la utilización de herramientas de seguridad, la educación de los usuarios en esta problemática la implementación de prácticas sólidas de ciberseguridad.

El futuro del spyware presenta desafíos, incluyendo la protección de la privacidad, la legislación pertinente, la amenaza de Amenazas Persistentes Avanzadas (APTs) y el uso de Inteligencia Artificial en ataques de spyware. En resumen, la ciberseguridad continuará siendo una prioridad para proteger la información y la privacidad en línea en un entorno en constante evolución.

## 13. Bibliografía:


- *¿Qué es el spyware? - definición*. (2023, 19 abril). latam.kaspersky.com. https://latam.kaspersky.com/resource-center/threats/spyware
- Malwarebytes. (2020, 27 mayo). *Spyware: Qué es y cómo eliminarlo*. Malwarebytes. https://es.malwarebytes.com/spyware/
- N. (s. f.). ¿De verdad sabes todo lo que hay en tu ordenador? Descubre qué es un spyware y cómo eliminarlo paso a paso. *N26*. https://n26.com/es-es/blog/spyware
- International IT. (2022, 5 julio). Spyware:¿Qué es?¿Qué tipos hay? ¿Cómo protegerse? *International IT*. https://www.internationalit.com/post/spyware-qu%C3%A9-es-qu%C3%A9-tipos-hay-c%C3%B3mo-protegerse?lang=es
- Digital, L. I. (2020, 21 julio). *¿Qué es el spyware? definición, tipos y características*. Locura Informática Digital. https://www.locurainformaticadigital.com/2018/02/12/spyware-que-es-definicion-tipos/

- *¿Qué es el spyware? los 10 ejemplos más terribles (2023)*. (s. f.). SoftwareLab. https://softwarelab.org/es/blog/que-es-el-spyware/
- *Tipos de spyware*. (2023, 19 abril). www.kaspersky.es. https://www.kaspersky.es/resource-center/threats/types-of-spyware
- BBVA ESPAÑA & BBVA. (2022, 22 noviembre). Spyware: qué es, qué tipos hay y cómo se puede eliminar. *BBVA*. https://www.bbva.es/finanzas-vistazo/ciberseguridad/ataques-informaticos/spyware-que-es-que-tipos-hay-y-como-se-puede-eliminar.html
- Ramos, I. L. (2022, 30 septiembre). *Spyware: tipos y cómo protegerte*. LISA News. https://www.lisanews.org/ciberseguridad/spyware-tipos-y-como-protegerte/
- Alonso, N. (2023, 24 enero). *Spyware ¿Qué es y cómo eliminarlo?* Grupo Atico34. https://protecciondatos-lopd.com/empresas/spyware/
- Latto, N., & Belcic, I. (2023, 26 febrero). *Cómo eliminar el spyware de un PC*. Cómo eliminar el spyware de un PC. https://www.avast.com/es-es/c-remove-spyware-pc#topic-3
- *Inteligencia y monitoreo de amenazas cibernéticas*. (2023, 8 marzo). Acronis. https://www.acronis.com/es-es/blog/posts/cyber-threat-intelligence/
- Swissinfo.Ch. (2023, 1 noviembre). Los avances en la IA: posibles escenarios futuros. *SWI swissinfo.ch*. https://www.swissinfo.ch/spa/ia-cumbre_los-avances-en-la-ia--posibles-escenarios-futuros/48943548
- *Detectadas nuevas tácticas en los ataques a equipos industriales*. (2022, 1 febrero). www.kaspersky.es. https://www.kaspersky.es/about/press-releases/2022_detectadas-nuevas-tacticas-en-los-ataques-a-equipos-industriales
- Tablado, F. (2022, 3 octubre). *Espionaje industrial. definición, tipos y penas*. Grupo Atico34. https://protecciondatos-lopd.com/empresas/espionaje-industrial/

- Grustniy, L. (2019, 22 noviembre). Los riesgos del spyware comercial "legal" *Kaspersky Daily*. https://www.kaspersky.es/blog/stalkerware-spouseware/18179/

- García, J. (2021, 06 julio). Kaseya y su espeluznante ataque de ransomware: esto es todo lo que sabemos hasta el momento https://www.xataka.com/seguridad/kaseya-su-espeluznante-ataque-ransomware-esto-todo-que-sabemos-momento
- Sabán, A. (2021, 05 julio). El histórico ciberataque de REvil a Kaseya deja récords: un millón de sistemas afectados y 70 millones de dólares para recuperarlo todo. https://www.genbeta.com/seguridad/historico-ciberataque-revil-a-kaseya-deja-records-millon-sistemas-afectados-70-millones-dolares-para-recuperarlo-todo