Virus, ransomware y malware, diferencias

Cuando se trata de ciberseguridad, algunos términos se utilizan a menudo indistintamente, lo que puede resultar confuso. Los primeros ataques de malware solían denominarse virus. Del mismo modo, los primeros productos de ciberseguridad se presentaban a menudo como soluciones antivirus, reforzando la idea de que los virus son la principal ciberamenaza. Sin embargo, en las últimas décadas, las estrategias utilizadas por los ciberdelincuentes han evolucionado enormemente, dando lugar a nuevos tipos de software malicioso con diferentes métodos de entrega, objetivos y efectos en sus sistemas.

Comprender las diferencias entre virus, malware y ransomware puede ayudarle a identificar el riesgo a tiempo, poner en marcha las medidas de prevención adecuadas para los distintos escenarios y evitar la pérdida de datos.

¿Qué es el malware?

Malware, abreviatura de «software malicioso», es un concepto general que incluye cualquier código malicioso externo que pueda dañar un dispositivo o corromper datos. Cuando se habla de ciberseguridad en general, malware suele ser el término más amplio que puede utilizarse en la mayoría de los contextos. El ransomware y los virus son dos tipos de malware. Otros tipos de malware son:

El spyware permite a los piratas informáticos rastrear la actividad de otro dispositivo. Los programas espía recopilan datos personales, como información sobre tarjetas de crédito, contraseñas, nombres de usuario, etc., para que los piratas informáticos los utilicen posteriormente para entrar en las máquinas.

Los bots son programas maliciosos que conectan las máquinas pirateadas a un servidor central. Esta red de máquinas se conoce como botnet. Las redes de bots pueden pasar desapercibidas aunque incluyan millones de dispositivos. Aprovechando la potencia de una máquina pirateada, los botnets pueden enviar mensajes de phishing y spam, robar información personal y realizar ataques de denegación de servicio (DDoS).

Los rootkits permiten a los piratas informáticos controlar un dispositivo sin que el usuario sea consciente de ello. Una vez instalado, un rootkit puede cambiar la configuración del sistema y descargar otros archivos maliciosos.

Los gusanos son programas que se propagan automáticamente entre ordenadores de la misma red sin necesidad de un archivo host. Los gusanos pueden eliminar o modificar información, robar datos o instalar malware adicional. Hoy en día, los gusanos no son tan populares, pero otros programas maliciosos siguen utilizando el mismo método de ataque.

Los troyanos, a diferencia de los gusanos, necesitan un host para funcionar. Se trata de malware encubierto, ya que generalmente se camuflan como archivos legítimos. Los troyanos se propagan principalmente a través del phishing. Sin embargo, no es la única manera. Los ataques troyanos aparecen a veces integrados en un falso antivirus que aparece en un sitio web que ofrece protección para un dispositivo. Una vez instalados en un ordenador, los troyanos permiten espiar y modificar datos.

El adware es malware en forma de conocidas ventanas emergentes. Suele ir de la mano de juegos gratuitos u otros programas sin licencia. A veces, la única amenaza que plantea es ralentizar su máquina. Sin embargo, en algunos casos, también puede dar lugar a la instalación de spyware.

El malware sin archivos es un código malicioso que entra directamente en la memoria del ordenador y corrompe programas de confianza como PowerShell o los scripts de Windows. A diferencia de otros tipos, el malware sin archivos no suele dejar rastro y, por tanto, es más difícil de detectar por los escáneres.

Sin embargo, los virus y el ransomware son los tipos de malware más extendidos.

¿Qué es un virus?

Un virus es un programa malicioso que se propaga a través de sitios web y archivos infectados. Cuando un dispositivo se expone a un virus, éste se instala y comienza a ejecutarse sin que el usuario lo sepa. Los virus pueden corromper datos, dañar un

dispositivo e interferir en su rendimiento, formateando el disco duro. Algunos virus pueden replicarse y propagarse por una red local. Incluso un simple virus puede ralentizar considerablemente el sistema al utilizar la memoria del ordenador y provocar fallos frecuentes.

¿Cómo se propagan los virus?

Incluso los administradores de sistemas y usuarios más cuidadosos, que toman precauciones contra posibles amenazas de malware, probablemente se hayan visto expuestos a un virus en algún momento. Los virus se propagan de varias formas. Un virus puede introducirse en la red de un entorno a través de actividades cotidianas como:

Intercambio de datos entre dispositivos

Visitar sitios web infectados (un dispositivo puede infectarse incluso sin descargar archivos).

Descarga de archivos torrent u otro software gratuito

Uso de dispositivos de almacenamiento externos (como unidades USB) que estaban previamente conectados a un ordenador infectado.

Abrir archivos adjuntos de correo electrónico infectados

Virus: mitos y realidades

Mito 1: Definitivamente sabrá cuando su ordenador está infectado.

Realidad: El malware suele propagarse sin ser detectado. Por eso no siempre podrá saber si un dispositivo está infectado.

Mito 2: Los sitios web creíbles no contienen virus ni otros programas maliciosos.

Realidad: Los piratas informáticos pueden ejecutar anuncios maliciosos en sitios web fiables. Incluso ver un anuncio sin hacer clic en él puede instalar malware. A veces, incluso los sitios web más conocidos pueden estar infectados con malware.

Mito 3: Los dispositivos de Apple están a salvo de virus.

Realidad: Se trata de un error muy arraigado, ya que cualquier dispositivo puede infectarse, ya ejecute macOS u otro sistema operativo. Los piratas informáticos perfeccionan sus programas para penetrar en cualquier sistema y entorno.

Mito 4: Los correos electrónicos de fuentes creíbles no pueden infectarse. Siempre es seguro abrir archivos adjuntos de correo electrónico de fuentes fiables.

Realidad: El malware suele propagarse sin ser detectado.

Hecho: aunque un correo electrónico proceda de una fuente de confianza (colega, amigo, etc.), no hay garantía de que sea seguro. Algunos virus se cuelan en la lista de contactos e infectan los correos electrónicos. Por tanto, si un archivo adjunto a un correo electrónico parece sospechoso, es mejor evitar abrirlo.

Mito 5: Cuando no hay datos críticos en un ordenador, el software malicioso no es una amenaza.

Realidad: aunque un dispositivo no almacene datos críticos, el malware sigue suponiendo una amenaza para la seguridad. El malware rara vez busca datos. En cambio, accede a una lista de contactos para enviar correos electrónicos basura o utiliza la memoria y la potencia de una máquina y, en consecuencia, de toda la red.

Mito 6: Los cortafuegos ofrecen una protección antivirus completa.

Realidad: Los cortafuegos proporcionan varios tipos de protección, principalmente filtrando el tráfico y restringiendo el acceso no autorizado a los datos. Sin embargo, los programas maliciosos pueden acceder a un dispositivo y propagarse por la red.

¿Qué es un virus ransomware?

En sentido estricto, no existe el término «virus ransomware». A diferencia de los virus, el ransomware no es una infección autorreplicante, pero los delincuentes pueden utilizar virus como parte de ataques de ransomware más complejos. Las funciones del ransomware se basan en el cifrado, una de las tecnologías de seguridad más eficaces creada inicialmente para proteger los ordenadores. El cifrado transforma los datos en un código secreto que sólo puede descifrarse utilizando una clave de descifrado.

Los hackers piden a las víctimas que paguen un rescate, normalmente en Bitcoin, para obtener la clave de descifrado y recuperar el acceso a sus archivos. Sin embargo, no todos los ataques de ransomware persiguen un beneficio económico. En algunos casos, como con los ransomware wipers (por ejemplo, NotPetya), el objetivo del hacker es la interrupción o la eliminación de datos, por lo que los delincuentes pueden generar direcciones falsas de criptocarteras o solicitar a sus víctimas el pago de rescates poco realistas.

En sentido estricto, no existe el término «virus ransomware».

Naturalmente, las empresas temen perder la confianza y sufrir daños en su reputación. Por lo tanto, pagar el rescate parece una solución rápida para resolver la situación. Sin embargo, pagar el rescate nunca garantiza recuperar el acceso a sus sistemas.

En lugar de financiar a los hackers y preguntarse si podrá recuperar el acceso a sus datos, una solución mucho mejor es hacer backup de sus cargas de trabajo. El mejor enfoque para la protección contra el ransomware es tener un plan de backups 3-2-1 que incluya backups inmutables y aislados de la red. Un plan de este tipo significa que deberías tener un mínimo de tres (3) copias de backups, almacenar dos

(2) de ellas en soportes diferentes y mantener una (1) externa. Con este plan de backups, su proceso de recuperación será rápido y sencillo, incluso después de un ataque de ransomware.

¿Cómo se propaga el ransomware?

Algunas de las formas más comunes de propagación del ransomware son:

Los correos electrónicos de suplantación de identidad son correos electrónicos no deseados que incluyen un archivo adjunto o un enlace malicioso. Una vez abierto el archivo adjunto o el enlace, el ransomware se descarga en la máquina. A veces, el remitente del correo electrónico puede ser alguien de tus contactos.

Los enlaces de los mensajes en las redes sociales pueden contener un enlace malicioso que puede activar el ransomware en un dispositivo.

Los **sitios web maliciosos** pueden dar lugar a la instalación de ransomware después de visitarlos.

Esto es habitual en plataformas de streaming de vídeo y otros sitios web de contenido gratuito. **El malware adicional** ataca dispositivos que ya pertenecen a una botnet (un servidor que agrupa ordenadores pirateados). En este caso, el dispositivo se infecta aún más con software malicioso adicional.

Ransomware: mitos y realidades

Mito 1: El ransomware ataca a las empresas y no a los particulares.

Realidad: El ransomware no distingue. Tanto los particulares como las empresas pueden ser destinos de ataques de ransomware.

Mito 2: Siempre se recuperan los datos después de pagar el rescate.

Realidad: En la mayoría de los casos, quienes pagan el rescate no recuperan el acceso a sus datos. Pagar el rescate parece una solución fácil y rápida para hacer desaparecer el problema. Sin embargo, pagar el rescate supone financiar la ciberdelincuencia e incentivar a los hackers a realizar más ataques sin tener garantías de obtener las claves de descifrado.

Mito 3: El ransomware no puede cifrar los backups.

Realidad: Aunque los backups periódicos son la mejor forma de proteger los datos, existe el riesgo de que estos backups incluyan cargas de trabajo infectadas o sean corrompidos por terceros. Para mitigar estos riesgos, es esencial ejecutar análisis periódicos de malware,

seguir la **regla 3-2-1 para hacer backups** y aplicar medidas de seguridad como el cifrado, la inmutabilidad y el control de accesos basado en roles a los datos de las copias de seguridad.

Ransomware frente a malware frente a virus

Gol del atacante	El malware está diseñado para causar un amplio intervalo de daños en un ordenador, dependiendo del tipo de malware.	El ransomware está diseñado para bloquear el acceso a los datos hasta que el usuario pague un rescate.	Un virus está diseñado como un código malicioso adjunto a un archivo independiente. Un virus puede formatear un disco duro, o puede ser inofensivo.
Impacto en el sistema	El malware puede controlar y robar datos, utilizar los recursos de un ordenador, destruir el sistema, etc.	El ransomware dañar un dispositivo, bloquea el sistema y cifra todos los datos.	Los virus pueden corromper datos, degradar el rendimiento de un dispositivo, etc.
Variedad	Hay muchos tipos de malware: gusanos, spyware, rootkits, troyanos, ransomware, etc.	Existen tres tipos diferentes: infector de archivos, crypto. locker, doxware y ransomware.	Los virus se presentan en formas más comunes: macrovirus, virus polimórficos, etc.
Método de entrega	Según el tipo, el malware puede propagarse a través del correo electrónico, la instalación de datos, la navegación por Internet, la explotación de vulnerabilidades del sistema, etc. Algunos tipos de malware sólo pueden ser activados por un usuario, mientras que otros pueden infectar el sistema sin que el usuario intervenga.	El ransomware se propaga principalmente como un archivo adjunto malicioso en correos electrónicos de phishing o como enlaces en publicaciones de redes sociales.	Los virus se propagan al descargar o intercambiar archivos, visitar sitios web maliciosos, etc. y son desencadenados por un usuario.
Facilidad de eliminación	Seguir las reglas de ciberseguridad y hacer backup de los datos es la mejor solución para evitar la infección por malware y proteger los datos.	El ransomware es uno de los programas maliciosos más delicados. La mejor para el ransomware es la prevención y hacer	Una de las formas más comunes y eficaces de proteger un «cura» dispositivo de los virus es el software antivirus. backups.

¿Cómo evitar ransomware, virus y otras amenazas?

Después de conocer las diferencias entre los tipos de malware, la primera pregunta que nos viene a la cabeza es: ¿Se puede prevenir un ataque de malware? Hay muchas formas de proteger un dispositivo de una infección. La mejor solución es seguir las reglas básicas de ciberseguridad:

Consigue protección antivirus, antispyware y cortafuegos, y mantenla siempre actualizada.

Actualice regularmente su sistema operativo y sus aplicaciones.

Mejore los ajustes de seguridad de su navegador y bloquee las ventanas emergentes.

Evite abrir mensajes y correos electrónicos de remitentes desconocidos.

No abra archivos adjuntos, enlaces ni sitios web sospechosos.

Evalúe programas, archivos y software gratuitos antes de descargarlos.

Establezca contraseñas seguras y cambie sus datos de acceso con regularidad.

Cumplir estas reglas minimiza el riesgo de que un software malicioso infecte un dispositivo. Sin embargo, nada puede garantizar una seguridad del 100%. Por eso es crucial hacer copias de seguridad de los datos en varias ubicaciones, preferiblemente siguiendo el plan de backup 3-2-1 que incluye backups inmutables, cifrados y aislados de la red. De este modo, incluso en caso de ataque de ransomware, podrá restaurar sus datos con unos pocos clics.

¿Cómo detectar el malware?

Otra pregunta frecuente es cómo determinar si un ordenador o una red han sido infectados. Un ordenador puede estar infectado si experimenta algunos de los siguientes problemas:

Rendimiento lento del ordenador y fallos frecuentes

Comportamiento inestable del ordenador (un ordenador envía mensajes o correos electrónicos no deseados sin la participación del usuario, o abre/cierra programas, etc.)

Pérdida inexplicable de datos

Ventanas emergentes y otros mensajes que aparecen en pantalla Pantalla azul de la muerte (BSOD)

Sin embargo, lo mejor es utilizar un software completo de detección de malware que combine varios métodos de detección con el aprendizaje automático. Estas soluciones pueden escanear su sistema en busca de firmas de virus conocidas o identificar patrones de código similares, supervisar los sistemas en busca de actividades inusuales y ejecutar pruebas de sandbox con archivos sospechosos.

¿Cómo eliminar el malware?

Detectar y eliminar malware puede ser una tarea complicada. A menos que sea un profesional, es fácil pasar por alto algunos elementos y equivocarse. Además, es difícil saber si el malware ha modificado el sistema hasta el punto de que sea imposible revertir los daños. Un procedimiento típico para eliminar malware es:

Ejecute un software antimalware para buscar posibles amenazas.

Una vez detectado el malware, elimine los archivos infectados.

Si no puede hacerlo automáticamente, pida ayuda al técnico de su proveedor de seguridad. Después de formatear una unidad, recupere los datos de los backups (algunas soluciones de copia de seguridad, incluida NAKIVO Backup & Replication, permiten analizar los backups en busca de malware antes de realizar la recuperación) y reinstale los programas si es necesario.

Analizar cómo se infectó un ordenador para evitar ataques de malware en el futuro.

Tómese su tiempo para informar a todos los usuarios de las reglas de ciberseguridad.

Si algunos de tus archivos están cifrados como resultado de un ataque de ransomware, haz lo siguiente:

Nunca pagues el rescate.

Si un ordenador infectado está conectado a una red, desconéctelo o apague el punto de acceso (en caso de conexión Wi-Fi).

Haz una foto de la pantalla de bloqueo que aparece en el monitor. Puede ayudar a identificar el tipo de ransomware.

Utiliza cualquier soporte de sólo lectura con software antimalware, escanea todos los discos del ordenador y elimina el malware.

Si algo va mal, ponte en contacto con un técnico especializado.

El malware más dañino

MyDoom

Los ciberataques no sólo provocan la corrupción de datos y daños informáticos, sino también importantes pérdidas financieras. Uno de los ciberataques más caros fue el provocado por el programa malicioso MyDoom, que causó unos daños estimados en 38.000 millones de dólares. Técnicamente, MyDoom, también conocido como Novarg, es un gusano que se propaga a través de correos electrónicos de phishing.

La gravedad del ataque se debió al enorme volumen de correo electrónico enviado. En un momento dado, en 2004, MyDoom era responsable del envío de una cuarta parte de todos los correos electrónicos. Después de infectar los ordenadores, MyDoom tomó todas las listas de correo electrónico y envió copias de sí mismo. A continuación, los ordenadores infectados formaron una red de bots para realizar ataques DDoS.

MyDoom sigue circulando. Incluso 16 años después de su creación, MyDoom sigue enviando más de mil millones de correos electrónicos con una copia de sí mismo. Nunca se encontró al creador de este gusano, aunque se ofreció una recompensa de 250.000 dólares por encontrar al atacante o atacantes.

ILOVEYOU

La creación de este malware fue un punto de inflexión, o mejor dicho, un punto de no retorno.

ILOVEYOU fue uno de los primeros ciberataques realizados a través del correo electrónico. Este gusano consiguió infectar 50 millones de ordenadores en 10 días, causando un total de

15.000 millones de dólares de daños. Primeramente, envió un correo electrónico que parecía una carta de amor. Y después de la instalación, envió 50 correos electrónicos maliciosos más a los contactos de la víctima.

El gusano fue desarrollado por Onel de Guzman, un estudiante universitario de Filipinas. Como no disponía de fondos suficientes, programó el gusano para que se conectara a los servicios en línea con una cuota de admisión. No podía imaginarse lo grande que llegaría a ser. En aquella época, Filipinas no tenía leyes contra la ciberdelincuencia, por lo que Onel de Guzmán nunca fue procesado. Ahora, con 44 años, el hacker vive en Manila y se arrepiente de haber creado ILOVEYOU.

WannaCry

WannaCry apareció por primera vez en 2017. Este ransomware infectó más de 200.000 ordenadores en unos 150 países, causando daños por valor de más de 4.000 millones de dólares. WannaCry causó pérdidas masivas no solo a empresas y particulares, sino también a instituciones gubernamentales y hospitales. Los hackers exigieron un rescate de 300 dólares en bitcoins. Más tarde, el rescate aumentó a 600 dólares.

Resultó que el malware se aprovechó de la vulnerabilidad de Microsoft en el protocolo Server Message Block (SMB). Dos meses antes del ataque de ransomware, Microsoft publicó un parche de seguridad para proteger los sistemas de los usuarios. Sin embargo, quienes no mantuvieron actualizados sus sistemas operativos quedaron expuestos al ataque de WannaCry.

NotPetya (ExPetr)

El ciberataque ruso de 2017 conocido como NotPetya destaca como uno de los ataques de ransomware más devastadores hasta la fecha. NotPetya, que solo tardó 45 segundos en hacer caer toda la red bancaria, afectó a más de 2.000 organizaciones de todo el mundo, incluidos gigantes del sector como Maersk, Merck, la filial de FedEx TNT Express y Mondelez. El coste estimado de los daños superó los

10.000 millones de dólares, aunque las pérdidas reales superaron con creces esta cifra. Por ejemplo,

Maersk necesitó 10 días y 600 empleados para reconstruir la red, y la recuperación total tardó meses.

NotPetya, que supuestamente tenía como destino el gobierno ucraniano, era un ransomware diseñado para perturbar y destruir más que para obtener beneficios económicos. El ransomware explotaba la herramienta de penetración estadounidense EternalBlue (filtrada en una filtración de datos anterior), que también se utilizó en el ataque WannaCry a principios de ese año, y Mimikatz, una vulnerabilidad de seguridad conocida desde 2011. A diferencia de las versiones anteriores de Petya, que necesitaban la interacción

del usuario para infectar el sistema, NotPetya podía propagarse por las redes en cuestión de segundos disfrazándose de una actualización rutinaria del software de contabilidad.

Ryuk

El primer ataque de Ryuk contra Tribune Publishing en 2018 causó interrupciones en el New York Times y el Wall Street Journal, retrasando su impresión durante varios días. Más tarde, el grupo de piratas informáticos Wizard Spider utilizó a Ryuk para atacar grandes organizaciones gubernamentales, sanitarias, educativas y manufactureras de todo el mundo. El ransomware Ryuk se ha asociado con los mayores rescates de hasta 12,5 millones de dólares, mientras que la ganancia global de los hackers alcanzó los 150 millones de dólares en 2021.

Ryuk suele penetrar en el sistema a través de correos electrónicos no deseados que contienen una infección TrickBot. Ryuk es también uno de los ransomware como servicio (RaaS) más utilizados en la darknet. Los desarrolladores lo venden a otros hackers, llevándose un porcentaje del pago del rescate.

ShrinkLocker

Visión general de ShrinkLocker

ShrinkLocker es una nueva cepa de ransomware detectada por Kaspersky en mayo de 2024. Este ransomware se aprovecha de la función de cifrado de Windows BitLocker para bloquear a los usuarios de sus dispositivos sin ninguna opción de recuperación.

Cómo aprovecha ShrinkLocker BitLocker de Windows

ShrinkLocker está basado en el obsoleto lenguaje de programación para Windows – VBSscript. Después de entrar en el sistema, primero identifica el SO Windows y se apaga (2000, 2003, XP, Vista) o ejecuta las partes de su código que corresponden al SO específico.

ShrinkLocker se aprovecha de BitLocker para cifrar los datos y luego elimina los protectores predeterminados como el PIN, la clave de inicio, la clave de recuperación, etc., dejando a las víctimas sin medios para recuperar los datos cifrados. A continuación, los delincuentes acceden a la clave de cifrado de BitLocker mediante TryCloudflare, la herramienta legítima de CloudFlare para desarrolladores.

Después de un ataque exitoso, ShrinkLocker elimina todos sus archivos y borra los registros de PowerShell para evadir la detección.

No es la primera vez que el ransomware utiliza BitLocker para cifrar datos, sin embargo, la nueva cepa fue más allá para maximizar los daños y dificultar su detección. Microsoft anunció que BitLocker se activará automáticamente en Windows 11 24H2, lo que aumenta el alcance potencial de las víctimas.

Ejemplos de ataques ShrinkLocker

Hasta ahora, este ransomware ha atacado a fabricantes de acero y vacunas en México, Jordania e Indonesia. Los atacantes no dejan ningún archivo con el rescate e intencionadamente hacen que sus direcciones de correo electrónico de contacto sean difíciles de detectar, lo que sugiere que su objetivo son las interrupciones más que el rescate en sí.

Conclusión:

Hoy en día, la ciberseguridad es uno de los retos más importantes. Los virus y ransomware, junto con otros tipos de malware, suponen una grave amenaza para la integridad y seguridad de los datos. La mejor solución para evitar ataques es seguir las reglas generales de ciberseguridad. Para evitar un largo proceso de recuperación y reconstrucción de un sistema desde cero, haga copias de seguridad de sus datos.