Virus y Malware

19/10/2023

Guillermo Bellettini
Seguridad
Creado por: Nicolas Pavel Ballesteros Barrado

Contenido

Definición de Virus informático y ejemplo de un caso famoso

Un virus informático es un tipo de malware que se adhiere a otros programas, se autorreplica y se propaga de un ordenador a otro. Cuando un virus infecta un ordenador, hace copias de sí mismo y se adhiere a otros archivos o documentos.

Funcionamiento de ILOVEYOU:

El virus ILOVEYOU se propagaba a través del correo electrónico y utilizaba tácticas de ingeniería social para engañar a los usuarios.

Correo electrónico atractivo: Los usuarios recibirán un correo electrónico con un asunto tentador como "ILOVEYOU". El mensaje contenía un archivo adjunto llamado "LOVE-LETTER-FOR-YOU.txt.vbs", que parecía ser una carta de amor.

Archivo adjunto malicioso: Cuando los usuarios abrían el archivo adjunto, se ejecutaba un script VBS (Visual Basic Script) malicioso que infectaba la computadora de la víctima.

Propagación: Una vez que se ejecutaba, el virus "ILOVEYOU" se copiaba en el sistema y se enviaba a todos los contactos del usuario a través del correo electrónico, multiplicando su propagación. También se propagaba mediante el sistema de mensajería IRC (Internet Relay Chat).

Daño: El virus "ILOVEYOU" tenía la capacidad de sobrescribir o borrar archivos, incluyendo documentos y medios, y causaba daños graves en los sistemas infectados.

Impacto y consecuencias:

El virus "ILOVEYOU" tuvo un impacto devastador en todo el mundo. Se propagó con rapidez y provocó una interrupción masiva en redes y sistemas informáticos. Además de los daños causados por la pérdida de datos y la interrupción de servicios, también provocó importantes costos económicos.

El virus "ILOVEYOU" fue uno de los primeros ejemplos de un ataque cibernético a gran escala impulsado por ingeniería social. Llegó a una mayor concienciación sobre la importancia de la seguridad informática y la necesidad de educar a los usuarios sobre las amenazas potenciales en línea.

Definición de Troyano y un ejemplo de un caso famoso

Un troyano, en el contexto de la informática, es un tipo de software malicioso que se disfraza como un programa legítimo o inofensivo para engañar a los usuarios. Su nombre proviene de la historia del caballo de Troya, donde un objeto aparentemente inocuo ocultaba un peligroso contenido en su interior. Los troyanos realizan acciones no autorizadas por el usuario, como robar datos confidenciales, dañar sistemas, tomar el control de dispositivos o permitir a un atacante acceder de forma remota a la máquina infectada. Suelen propagarse a través de descargas de software, correos electrónicos maliciosos o sitios web falsos.

Un ejemplo de un caso famoso de un virus troyano es Zeus, que se dio a conocer en 2007. Zeus es un troyano diseñado para ejecutarse en sistemas Windows y se propaga a través de archivos adjuntos de correos electrónicos y sitios web maliciosos que a menudo implican el phishing. Lo que lo hizo notorio fue su rápida propagación y su capacidad para copiar las entradas del teclado de los usuarios infectados. Esto permitía a los atacantes robar información confidencial, como contraseñas y datos financieros, de las computadoras infectadas.

Zeus fue un ejemplo de un troyano que se centraba en el robo de información confidencial y su propagación se debía en gran medida a la ingeniería social utilizada para engañar a los usuarios y hacer que descargaran el malware sin darse cuenta.

Definición de Gusano informático y un ejemplo de un caso famoso

Un gusano informático es un tipo de malware o software malicioso que tiene la capacidad de replicarse y propagarse a través de conexiones de red. A diferencia de los virus, los gusanos no suelen infectar archivos de ordenador, sino que se enfocan en infectar otros ordenadores en la misma red. Los gusanos informáticos son programas que realizan copias de sí mismos y las alojan en diferentes ubicaciones de un sistema informático.

Estos gusanos pueden ingresar a un sistema a través de diversas vías, como vulnerabilidades de software, la internet, correos electrónicos, mensajes instantáneos, o incluso a través de dispositivos de almacenamiento externo, como discos duros. Su característica distintiva es que pueden propagarse de forma independiente sin la ayuda de una acción humana, a diferencia de los virus que requieren un anfitrión para replicarse. Para propagarse, los gusanos aprovechan las fallas de seguridad en los sistemas de destino y utilizan la red informática como un medio para su expansión.

Los gusanos informáticos representan una amenaza en el mundo de la ciberseguridad, ya que pueden propagarse rápidamente y causar daños significativos a sistemas y redes. Por lo tanto, es crucial contar con medidas de protección y seguridad cibernética para prevenir infecciones por gusanos y otros tipos de malware.

El gusano Morris, también conocido como el "Worm de Internet," fue uno de los primeros gusanos informáticos en la historia de la informática. Fue creado por Robert Tappan Morris en 1988 y se propagó a través de ARPANET, la precursora de Internet. El gusano se distribuyó en universidades y centros de investigación conectados a ARPANET.

El gusano Morris se hizo notorio porque no fue diseñado para causar daño, pero tenía un error en su código que hizo que se replicara de manera incontrolada y consumiera recursos en las computadoras infectadas. Esto resultó en un colapso de muchas máquinas y sistemas, lo que causó interrupciones significativas en la red.

El caso del gusano Morris llevó a una mayor conciencia sobre la importancia de la seguridad en línea y fue un punto de inflexión en la historia de la ciberseguridad, lo que resultó en una mayor atención a la prevención de gusanos y otros tipos de malware en Internet.

Definición de adware y un ejemplo de un caso famoso

Un adware en informática se refiere a un tipo de programa o software malicioso diseñado para mostrar publicidad no solicitada en dispositivos informáticos, como computadoras y dispositivos móviles. La palabra "adware" proviene de la combinación de las palabras "advertising" (publicidad) y "ware" (software o programa informático). Este tipo de malware tiene como objetivo principal la generación de ingresos para sus creadores a través de la exhibición de anuncios en línea.

Los adware suelen mostrar anuncios de manera intrusiva, lo que puede resultar en molestias para los usuarios. Además de mostrar publicidad no deseada, algunos programas shareware permiten utilizar el software de forma gratuita a cambio de mostrar anuncios, y los usuarios aceptan esta publicidad al instalar el programa.

Este tipo de software a menudo recopila información sobre el comportamiento de los usuarios, como los tipos de sitios web que visitan, con el fin de mostrar anuncios personalizados. En su nivel más extremo, el adware puede recopilar información personal y rastrear la actividad en línea de los usuarios, lo que plantea riesgos de privacidad.

Un ejemplo de un caso famoso de adware es el adware Conduit. Conduit fue una compañía que desarrolló una plataforma para crear barras de herramientas personalizadas y extensiones de navegador para su distribución. Si bien la compañía afirmaba ofrecer herramientas útiles, sus productos a menudo se consideraban adware debido a sus tácticas de distribución y su capacidad para cambiar la configuración del navegador sin el consentimiento del usuario.

El adware Conduit era conocido por:

Infiltración no deseada: Conduit a menudo se incluía en paquetes de software descargados de Internet. Los usuarios no siempre eran conscientes de que estaban instalando Conduit junto con otro software.

Cambios en la configuración del navegador: Una vez instalado, Conduit podía cambiar la página de inicio del navegador y el motor de búsqueda predeterminado sin el permiso del usuario.

Mostrar publicidad no deseada: Conduit generaba ingresos mostrando anuncios publicitarios en forma de barras de herramientas y extensiones de navegador. Estos anuncios podían ser intrusivos y molestar a los usuarios.

Dificultad para eliminar: Conduit a menudo era difícil de eliminar por completo del sistema, lo que resultaba en una experiencia frustrante para los usuarios.

Debido a sus tácticas y efectos no deseados, el adware Conduit se consideró perjudicial y no deseado por muchos usuarios de computadoras. Este caso sirve como un ejemplo de cómo el adware puede afectar negativamente la experiencia del usuario y la seguridad de la computadora.

Definición de Ransomware y un ejemplo de un caso famoso

El Ransomware, en informática, es un tipo de malware o código malicioso que tiene la capacidad de bloquear o cifrar los archivos y sistemas de una computadora o dispositivo. Este software malicioso toma el control del equipo infectado y restringe el acceso del usuario a sus archivos o incluso a todo el sistema. Para desbloquear o descifrar los archivos, los ciberdelincuentes exigen un rescate, por lo general, en forma de pago en criptomonedas. El término "Ransomware" proviene de la combinación de las palabras "ransom" (rescate) y "ware" (software).

Existen diferentes variantes de ransomware, pero su objetivo común es cifrar o bloquear los archivos de la víctima y luego exigir un pago a cambio de la clave o herramienta necesaria para recuperar el acceso. El ransomware puede propagarse a través de correos electrónicos maliciosos, descargas de software infectado, o explotando vulnerabilidades en sistemas y redes.

Una vez que un dispositivo o sistema se infecta con ransomware, la víctima se enfrenta a la difícil decisión de pagar el rescate o intentar recuperar los archivos por otros medios, como la restauración desde copias de seguridad. Es importante destacar que no se recomienda pagar el rescate, ya que esto no garantiza que los ciberdelincuentes cumplan su promesa de desbloquear los archivos y puede fomentar futuros ataques.

El ransomware es una de las amenazas de ciberseguridad más perjudiciales y ha afectado a individuos, empresas y organizaciones en todo el mundo. La prevención y la educación en ciberseguridad son esenciales para protegerse contra este tipo de malware.

Un ejemplo de un caso famoso de ransomware es el ataque WannaCry, que tuvo lugar en mayo de 2017 y afectó a miles de organizaciones en todo el mundo. WannaCry es un ransomware que se propagó rápidamente explotando una vulnerabilidad en el sistema operativo Windows. El ataque comenzó en Europa y se extendió a nivel global en cuestión de horas.

WannaCry cifró los archivos de las computadoras infectadas y mostró un mensaje de rescate en pantalla exigiendo un pago en Bitcoin para desbloquear los archivos. El ataque afectó a hospitales, empresas, gobiernos y usuarios individuales. Además de los daños financieros, también causó interrupciones en los servicios de atención médica y otros sectores.

Este caso resaltó la importancia de mantener actualizados los sistemas operativos y parchear las vulnerabilidades conocidas, ya que WannaCry se aprovechó de una vulnerabilidad de Windows que Microsoft había parcheado previamente. Aunque muchas víctimas optaron por no pagar el rescate, el ataque puso de manifiesto la amenaza significativa que representa el ransomware y la necesidad de tomar medidas sólidas de seguridad cibernética para prevenirlo.

Este ataque se convirtió en un ejemplo icónico de los riesgos asociados con el ransomware y llevó a un aumento en la conciencia sobre la importancia de la ciberseguridad a nivel global.

Definición de Spyware y un ejemplo de un caso famoso

El spyware, en informática, es un tipo de software malicioso que se instala en una computadora sin el conocimiento ni el consentimiento del usuario. Por lo general, se instala de manera oculta junto con otros programas que se descargan e instalan de manera consciente, lo que dificulta su detección. Una vez en el sistema, el spyware recopila información personal y datos sobre las actividades del usuario para luego enviarlos a terceros sin su autorización.

Este tipo de software malicioso tiene el propósito de espiar las actividades en línea del usuario, recopilando datos confidenciales como contraseñas, historiales de navegación, información financiera y más. La información recopilada por el spyware se utiliza con fines diversos, que van desde la publicidad dirigida hasta actividades fraudulentas como el robo de identidad. El spyware también puede ralentizar el rendimiento de la computadora y dificultar la navegación en Internet debido a las ventanas emergentes no deseadas.

Un ejemplo de un caso famoso de spyware en informática es el caso del spyware FinFisher, también conocido como FinSpy. FinFisher es una herramienta de espionaje cibernético desarrollada por la compañía británica Gamma Group. Esta herramienta se comercializa principalmente a gobiernos y agencias de aplicación de la ley como una solución de vigilancia.

El caso de FinFisher ganó notoriedad en 2012 cuando se descubrió que se estaba utilizando en varios países para espiar a activistas de derechos humanos y disidentes políticos. El software se distribuía camuflado en correos electrónicos y archivos adjuntos maliciosos, lo que permitía a los atacantes tomar el control de las computadoras de las víctimas, acceder a sus comunicaciones y robar información confidencial.

Este caso destacó la preocupación sobre el abuso de herramientas de espionaje cibernético por parte de gobiernos y la necesidad de regulaciones más estrictas en la venta y uso de dichas herramientas. A raíz de este escándalo, se llevaron a cabo investigaciones y se tomaron medidas para limitar la distribución de FinFisher y herramientas similares.

El caso de FinFisher es un recordatorio de cómo el spyware puede ser utilizado con fines de espionaje y vigilancia, y subraya la importancia de la ciberseguridad y la protección de la privacidad en el mundo digital.