Malware en K12

Para principiantes

Bienvenido a nuestra serie sobre ciberseguridad en las escuelas K-12 (primaria y secundaria) Nos vamos de excursión por algunas de las amenazas más comunes a las que se enfrentan las escuelas, amenazas que dificultan un entorno de aprendizaje seguro y pueden tener consecuencias para los alumnos incluso después de salir de la escuela. Hablaremos de **qué son, cómo afectan a las escuelas y cómo prevenirlas.**

Parada de hoy: **malware**.

jamf

EN ESTE E-BOOK, NOS SUMERGIREMOS EN EL MALWARE EN LA EDUCACIÓN CUBRIENDO:

1 Diferentes tipos de malware >

2 Impacto del malware en las instituciones K-12 >

3 Cómo defenderse del malware >

4 Herramientas para crear un entorno de aprendizaje seguro >

¿Qué es el malware?

El malware —software o firmware malintencionado— es una amenaza importante para las escuelas primarias y secundarias. Se presenta en muchas formas y por muchos medios, por lo que es un reto defenderse contra él. Generalmente, el malware se utiliza para arriesgar la confidencialidad, integridad y/o disponibilidad de los datos o aplicaciones de un sistema.

Por ejemplo, el grupo de piratas informáticos Vice Society atacó escuelas con **43 ataques de ransomware entre junio de 2022 y mayo de 2023**. La Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA) **explica el método de Vice Society**:

1. Explotar la vulnerabilidad de aplicaciones de Internet para recopilar credenciales comprometidas y obtener acceso inicial.
2. Explorar la red e identificar formas de aumentar el acceso a los datos.
3. Evadir la detección disfrazando el malware como archivos legítimos.
4. Filtrar datos al exterior.
5. Desplegar ransomware, amenazando con liberar datos sensibles a menos que se pague el rescate.

Naturalmente, esto es motivo de preocupación. Pero las escuelas tienen la capacidad de reducir sus probabilidades de ser víctimas de estos ataques.

Lleve el aprendizaje sobre seguridad a la clase

Malware combina dos palabras: "malicioso", algo que es dañino, y "software", los programas que se ejecutan en una computadora, para referirse a programas informáticos dañinos. Estos programas malignos pueden hacer muchas cosas, como espiar a la gente, robar información, apoderarse de una computadora o intimidar a la gente para que les dé dinero.

Ideas para la lección:

1. Pida a los alumnos que creen un boceto que ilustre qué es el malware

2. Crear un rap sobre la seguridad del malware

Diferentes tipos de malware

RANSOMWARE

El ransomware, en esencia, es una forma de malware en la que agentes maliciosos acceden a los archivos de un usuario, los cifran o codifican y los hacen inaccesibles. Para restablecer el acceso, los usuarios deben pagar un rescate a los atacantes. Los atacantes pueden exigir un pago para descifrar o decodificar los datos y confirmar que han eliminado los datos de sus sistemas.

TROYANOS

Los troyanos son un tipo de malware que aparenta ser un programa legítimo, pero en realidad contiene código malicioso. Este código podría estar empaquetado con archivos descargados de Internet, incluidos paquetes de software legítimos pirateados o comprometidos.

Los troyanos se utilizan para crear backdoors (puertas traseras) que permiten a los malhechores entrar y salir de una red, explotar vulnerabilidades en las aplicaciones, distribuir ransomware y mucho más. A diferencia de los virus y gusanos, los troyanos no se autorreplican ni se propagan a otros sistemas, aunque pueden contener malware que sí lo haga.

VIRUS

Al igual que los virus que nos enferman y se propagan, los virus de malware son capaces de autorreplicarse y propagarse a otros dispositivos tras la interacción del usuario. Permanecen latentes hasta que son activados por una acción del usuario, lo que dificulta la identificación del origen del virus.

Los virus sirven para muchos propósitos a los actores maliciosos, como desactivar o lanzar ciertas aplicaciones, mostrar ventanas emergentes o enviar correos electrónicos masivos sin que el usuario lo sepa. Pueden propagarse a través de enlaces de correo electrónico, archivos adjuntos o descargas en línea para perturbar los sistemas, causar graves problemas operativos y provocar pérdidas y fugas de datos.

Lleve el aprendizaje sobre seguridad a la clase

Idea de la lección:

1. Haga que los alumnos creen un breve video sobre un tipo diferente de malware

2. ¡Crea un juego! Crear un juego de pares que ayude a los alumnos a relacionar los nombres de los malware con lo que son

GUSANOS

Al igual que los virus, los gusanos tienen la capacidad de autorreplicarse. A diferencia de los virus, pueden propagarse por sí solos a otros dispositivos al, digamos, abrirse camino hasta otros dispositivos por sí solos. Los gusanos se utilizan para crear backdoors, desplegar más malware, recopilar datos, sobrecargar redes y mucho más. Se propagan mediante ataques de phishing y otros medios de comunicación o intercambio de archivos, aprovechando las vulnerabilidades del software y de la red.

CRIPTOJACKING

El criptojacking —la toma de control (en segundo plano) de una computadora para minar criptomonedas— es una amenaza creciente para las instituciones. Según Sonicwall, en el primer semestre de 2023 se registró un aumento de 320 veces en el criptojacking en comparación con 2022. El criptojacking, a diferencia del ransomware, no anuncia a gritos su existencia en un dispositivo. Por el contrario, sobrecarga la potencia de cálculo de un dispositivo, reduciendo la velocidad de su sistema hasta en un 70%.

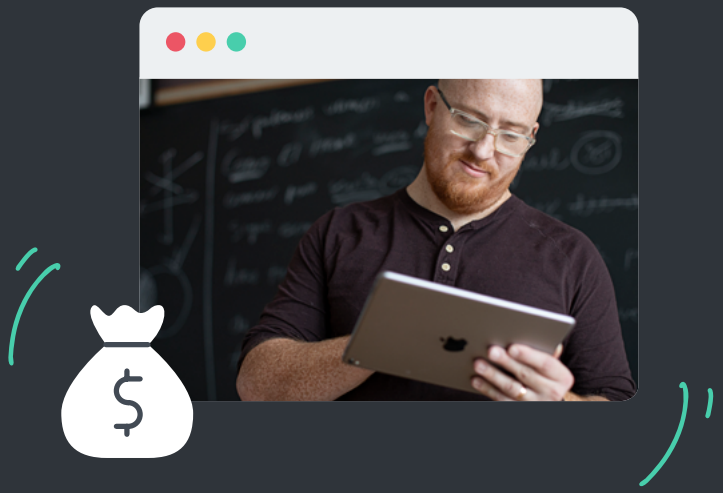
Permanezca atento: más adelante, en esta serie de e-books, profundizaremos en esta creciente amenaza para las escuelas.

SPYWARE

El spyware es un malware que, bueno, espía la actividad de un dispositivo. Por ejemplo, puede registrar los movimientos del mouse, los clics y cualquier acción que realice el usuario. Puede utilizarse para recopilar credenciales o información personal.

Aunque técnicamente no se trata de programas espía, algunas escuelas han optado por vigilar las computadoras de los alumnos con la intención de mantenerlos concentrados y seguros. Pero, ¿es esto realmente más seguro? Este tipo de software **suscita preocupación por la privacidad** y el bienestar de los estudiantes sin proporcionar definitivamente un entorno más seguro.

MALWARE EN LAS ESCUELAS K12



El **80 %** **de los encuestados del sector de la educación inferior se vieron afectados por ransomware, lo** que representa un aumento del 24 % con respecto a 2022. En promedio, el costo de recuperar los datos (excluyendo el pago de un rescate) fue de **$1.59 millones de dólares.**

El malware **puede entrar en un sistema a través de un profesor, un alumno o un administrador**, y los datos pertenecientes a cada uno de estos grupos pueden verse comprometidos por el malware. En **2020, una filtración de datos del Sistema de Escuelas Públicas de Toledo** dio lugar a que unos delincuentes intentaran abrir tarjetas de crédito, pedir préstamos para la compra de autos y otras operaciones similares utilizando la información de los niños del sistema escolar. Y un ataque en 2020 a un distrito escolar estadounidense incluyó información personal identificable (PII) de más de 500,000 estudiantes y otra información de más de 56,000 empleados. Los estudiantes, algunos de los cuales tardan años en poder consultar sus informes de crédito u otras medidas, están especialmente en peligro cuando se trata de que sus datos se vean comprometidos.

El ransomware es el tema de moda en la ciberseguridad educativa. Esta amenaza que suena a teatro es, por desgracia, muy real y muy común, especialmente para las escuelas. De hecho, las **escuelas de primaria y secundaria son el principal objetivo** del ransomware. La publicación de Sophos, **The State Of Ransomware in Education 2023** (El estado del ransomware en la educación, 2023) informa que **80% de los encuestados de educación inferior fueron atacados por ransomware, un aumento del 24% desde 2022. En promedio, el costo de recuperar los datos (excluyendo el pago de un rescate) fue de $1.59 millones de dólares.**

¿Por qué las escuelas son un objetivo tan interesante para el ransomware?

Las escuelas no siempre están preparadas con los mismos recursos que las empresas, ya sea por falta de concientización, de fondos o de soluciones informáticas adecuadas. Como resultado, las **escuelas que son víctimas de ciberataques experimentan**:

de **3** a **21** días de **aprendizaje perdidos**

Posiblemente **meses** de recuperación

Casi **900,000 dólares** en **pagos** de rescates

(si deciden pagar el rescate)

Posible exposición de **datos sensibles**

Afortunadamente, la **mayoría de las escuelas recuperan sus datos**.

73% utilizaba copias de seguridad

47% pagó al azar

2% utilizó otros medios

Pero tenga en cuenta que esto no significa necesariamente que sus datos estuvieran contenidos: los actores maliciosos pueden haber vendido o distribuido los datos.

PREVENCIÓN DE MALWARE

Según el informe de Sophos sobre el estado de la educación, los ataques de ransomware se deben principalmente a:

- Vulnerabilidades explotadas
- Credenciales comprometidas
- Correos electrónicos maliciosos
- Phishing

Parte de la batalla consiste en detener los ataques de malware antes de que puedan arraigar en su sistema. Y como ninguna defensa es impecable, la otra parte es ser capaz de recuperarse con un impacto mínimo en el aprendizaje, las finanzas y el tiempo de inactividad. Ser atacado con malware no es una cuestión de "si", sino de "*cuándo*". Centrémonos en un puñado de formas de reducir el efecto del malware en su sistema.

Aunque sus dispositivos y las normas de su centro de estudios están diseñados para evitar que el malware entre en su dispositivo, ¡usted también puede ayudar a evitarlo!

Esto es lo que puede hacer:

1. Nunca comparta sus datos de acceso con nadie.

2. No descargue archivos o programas de Internet: asegúrese de que proceden de una fuente de confianza; si no está seguro, pregunte.

3. Preste atención a dónde le lleva un enlace. ¿El nombre y el aspecto del sitio web son como deberían? Si le parece sospechoso, no introduzca sus datos. A menudo es mejor volver a escribir el sitio web para asegurarse de que está en la página correcta.

4. Mantenga sus dispositivos actualizados con el software más reciente.

ACTUALIZACIONES Y DISTRIBUCIÓN DE SOFTWARE

Mantener actualizado el software —tanto las aplicaciones como los sistemas operativos— puede reducir las posibilidades de que se explote una vulnerabilidad del mismo. Los ciberdelincuentes pueden crear programas maliciosos que se dirijan a las vulnerabilidades de los programas más utilizados para aumentar los privilegios y/o distribuir programas maliciosos adicionales.

Dado que las descargas en línea —de fuentes confiables o no— pueden contener programas maliciosos, restringir las descargas de software puede ayudar a evitar problemas. Dependiendo de cómo se gestionen sus dispositivos, existen varias opciones para desplegar aplicaciones aprobadas por IT a los usuarios:

- Portal Self Service de Jamf
- App Store
- Apple School Manager
- **A través de su plataforma de MDM**

AUTENTICACIÓN MULTIFACTOR

La autenticación multifactor (MFA) es una primera línea de defensa para evitar que unas credenciales comprometidas provoquen un desastre. La MFA requiere dos o más factores de autenticación para acceder a una cuenta. Estos factores incluyen:

- Algo que **conozca**, como una contraseña o pin
- Algo que **tenga**, como una app de autenticación o un control tipo llavero
- Algo que pueda escanear y **esté** en usted, como una huella digital, una retina o su rostro

Los dispositivos que ofrecen autenticación biométrica, como un iPad, pueden facilitar la tarea a los alumnos más jóvenes que no tengan acceso a otro dispositivo de autenticación. Las escuelas o distritos pueden añadir otra línea de defensa utilizando el inicio de sesión único con MFA para limitar el número de contraseñas que los alumnos tendrían que recordar.

COPIAS DE SEGURIDAD

Como se ha insinuado en párrafos anteriores, las copias de seguridad pueden marcar la diferencia a la hora de recuperar o no sus datos en un ataque de ransomware. Las copias de seguridad periódicas también pueden proporcionar un punto de restauración si sus sistemas se ven comprometidos por otros tipos de malware. Estas dos ventajas por sí solas hacen que las copias de seguridad sean fundamentales para mantener la integridad y seguridad de los datos.

Lleve el aprendizaje sobre seguridad a la clase

Idea de la lección:

1. Haga que los alumnos creen una presentación sobre un consejo de prevención diferente y por qué ayuda a mantener la seguridad de todos

ADMINISTRACIÓN DE DISPOSITIVOS

La administración de dispositivos móviles (MDM) actúa como base para mantener los dispositivos en forma. La MDM ofrece a los administradores la posibilidad de:

- Mantener un inventario de los dispositivos conectados a los recursos escolares
- Determinar el cumplimiento de las normas de seguridad de un dispositivo y actuar en consecuencia
- Actualizar los dispositivos y su software a las últimas versiones
- Exigir determinadas políticas de seguridad para reducir el riesgo de transgresión de datos
- Restringir el acceso a determinadas aplicaciones o sitios web

FILTRADO DE CONTENIDOS

A pesar de la buena educación de los usuarios, la gente comete errores, sobre todo en los dispositivos móviles, donde es difícil ver o previsualizar los enlaces. **Las herramientas de filtrado de contenidos** pueden ayudar a prevenir el éxito de los ataques al bloquear los enlaces maliciosos. Por ejemplo, si un estudiante recibe un correo electrónico de phishing bien disimulado y hace clic en un enlace destinado a recolectar sus credenciales, el filtrado de contenidos puede bloquear su acceso a ese sitio web.

INFRAESTRUCTURA DE SEGURIDAD

Aunque no todas las escuelas o distritos cuentan con el personal, las finanzas o los recursos necesarios para aplicar y exigir el cumplimiento a las partes de una infraestructura de seguridad, proporcionan un objetivo al que aspirar. Este tipo de infraestructuras puede ayudar a guiar a los departamentos de IT hacia la configuración más segura posible para sus recursos y personal:

- Cyber Essentials de la Agencia de Ciberseguridad y Seguridad de las Infraestructuras (CISA) de EE.UU.
- Ciberesenciales del Reino Unido
- la Biblioteca de Infraestructuras de IT (ITIL)

jamf

Lleve el aprendizaje sobre seguridad a la clase

Educación de los usuarios:

Nunca es demasiado pronto para empezar a educar a estar alertas de la ciberseguridad. Los estudiantes, el profesorado y el personal deben estar informados sobre comportamientos riesgosos, como:

- Hacer clic en enlaces antes de considerar su legitimidad
- Compartir sus credenciales de acceso
- Insertar unidades USB desconocidas u otros medios extraíbles en su dispositivo
- Descargar software de sitios de terceros
- No actualizar sus dispositivos o aplicaciones

Los ataques de phishing son extremadamente comunes; los usuarios deben estar atentos para reconocer los intentos de phishing. Características como éstas pueden ser indicadores:

- URL similares con caracteres especiales o formato extraño
- Errores ortográficos o lenguaje inusual en los correos electrónicos (aunque los atacantes ahora crean mensajes cada vez mejores)
- Exigencia urgente para actuar
- Mensajes inusuales o no solicitados, incluso de personas conocidas

IMPLANTACIÓN: JAMF SCHOOL Y JAMF SAFE INTERNET

Bien, ya hemos hablado de algunas formas de prevenir el malware. Pero, ¿cómo aplicamos realmente estas estrategias?

Jamf School

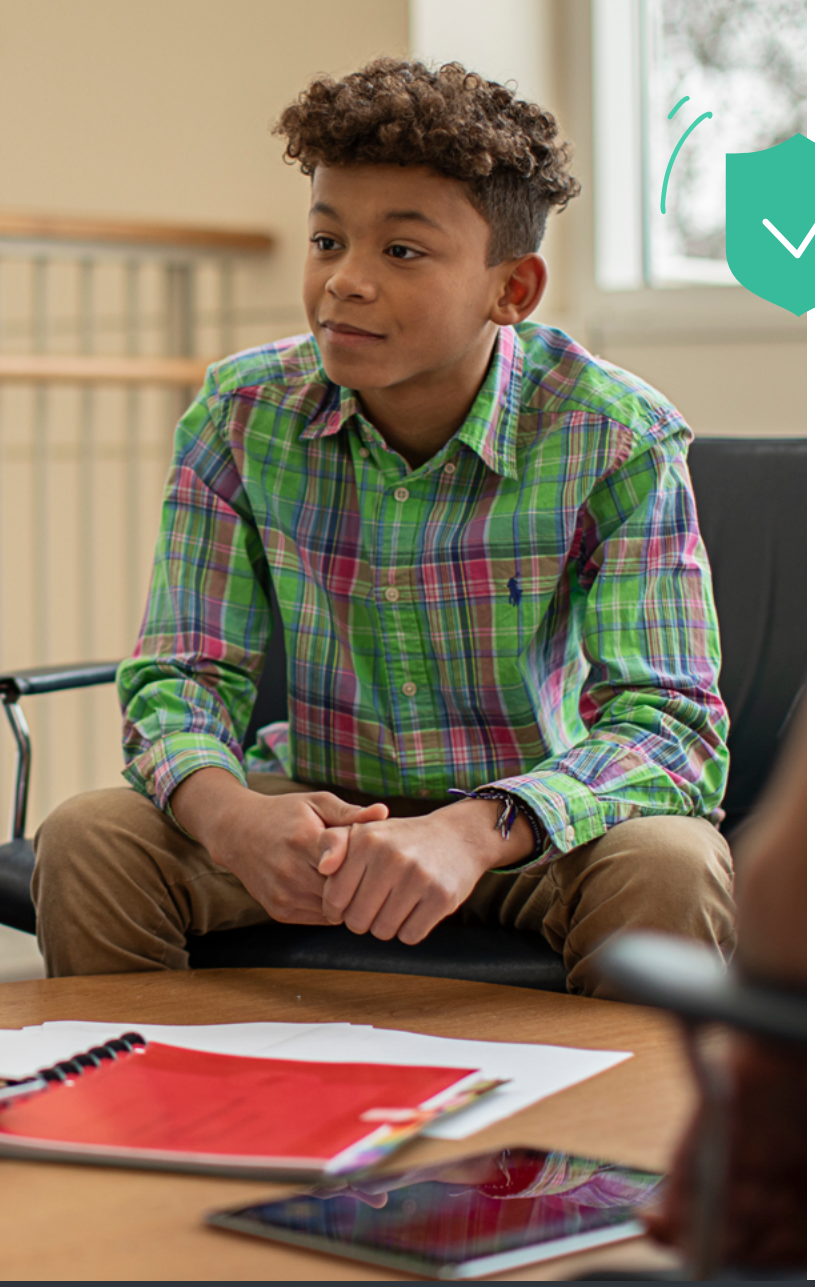
Hemos mencionado que la MDM es la base para mantener sus dispositivos seguros. Aunque no es suficiente por sí sola, es fundamental, ya que proporciona la transparencia necesaria sobre los dispositivos que interactúan con los datos de estudiantes y empleados.

En cierto modo, la **administración ES seguridad.**

Jamf School es una MDM para escuelas que facilita la implementación, administración y protección de Mac, iPad, iPhone y Apple TV. Ofrece:

- Transparencia de los dispositivos, usuarios y aplicaciones administrados
- Implementación y actualización sencillas del software
- Posibilidad de configurar los parámetros de seguridad del dispositivo, incluidas las políticas de contraseñas y el filtrado de contenidos
- Implementación y actualización de aplicaciones sólidas y seguras con aplicaciones verificadas
- Herramientas de administración del aula para mantener la atención de los alumnos

La seguridad empieza en la administración: conocer los dispositivos —y lo que hay en ellos— significa que puede respaldar la seguridad del dispositivo, desde las actualizaciones del software necesario hasta la implementación de controles de seguridad específicos.



Jamf Safe Internet

Jamf Safe Internet va más allá de la MDM para crear un entorno de aprendizaje seguro al permitir a los estudiantes navegar de forma privada sin encontrarse con malware u otros tipos de contenidos peligrosos. Compatible con dispositivos Apple, ChromeOS y Windows, Jamf Safe Internet es:

Totalmente personalizable con la flexibilidad de establecer o cambiar fácilmente las políticas que se aplican a diferentes grupos en función del tipo de dispositivo, la geografía u otros atributos. Jamf Safe Internet funciona con cualquier dispositivo administrado, ya sea que viva en un carrito, haya sido asignado por la escuela o sea de propiedad personal.

Potente filtrado de contenidos con:

- Google Safe Search reforzado
- Modo restringido de YouTube para solo mostrar contenidos educativos
- Aprendizaje automático avanzado para detectar y prevenir amenazas no descubiertas
- Protección en tiempo real dentro de la red para impedir el acceso a sitios de phishing y otros dominios maliciosos

Seguridad sin vigilancia permitiendo a los alumnos la libertad de explorar Internet y desarrollar su ciudadanía digital, sin violar su intimidad ni ponerlos en peligro.

jamf

Vea cómo Jamf puede ayudarle a formar parte de su solución tecnológica, de seguridad y de filtrado de contenidos

Empiece ahora

www.jamf.com/es/