¿Qué es ransomware

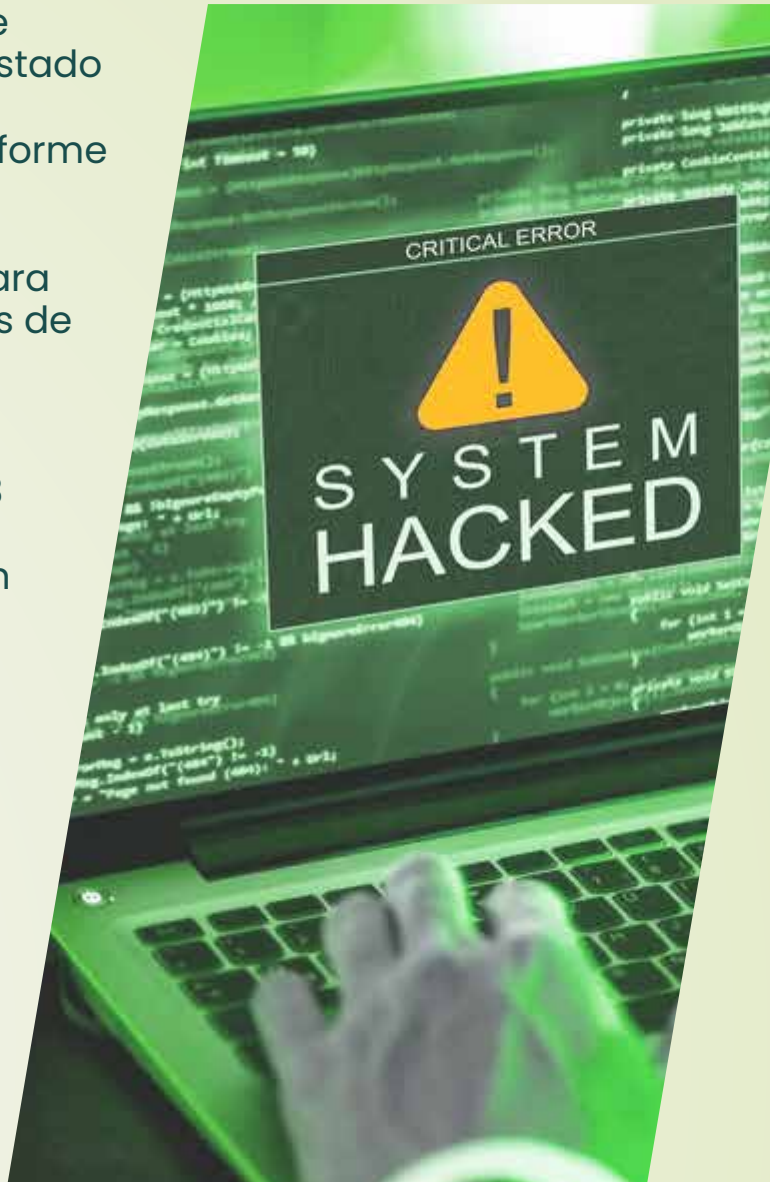
y cómo minimizar el riesgo?

intexus

CREANDO UN MUNDO CONFIABLE

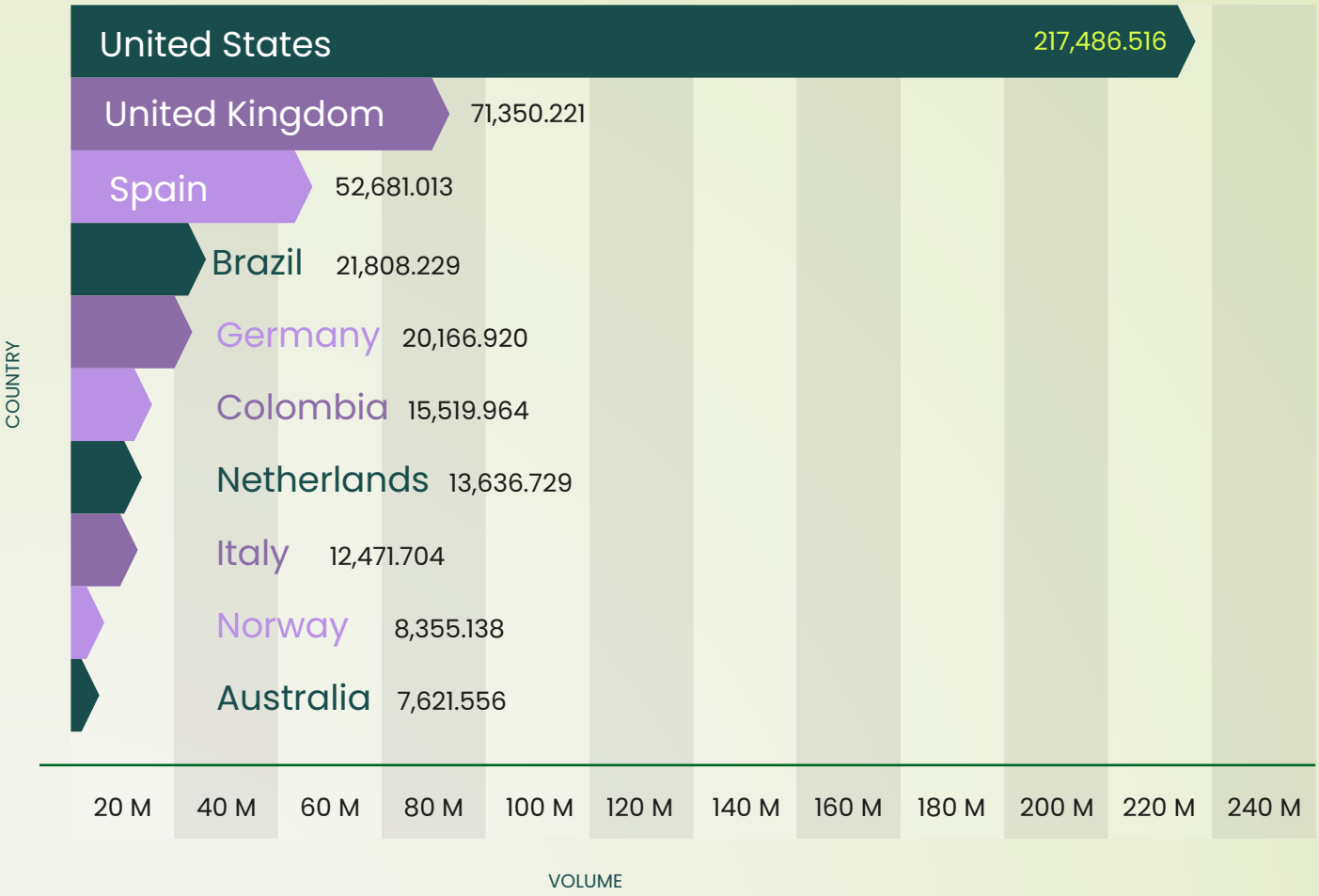
Informe de ataques Ransomware 2023

Colombia y Brasil son los 2 países de Latinoamérica que aparecen en el listado de los 10 países del mundo con más ataques de ransomware según el informe “Amenazas Cibernéticas 2023” de la empresa SonicWall, recordando la importancia de la ciberseguridad para las organizaciones latinoamericanas de todas las industrias.



Según SonicWall, los ataques de ransomware aumentaron en el 2023 un 38% respecto al año anterior en América Latina, donde se registraron 3.277.414 ciberataques diarios en el 2023, es decir, 2,274 ataques por minuto o un equivalente a 38 ataques segundo.

Top 10 de países con más ataques de ransomware- **SonicWall**



Los primeros ciberataques

El cibercrimen ha evolucionado con el pasar de los años, el avance de la tecnología y el conocimiento especializado en programación que detecta fallos o brechas de seguridad en nuestra estructura de redes y sistemas. Cada día los ataques informáticos son más sofisticados y creativos, es por eso que gobiernos e industrias buscan soluciones que les ayude a anticiparse, previniendo y minimizando el impacto de un cibercrimen.

Virus y Malware

Los primeros ataques se efectuaban a través de virus informáticos, pequeños códigos maliciosos de programación, que se crean con el objetivo de causar daño a sistemas en los que se ejecuten, desde servidores, computadores de mesa, portátiles y dispositivos móviles. Incluso ya se pueden detectar virus que atacan dispositivos IoT (lavadores, refrigeradores, smart tv, entre otros), al transmitirse desde internet.

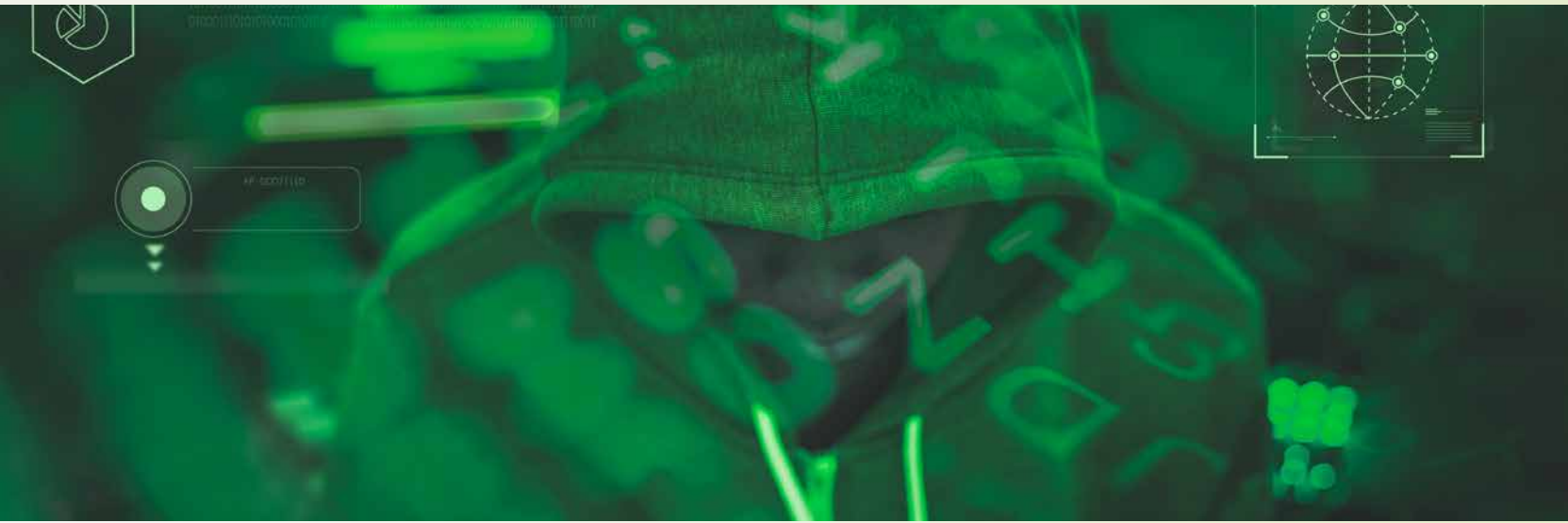
La característica principal de un virus es que solo puede ser activado o ejecutado por el usuario, ya sea haciendo clic en un archivo adjunto en un email o ejecutando un archivo en el cual va adherido el código malicioso y además tiene la capacidad de replicarse. Los virus más conocidos son Melissa, ILoveYou, WannaCry, entre otros y generalmente, robaban información y la enviaban a destinos desconocidos, eliminaban archivos de imagen o lograban dañar archivos determinados.

Los malware, también son códigos maliciosos en general que contienen virus, entonces un virus es un tipo de malware, pero encontramos otros tipos de este tipo como:

- **Gusanos:** programas que realizan copias de sí mismos.
- **Troyanos:** oculta software malicioso dentro de un archivo que parece normal.
- **Keyloggers:** registra todas las pulsaciones de teclas que realice en el ordenador.
- **Spyware:** recopila información confidencial de usuarios, sus equipos o los hábitos de navegación y se la envía a terceros.
- **Adware:** diseñado para mostrar anuncios en su pantalla.
- **Ransomware:** encripta y secuestra la información pidiendo un rescate para su liberación. Y muchos otros.

Estos ataques se pueden contener por medio de los antivirus y los antimalware. Un antivirus es un sistema preventivo que escanea y detecta los virus antes de ser ejecutados y actúan como vacunas o firmas de identificación de patrones o huella digital de los virus para ser aislados en cuarentenas informáticas o eliminados del sistema según decisión del usuario.

Por su parte un antimalware, escanea y detecta malware que se está ejecutando y los elimina automáticamente o los lleva a cuarentena para su posterior tratamiento del usuario.



¿Qué es Ransomware?

El ransomware es un tipo de malware, es decir, es un algoritmo criptográfico programado para impedir el acceso a los datos. Su nombre se deriva de la unión de la palabra ransom que en inglés significa rescate y ware que traduce mercancía. Puede infectar desde dispositivos de escritorio, dispositivos móviles con sistemas operativos IOs y Android, hasta dispositivos IoT y sistemas de redes en las compañías.

El ransomware se apropia de los datos cifrando toda la información. Estos ataques se caracterizan por tener fines económicos extorsivos y los daños dependen del tipo de ransomware utilizado.

Tipos de ataques ransomware

Un ransomware de daño leve, impedirá el uso del dispositivo y notificará por medio de una alerta de antivirus la existencia de dicho malware, solicitando el pago de una actualización para solucionarlo y así obtener el desbloqueo de manera remota. Estas alertas continuarán molestando al usuario hasta que se pague la supuesta actualización. Estos ciber delincuentes también se pueden hacer pasar por autoridades oficiales como Policía Digital, FBI, INTERPOL, entre otras y cobrar una falsa sanción económica por actos indebidos online.

Existe otro tipo de **ransomware de daño medio** que bloquea la pantalla e impide el uso del dispositivo y aunque los datos están intactos, solo se puede desbloquear por medio del pago, hay algunas maneras técnicas en modo seguro de recuperar el control nuevamente con normalidad.

Un ransomware de daño fuerte es más sofisticado y complejo, puede encriptar toda la información de los discos duros del dispositivo haciéndolos ilegibles y no existe antivirus o desarrollo de seguridad o de cifrado que pueda enfrentar este tipo de ataque o recuperar la información. Generalmente cuando este tipo de ataque ocurre, aparece un banner que cubre toda la pantalla del equipo exigiendo el pago de una suma importante de dinero en bitcoins, a cambio de la no divulgación de la información o la recuperación desencriptada de los archivos comprometidos para volver a tener el control de los datos, sin embargo, el pago del rescate no garantiza la devolución o la no distribución de los datos a terceros. Es por esto, que las autoridades especializadas en ataques de ransomware nunca recomiendan el pago del rescate.

Son diferentes las maneras de adquirir un ransomware, la más común es por medio de emails no solicitados en los que se suplanta la identidad de entidades o instituciones oficiales del gobierno, educación, financieras y comerciales entre otras y que por medio de la ingeniería social, persuaden a las víctimas a que descargue algún archivo adjunto (PDF) o a que naveguen una página clonada. Mientras la víctima navega el sitio falso, se va descargando el malware internamente en segundo plano.

También le puede interesar: Prevenir un ciberataque es posible reforzando la soberanía digital.

Acciones y estrategias para la prevención del Ransomware

Aunque todavía no hay un parche de seguridad, desarrollo o plataforma que enfrente y resuelva un ataque de ransomware desencriptando la información, si podemos adoptar algunas medidas preventivas que nos ayudarán a estar preparados y reducir los riesgos.

Las acciones más recomendadas e inmediatas son:

- Concientizar al personal sobre los ataques informáticos, evitando descargar archivos en correos sospechosos o no solicitados que representen alguna entidad reconocida.Aplica en el acceso a redes sociales en jornada laboral.
- Evitar a toda costa el ingreso de usuarios no autorizados, esto se logra por medio de la implementación de soluciones de autenticación multifactor.
- Protección de los equipos físicos y redes con la instalación de programas antimalware, realizando actualizaciones periódicas y evitando el uso de software ajeno a la compañía. Evitar el uso de unidades de memoria desconocidas (USB).
- Garantizar la autenticidad de la información de intercambio y en tránsito por medio de certificados y firmas digitales.
- Contar con un servidor accesible desde internet pero con una configuración DMZ (red o zona desmilitarizada) es decir, preparar una red aislada de la red interna que atienda todos los servicios externos de internet y así evitar que el atacante alcance los servidores y la red interna. Se deben instalar detectores de intrusos por su riesgo y exposición abierta a internet.
- Protección de la información sensible por medio de soluciones de cifrado criptográfico en unidades HSM (Host Security Module) y el uso de gestores de llaves criptográficas, así como realizar copias de seguridad de forma constante.

Los anteriores son algunas medidas que se pueden implementar para disminuir el riesgo de caer en un ataque informático de ransomware, sin embargo se deben contemplar estrategias, marcos y programas de seguridad más robustos, para blindar a las compañías desde todos los frentes, que cuenten con parámetros y políticas definidas para proteger la información, los dispositivos, y los activos.

Un ataque de ciberseguridad pone en riesgo la estabilidad de una empresa con graves consecuencias de reputación, económicas u operativas. Prevenga y cuente con aliados especializados como Intexus para proteger su data de forma efectiva. Contáctenos hoy mismo para más información:

intexus

CREANDO UN MUNDO CONFIABLE

Contáctenos hoy mismo

www.
intexus
.la

@Intexus

info@intexus.la

Cel: +57 316 026 0947