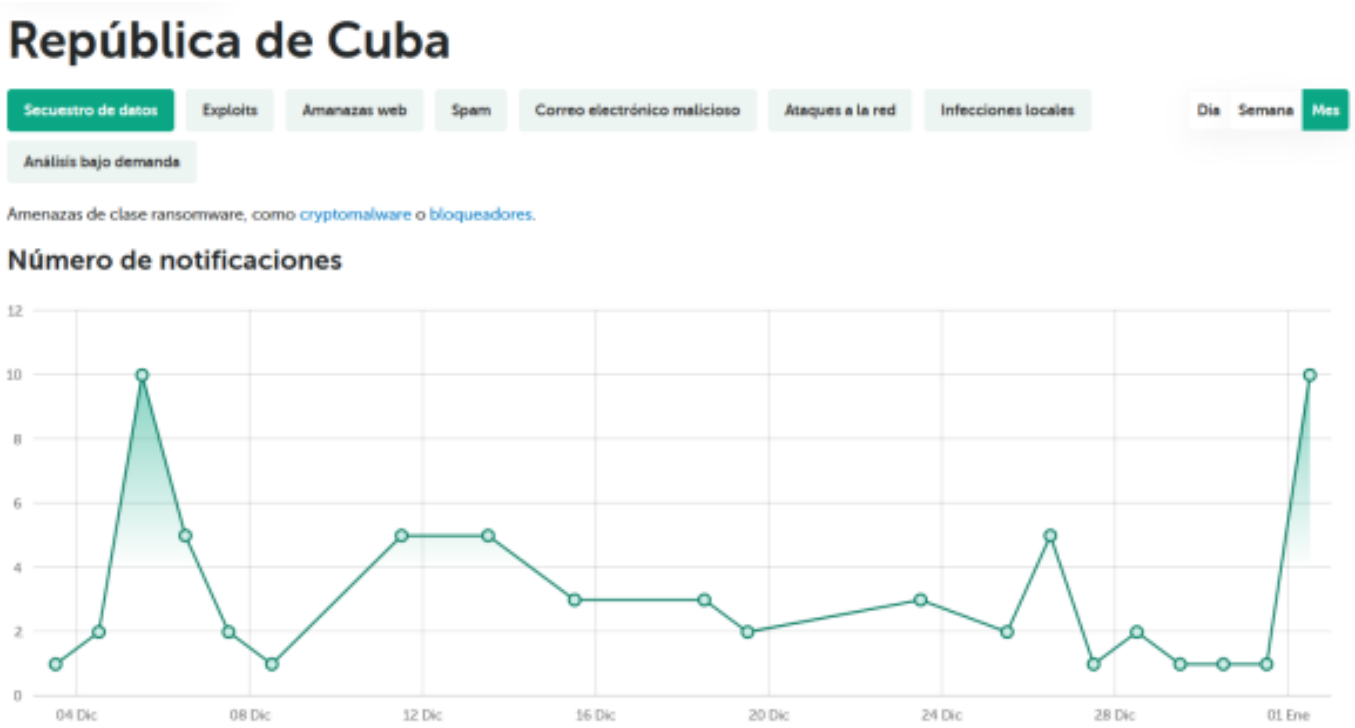
Si de secuestro de datos se trata, lo mejor que resulta es estar siempre alertas.
Última actualización: Jueves, 04 Enero 2024 10:55
Visto: 134

Inicia el año 2024 lleno júbilo y alegría en todo el mundo, sin embargo, las amenazas presentes en el ciberespacio no se detienen. Hoy mis estimados lectores vengo hablarles acerca de una de las amenazas que se ha traslado al mundo digital en los últimos años. Me refiero al secuestro de datos (ransomware según su terminología en idioma inglés).

El ransomware es un tipo de software malicioso diseñado para facilitar diferentes actividades nefastas, como impedir el acceso a los datos personales a menos que se pague un rescate.

Los ataques de ransomware por lo general tienen un serio impacto negativo en la economía cuando son ejecutados con éxito. Pueden causar daños financieros considerables, reducen la productividad, interrumpen las operaciones comerciales normales y dañan la reputación de individuos o empresas. Según las estadísticas de 2023, publicadas en el boletín de seguridad de la compañía multinacional rusa Kaspersky dedicada a la seguridad informática, los troyanos cifradores atacaron a 193 662 usuarios únicos, entre ellos 52 999 pertenecientes a empresas gubernamentales. Durante el periodo abarcado por el citado informe, **se reportan 23 364 modificaciones de cifradores y 43 nuevas familias**. Vale destacar que Cuba no está ajena a este problema de seguridad. **Durante el último mes del año se han notificado un total de 65 amenazas de este tipo como se muestra en la siguiente figura.**



Con información de estadísticas: Sitio oficial de Kaspersky Lab, 2023

Estos ataques también pueden resultar en una pérdida permanente de información o archivos. Lo más lamentable que tienen estos ataques es que incluso pagar el rescate no garantiza que el sistema o los archivos sean desbloqueados. Para las empresas que pagan el rescate, el costo de recuperarse del ataque se duplica en promedio. Solo por poner un ejemplo de su impacto en el 2021, estos ataques le costaron al mundo un total 20.000 millones de dólares. De todas estas estadísticas, está claro que se debe entender primero el comportamiento del ransomware y sus variantes para detectar y mitigar eficazmente los ataques futuros. Debido a su rentabilidad, siguen surgiendo nuevas variantes de ransomware que eluden las aplicaciones antivirus tradicionales y otros métodos de detección. Por lo tanto, **es fundamental idear una nueva generación de contramedidas eficientes.**

Las soluciones preventivas apuntan a bloquear, mitigar o revertir el daño causado por el ransomware. **Los enfoques preventivos comunes incluyen:**

- **Almacenar datos y/o copias de seguridad.** Mantener copias de seguridad regulares de los datos almacenados en una computadora o una red puede minimizar en gran medida el impacto del ransomware. En cambio, el daño se limita simplemente a cualquier dato que se ha creado desde la última copia de seguridad. Esto implica altos costos para las empresas. Hay gastos generales en

la reserva de grandes cantidades de datos, por lo que elegir la frecuencia con que se deben tomar copias de seguridad y cuánto tiempo se mantendrán son decisiones importantes que deben tomarse.

- **Aumentar la conciencia y la capacitación de los usuarios.** Sensibilizar a los usuarios sobre los ataques de ransomware y entrenar a los usuarios sobre cómo evitarlos puede prevenir ataques antes de que ocurran.
- **Hacer cumplir un estricto control de acceso.** El control de acceso evita el cifrado de ransomware restringiendo el acceso de los usuarios al sistema de archivos. Por lo general se propone establecer en las organizaciones políticas de menor privilegio y separación de funciones mediante el control del acceso basado en el rol que ejecuta cada usuario; se debe siempre restringir el acceso a los datos lo más lejos posible de la jerarquía del directorio; así como se sugiere auditar rutinariamente los permisos y funciones establecidas para cada usuario.
- **Los antivirus no son suficiente:** Se sugieren implantar sistemas de protección que combinan el antivirus tradicional con otras herramientas de monitoreo e Inteligencia Artificial, permitiendo tener un control mayor en caso de amenazas o vulneraciones a la seguridad de una organización. De cualquier forma el mecanismo de seguridad que se implemente se debe mantener actualizado para que sea capaz de identificar las nuevas amenazas que surjan.

Una vez perpetrado el ataque para detectarlo **algunas sugerencias son:**

- **Revisión de la información del sistema.** En algunas ocasiones se puede utilizar la información del sistema, como archivos de registro o cambios en el propio Registro del Sistema Operativo, como método de detección. Se sugiere realizar una monitorización continua de los valores del registro, junto con la actividad del sistema de archivos.
- **Análisis de nota de rescate:** Después de la ejecución de un ataque de ransomware, una nota de rescate generalmente no se le da mucha importancia. Esta nota se puede guardar en la computadora en forma de un archivo de texto o mostrarse en la pantalla del usuario. La misma informa al usuario de que sus archivos personales han sido cifrados o son inaccesibles y da pasos sobre cómo pagarlos y recuperarlos. El análisis estático y dinámico puede revelar los rasgos de las notas ransomware y de esta forma se puede determinar a que tipo de cepa pertenece y cuáles son sus principales características.
- **Auditoría de los archivos locales:** Grandes cambios realizados en un sistema de archivos de una computadora podrían indicar que un ataque de ransomware está en marcha. Hay varias métricas que se pueden utilizar para detectar cambios significativos en los

archivos. Las tres métricas identificadas a partir de la literatura científica son entropía, tipo de archivo y diferencias de archivo (es decir, similitud). Además, varios investigadores analizaron las operaciones de archivos de Entrada/Salida para detectar actividades sospechosas.

- **Análisis de tráfico de la red**: El análisis de tráfico de la red intercepta paquetes de red y analiza los patrones de tráfico de la comunicación para detectar ataques de malware en curso. Un comportamiento anómalo se puede revelar estudiando ciertas características de tráfico, como son por ejemplo tamaño del paquete, frecuencia de mensajería, presencia de dominios maliciosos, entre otros.
- **Utilización del Aprendizaje Automático y herramientas de Inteligencia Artificial**: Muchos estudios proponen modelos de aprendizaje automático que detectan ransomware clasificando los programas informáticos basados en su comportamiento. Con suficientes datos de entrenamiento, estos modelos pueden detectar ataques con un alto grado de precisión. Además, con frecuencia son capaces de detectar ransomware antes de que tenga la oportunidad de cifrar cualquier archivo. Sin embargo, encontrar un modelo adecuado requiere prueba y error, por lo que el sesgo o sobreadaptación puede ocurrir si no se toman las medidas adecuadas.

Cubadebate.