Kepler

RANSOMWARE

SE HA VUELTO NUCLEAR

55%

de los pequeños negocios
PAGA RESCATE A LOS HACKERS

Cada **14**
SEGUNDOS
una compañía es atacada por Ransomware

Para 2021 se pronostica:

Costos
57 VECES
más altos durante seis años y **MMUS$20.000** *en daños causados por Ransomware*

RANSOMWARE 2.0

- *Destruye respaldos*
- *Roba credenciales*
- *Expone a las víctimas públicamente*
- *Filtra información robada*
- *Amenaza a los clientes de las víctimas*

Kepler

Me atacó un Ransomware, **SECUESTRARON MIS DATOS,** *¿qué hago?*

Un Ransomware es un tipo de malware que tiene el objetivo de bloquear el uso del pc o parte de la información que contiene, para luego solicitar un rescate (generalmente en bitcoins) a cambio de su liberación.

Los atacantes **aprovechan vulnerabilidades del software** de los equipos, sus sistemas operativos, sus aplicaciones o simplemente engañando a usuarios con un correo electrónico infectado.

La gran mayoría de infecciones con Ransomware se debe a ataques de ingeniería social, donde en este proceso **engañan a los usuarios para dar accesos al malware o conseguir contraseñas de acceso.** Es esencial formar a los empleados enseñándoles a reconocer este tipo de situaciones y cómo reaccionar.

EN CASO DE SER INFECTADO POR ESTE MALWARE, SE RECOMIENDA TOMAR LAS SIGUIENTES MEDIDAS:

- Aislar los equipos con Ransomware (desconectar de la red).
- Toma un par de archivos encriptados para enviarlos a nuestro laboratorio para su análisis.
- Enviar la nota de rescate (puede ser un archivo de texto en el escritorio o una imagen en la pantalla) para su análisis.
- Clonar los discos duros infectados.
- Denunciar el incidente a la PDI.
- Cambiar todas las contraseñas de red y cuentas online.
- Desinfectar los equipos y recuperar los archivos cifrados.
- Restaurar los equipos.

Para prevenir un ataque de Ransomware se pueden tomar una serie de medidas técnicas que pueden mitigar este evento.

RESPALDOS

Realizar respaldos periódicos y automatizados de los equipos de escritorio y servidores, se recomienda que sean en una locación remota, ya que, si la copia de seguridad se encuentra en la misma red, también podría ser afectada e inutilizada. También es recomendado no solo utilizar respaldos del tipo cloud (Dropbox, Google Drive, OneDrive, etc), ya que existen familias de Ransomware que afectan a este tipo de plataformas. En Kepler contamos con un sistema de respaldo automatizado tanto para estaciones de trabajo como para servidores. Este respaldo remoto protege tu información del ransomware Más información a backup@kepler.cl

ACTUALIZACIÓN DE SOFTWARE
y licenciamiento

Los atacantes se enfocan en aprovechar vulnerabilidades de software, sistemas operativos o firmware, de forma manual y automatizada. En cuanto más actualizado esté un software, menos vulnerabilidad tendrá y más difícil será que logren entrar o infectar un sistema. Es recomendado mantener los sistemas actualizados automática y centralizadamente.

Si utiliza software a medida (desarrollo exclusivo), se recomienda realizar auditorias al software para evitar vulnerabilidades.

CONTROLES DE ACCESO
y mínimos privilegios

Es necesario mantener un nivel mínimo de privilegios de seguridad de usuarios. Evitar que tengan más privilegios de los que necesitan para evitar el mal uso de cuentas, contraseñas, permisos para instalar softwares, etc. Utilizar contraseñas robustas y si es posible, con multi-factor de autentificación para evitar un ingreso no deseado en caso de que estas contraseñas sean descubiertas por atacantes. Evitar el uso de cuentas de administración y deshabilitar cuentas de usuarios que no sean necesarias es esencial para complicar el acceso a datos a un atacante.

MINIMIZAR EXPOSICIÓN A *internet*

Evitar la exposición de la red interna de la empresa hacia Internet es clave. No todos los servicios de la red necesitan ser publicados o expuestos. En caso de ser necesario levantar un servicio, es importante utilizar herramientas que permitan limitar los accesos a la red, como es el caso de un firewall, donde se puedan establecer reglas para bloquear o permitir conexiones de entrada o salida de la red.

En un firewall se puede establecer que tipo de conexiones son permitidas (web, correo, db, etc), el sentido en que se permiten (hacia o desde Internet), a los equipos que se incluye en la regla y establecer direcciones bloqueadas que pueden ser detectadas automáticamente o de forma manual.

Otra utilidad importante es la DMZ, que permite mantener una red aislada de la red interna en la que es posible mantener los servicios aislados. Se recomienda mantener la red monitoreada y con los servidores actualizados.

CONFIGURACIÓN DE EMAIL

Fundamental es realizar un entrenamiento continuo a los usuarios para transformarlos en el primer filtro de seguridad de la organización. Luego utilizar filtros de spam para evitar que los correos de phishing (maliciosos) lleguen a los usuarios. Evitar el e-mail spoofing utilizando autentificación de correos entrantes (SPF, DMARC o DKIM). Escanear correos entrantes y salientes para detecta amenazas en posibles archivos infectados, configurar el sistema para que permita ver las extensiones de los archivos para evitar abrir archivos ejecutables. También es recomendado deshabilitar macros en los archivos de Office. En caso de necesitar abrir un archivo con macro, se recomienda primero verificarlo con una herramienta de antimalware o un Office Viewer para que no sea ejecutado código malicioso que permita tomar control del equipo.

REALIZAR UNA AUDITORÍA O ANÁLISIS *de seguridad de la red*

Es una buena práctica analizar los equipos con software anti-malware y establecer que se ejecuten periódicamente. Este debe ser actualizado y debe mantenerse activo. También es recomendable realizar una auditoría o análisis de seguridad de red que permitan entender las capacidades de defensa ante los ataques actuales. Estos análisis permiten tener un detalle de las vulnerabilidades activas y posibles brechas.

En conclusión, tener un programa de entrenamiento anual para todo el personal, realizar mejoras seguras en forma continua y permanente, analizar los equipos y las redes, minimizan las probabilidades de volver a ser víctima de un ataque y reduce drásticamente el costo de este. Si te interesa un análisis de vulnerabilidad efectuado por nuestro equipo de Ethical Hacker Certificados, escríbenos a redteam@kepler.cl

En Kepler existimos para proteger tu información frente a Ransomwares y otros factores de ataques, internos y externos.

PUEDES CONTACTAR A NUESTROS EQUIPOS *por los siguientes temas:*

Concientización en Ciberseguridad:
Transforma a tu personal en un firewall humano a través de un programa de concientización anual en ciberseguridad: capacita@kepler.cl

Respaldos:
Crea respaldos automatizados fuera de tu organización, sin errores humanos, lejos de su fuente de origen: backup@kepler.cl

Análisis de vulnerabilidades:
Permite que un grupo de expertos revisen las vulnerabilidades de tus instalaciones y te guíen en la mitigación de estas: redteam@kepler.cl

Peritaje informático:
Si ya fuiste víctima de un robo de información o ataque informático, podemos ayudar a descubrir información en fuentes digitales y presentarlas internamente o en tribunales: peritajes@kepler.cl

EDR + Hacker Hunting:
Permite que Kepler detecte a tiempo una intrusión y pueda tomar control de la situación, distrayendo al atacante, revelando y parchando la vulnerabilidad para luego eliminar al intruso recolectando evidencia del ataque: edr@kepler.cl