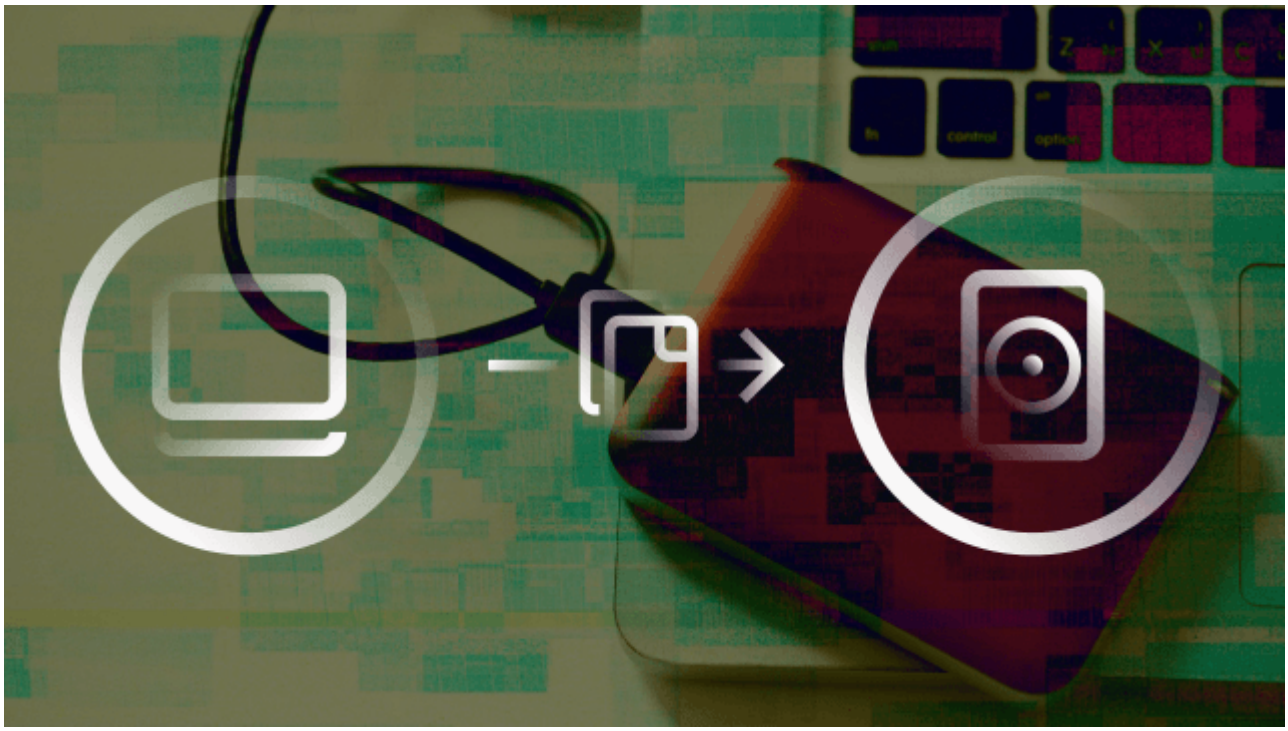
Ransomware, mejores prácticas para prevenir daños irrecuperables

Ransomware, mejores prácticas para prevenir daños irrecuperables.Hemos creído necesario crear esta pequeña guía, resumen o bitácora de viaje, pensando en los sistemas y servidores de clientes y lectores. Contiene algunos principios valiosos para ser menos vulnerables a este tipo de ataques y exposiciones de datos en la red.

Aquí no hay negocio grande o chico, todos estamos propensos a ser víctimas de este tipo de acciones, por tanto, como dice la sabiduría popular que hombre prevenido vale por dos, eso es lo que queremos hacer, prevenir.

Hospitales que detienen sus actividades por días, fábricas que cierran hasta tanto puedan recuperar su presencia en linea, etc. etc.Ejemplos pululan por montones.

Lo anterior sin olvidar que los creadores de malware evolucionan así mismo deben hacerlo nuestros sistemas, administradores, protocolos y procesos, no podemos anquilosarnos, quedarnos estancados o desactualizados porque concedemos mayores ventajas a nuestros atacantes.



Prevención

Haga copias de seguridad regularmente de sus archivos

Ransomware capitaliza el miedo: el miedo de quedar fuera de la máquina, perder el acceso a datos personales o de misión crítica, o interrumpir las operaciones comerciales. Elimine el apalancamiento del secuestrador de datos mediante una copia de seguridad periódica de sus archivos. Practique la regla 3-2-1 creando tres copias de seguridad en dos formatos diferentes con una almacenada fuera del sitio. Al realizar una copia de seguridad de sus datos, asegúrese de su integridad. Las copias de seguridad solo son valiosas si son accesibles. Pruebe periódicamente sus copias de seguridad para verificar que sean legibles. Simplifique (y documente) su procedimiento de copia de seguridad para que el personal autorizado pueda recuperarlos fácilmente cuando sea necesario.

¿Ha probado nuestro backup remoto?

Mantenga sus programas y sistema operativo actualizados

Muchos programas maliciosos de encriptación de archivos se aprovechan del sofware desactualizado y sus vulnerabilidades para hacer de las suyas.
Las fallas de seguridad se conjuran con parches y actualizaciones a tiempo, aquí enfatizo la palabra tiempo.
Utilizar de forma segura los componentes del sistema y las herramientas de administración.
Los ciberdelincuentes están abusando cada vez más de utilidades legítimas y herramientas de administración del sistema para instalar y ejecutar malware. Este modus operandi proporciona a los malos la eficiencia, la conveniencia y el sigilo.

Mitigue este tipo de ataques aplicando el principio de privilegio mínimo. Restrinja y limite la exposición otorgando a los usuarios finales acceso o privilegios suficientes para realizar una tarea o ejecutar una aplicación. Deshabilite los protocolos y programas (e inclusive complementos) innecesarios y desactualizados que de otra manera pueden dar a los atacantes puntos de entrada en sus sistemas.

Pr

Mantener la red y los servidores no solo es un consejo, es una necesidad estricta y sentida; esto porque el ransomware y en general este tipo de amenazas, aprovechan las redes infectadas para comunicarse con sus servidores de comando y control.
Los firewalls y los sistemas de detección y prevención de intrusos ayudan a detectar, filtrar y bloquear el tráfico y la actividad de la red. También proporcionan información forense que puede ayudar a detectar intentos de incursión y ataques reales.

Una sola máquina vulnerable es a veces todo lo que se necesita para infectar sistemas y servidores dentro de la red. Mantener los servidores parcheados y actualizados. Fortalezca sus credenciales de escritorio remoto contra ataques de fuerza bruta. Implementar políticas de autenticación y bloqueo de múltiples factores. Utilice canales encriptados para evitar que los atacantes husmeen en sus conexiones remotas.

También hay otros enfoques que puede considerar. La segmentación de la red no solo mitiga la congestión del tráfico local; también mejora la seguridad al asignar solo los recursos específicos para el usuario, lo que disminuye significativamente las formas en que los atacantes se mueven

lateralmente dentro de la red.

La categorización de datos puede lograr lo mismo. La clasificación de los datos no solo hace que el acceso sea más eficiente, sino que también determina su valor dentro de la organización. En última instancia, estas soluciones pueden ayudar a mitigar cualquier daño causado por una violación o un ataque.

Asegure sus puertas de enlace

La puerta de enlace del correo electrónico sigue siendo el principal vector de infección del ransomware . Detén estas amenazas en su camino al frustrar sus tácticas de llegada . Implemente mecanismos de seguridad en niveles contra el ransomware basado en correo electrónico y adopte las mejores prácticas contra los correos electrónicos no deseados diseñados socialmente. La misma discreción debe aplicarse a la puerta de enlace web: emplee la categorización de URL, elimine los complementos de navegador no utilizados y asegúrese de que los componentes de terceros (es decir, Java, Flash) estén actualizados.

Configure su firewall para incluir en la lista blanca solo los puertos y hosts específicos que necesita.

Nota: Como habrán podido notar, muchos de estos consejos son genéricos y aplican por igual para equipos de cómputo, redes y servidores web. Pero en este último caso: Hemos visto a los ciberdelincuentes apuntar con éxito a los servicios de alojamiento web basados en la nube para inyectar código en múltiples dominios web de alto tráfico en lugar de tratar de hacerlo uno a la vez. El multiplicador de fuerzas de atacar un servicio centralizado hace que los proveedores de la nube sean objetivos cada vez más tentadores. La paralización exitosa de un servicio que genera millones de dólares al día para el

proveedor, al mismo tiempo que interrumpe el servicio para potencialmente cientos o miles de empresas y decenas de miles o incluso millones de sus clientes, no solo representaría un día de pago masivo para una organización criminal. También socavaría la frágil confianza que muchas organizaciones ya tienen cuando se trata de la computación basada en la nube, y podría tener un efecto devastador en la transformación digital y nuestra economía digital.

Cuando sabemos que estamos infectados

Lo más obvio y conveniente es apagar y desconectar las máquinas infectadas para que no contamine otras conectadas a la red.

Asegure su perímetro

Hay varios vectores de ataque comunes para Ransomware. El Protocolo de escritorio remoto (RDP) es el más común, seguido del phishing / recolección de credenciales. A través de estos vectores de ataque, el actor de amenaza obtiene credenciales administrativas elevadas. Estas credenciales se usan para apagar los sistemas que detectan el ataque y para acceder a aplicaciones confidenciales como controladores de dominio y sistemas de respaldo. Si nota el ataque antes, puedes expulsar al atacante de su red mientras aún están en el acto.

Cerrar puertos RDP

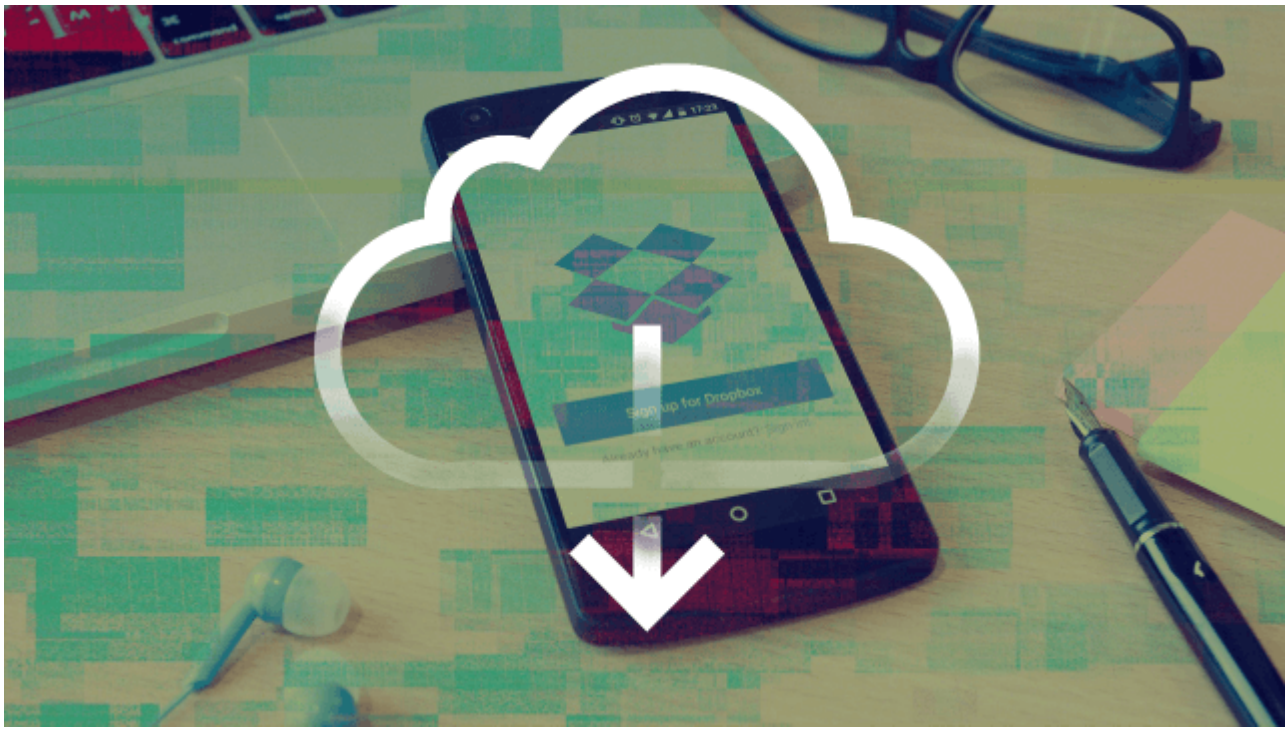
Cierre de inmediato los puertos RDP que están abiertos a Internet, independientemente de cuán seguros pueda creerlos. Tómese un tiempo para revisar los intentos de inicio de sesión y los registros para determinar si este fue el punto de ingreso. Dada la prevalencia de ataques basados en RDP, este paso siempre debe tomarse si se detecta un ransomware.

Cambiar credenciales administrativas

Dada la prevalencia de los kits de explotación de aprovechamiento de credenciales, se debe suponer que las credenciales administrativas actuales se han comprometido o que el atacante creó un nuevo conjunto de credenciales administrativas. De cualquier manera, al finalizar inmediatamente todas las sesiones de administrador iniciadas y restablecer todas las credenciales administrativas puede arrancar rápidamente a un atacante desde su red. Si NO se toma este paso, es muy posible que les permita observar su esfuerzo de recuperación y brindarles la oportunidad de volver a cifrar su red. Expóngalos y asegúrese de que permanezcan fuera, antes de comenzar a restaurar los sistemas.

Cambiar credenciales de usuario

Las credenciales de administrador de dominio normalmente se obtienen de una máquina subordinada de un empleado. Para asegurarse de que las credenciales de los usuarios no se reutilicen y se otorgue el mismo estado elevado unas horas más tarde, fuerce un cambio de contraseña en toda su base de usuarios.



Restaurar desde copias de seguridad en segundo lugar

Priorice la limitación del acceso a su red sobre la restauración desde sus copias de seguridad. Un escenario muy común en los ataques de ransomware implica un apuro por restaurar desde copias de seguridad. Si el acceso del atacante a la red no se excluye primero, también cifrarán la restauración. También es probable que en el proceso de restauración, observen la ubicación de una copia de seguridad previamente bien particionada. Luego, cifrarán o borrarán esa copia de seguridad para que la restauración ya no sea una opción. Esta es la razón por la que el acceso seguro tiene prioridad sobre el inicio de una restauración, independientemente de cuánto tiempo llevará. Una vez que se haya bloqueado el acceso, verifique sus copias de seguridad y asegúrese de que no se hayan visto afectadas. Con suerte, al menos una de sus copias de seguridad está disponible. Es una buena idea escanear la copia de seguridad con su punto de acceso / punto final para asegurarse de que no haya malware al acecho.

Una vez que esté seguro de que el acceso no autorizado a sus sistemas críticos es imposible, debe comenzar el proceso de evaluación del alcance y la omnipresencia del ataque y determinar cómo ejecutar su proceso de recuperación de desastres.

Recoger evidencia de ransomware

Si es posible, tome una foto con su teléfono móvil de lo que observó. Una imagen de la nota de rescate, o una imagen de un archivo cifrado puede ayudar en gran medida a diagnosticar lo que ha sucedido sin tener que volver a conectar o reiniciar una máquina afectada.

Después de la emergencia, la recuperación

Ahora que se ha neutralizado la amenaza inmediata, se puede realizar una evaluación completa de las máquinas impactadas y la operabilidad de la empresa. Las víctimas de ransomware pueden usar utilidades gratuitas como No More Ransom o ID Ransomware para determinar el tipo de ransomware que las ha afectado. También recomendamos encarecidamente a todas las víctimas de ransomware que informen el incidente a la policía .

Esperamos que este manual complemente lo que hemos expuesto previamente en nuestros blogs al respecto y cada vez seamos una comunidad no solo bien informada sino proactiva frente a este tipo de amenzas.

Consultar también: Ransomware en Windows server, características y patrones de ataque, qué hacer; ¿Porqué aumentan los ataques de ransomware a las empresas?; Backups y la restauración bare metal