Ransomware en Windows server, características y patrones de ataque, qué hacer

Ransomware en Windows server, características y patrones de ataque, qué hacer.En el mes de abril 2019 una conocida empresa de hosting en los Estados Unidos estuvo sometido a un intenso ataque de Ransomware en sus servidores Windows. Miles de sus clientes han estado offline más de una semana, con pérdidas millonarias no solo para la compañía de alojamiento web sino para los clientes o usuarios finales, que han visto como su esfuerzo no solo de generar contenido sino que, todos sus contenidos, páginas web y bases de datos han sido secuestrados y encriptados, pidiendose recompensa por recuperar su propia información. Se dice que el Ransomware involucrado es GlobeImposter (de la cual hay muchas variantes y que suele tomar control de las máquinas donde se abre, generalmente en un adjunto en un correo electrónico), que se instala a través de RDP (protocolo de escritorio remoto, un vector de ataque por fuerza bruta) , también puede ser la razón por la cual el proveedor de hosting ha deshabilitado el **acceso RDP** a sus servidores después del ataque. Una vez que un atacante obtiene acceso administrativo a través de un ataque de fuerza bruta en un puerto RDP vulnerable, el sistema se ve comprometido y puede introducir malware y / o usar herramientas de acceso remoto para hacer casi cualquier cosa.

La gente de TI (Tecnología de la Información) debería cerrar RDP si no lo usan. Si deben usar RDP, la mejor forma de protegerlo es mediante una lista blanca de IP en un **firewall** o no exponerla a Internet. Coloque RDP detrás de un firewall, solo permita RDP desde el tráfico local, configure una **VPN** al firewall, use una puerta de enlace RDP , cambie el puerto RDP predeterminado (TCP 3389) e imponer políticas de contraseñas seguras , especialmente en cualquier cuenta de administrador o con privilegios de RDP.
Ahora bien, esto no quiere decir que este sea el único puerto que podría verse vulnerado en un momento dado, solo se usa como ejemplo en un momento dado.

El problema inicial es la pérdida de información por supuesto que si, pero lo alarmante es que a pesar de suceder con tanta regularidad este tipo de intrusiones, los webmasters y dueños de sitios web no implementen de forma preventiva una política de backups o copias de seguridad. Es como los seguros de vida, es importante adquirirlos cuando se está vivo, cuando no se necesitan y no esperar a situaciones extremas para adoptarlos.
Reconstruir sitios web cuando no se cuenta con copias de seguridad recientes es una labor casi que imposible. ¿Cuánto

dinero está dispuesto a perder para decidirse a tomar medidas preventivas básicas como un Almacenamiento o backup remoto ?

A nivel de prevención, ¿qué podemos hacer?

Lista de verificación de endurecimiento de Windows Server

Históricamente, los esfuerzos de prevención de ransomware se enfocaban donde las infecciones casi siempre se originaban : dispositivos de punto final. Pero esta estrategia puede ser inadecuada para proteger los recursos de Windows Server. La mejor manera de bloquear el ransomware es practicar la defensa en profundidad y envolver a la organización en múltiples capas de protección.
Primero, equipe los puntos finales de la red con software **antimalware** de calidad y bien mantenido . Si bien es una buena medida preventiva, la mayoría del software antimalware se basa en firmas de malware. El nuevo malware sale a una velocidad constante, lo que hace que no sea realista depender del software antimalware basado en firmas para obtener una protección completa contra el ransomware.

A continuación, los administradores deben bloquear el uso de aplicaciones no autorizadas, scripts y archivos ejecutables en dispositivos de punto final a través de una política de restricción de software a través de la Política de grupo o Device Guard . Las herramientas de terceros pueden incluir en la lista blanca las aplicaciones autorizadas y evitar que se ejecuten otras.

Por último, ejecute la gestión integral de parches con puntos finales. Mantener el sistema operativo y las aplicaciones parcheadas evita que el malware explote fallas de seguridad.

Bloquear el servidor de Windows

Los administradores normalmente no usan navegadores web o clientes de correo en servidores de red, lo que ayuda a prevenir el ransomware. Pero si un punto final de la red sucumbe al malware, existe la posibilidad de que los contenidos del servidor también puedan ser vulnerables.

De alguna manera, los administradores deben proteger los sistemas de Windows Server contra ransomware con las mismas técnicas que se usan para proteger las estaciones de trabajo. Mantenga el sistema operativo Windows Server actualizado con parches y configure un software antimalware y una lista blanca de aplicaciones para el servidor. Las opciones pueden estar limitadas por el tipo de implementación del servidor. Por ejemplo, puede que no sea posible ejecutar estos esquemas de protección en Nano Server, la versión minimalista de Microsoft de su sistema operativo Windows Server 2016.

Ajustar privilegios de usuario

Windows Server es vulnerable al ransomware a través de archivos compartidos . Si el dispositivo de un usuario se

infecta con ransomware, puede cifrar los datos en el dispositivo del usuario y usar los permisos para cifrar el contenido de cualquier unidad del servidor de archivos asignada a ese dispositivo.

Los administradores pueden evitar que el ransomware acceda a los archivos en los servidores de la red al evitar el uso de los servidores de archivos tradicionales. Por ejemplo, almacene archivos dentro de una biblioteca de documentos de SharePoint para ofrecer un grado adicional de protección, siempre y cuando los puntos finales de la red no tengan una unidad asignada a la biblioteca.

Pero esta estrategia no siempre es práctica y no garantiza la protección. Como práctica recomendada, restrinja a los usuarios para que solo tengan acceso a los datos que necesitan. Un límite en el acceso del usuario compartimenta el daño de una infección de ransomware; Si el usuario no puede acceder a los datos, tampoco el ransomware.

Implementar protección continua de datos

En caso de un brote de ransomware, el personal de TI necesita una forma de recuperar datos cifrados.

Los productos de protección continua de datos realizan copias de seguridad de los datos a nivel de bloque de forma continua a medida que se modifican los datos. Si el ransomware cifra el contenido de un servidor de archivos, el sistema continuo de protección de datos interpretará el cifrado malicioso como una modificación de archivo y escribirá los bloques de almacenamiento modificados para hacer una copia de seguridad. Sin embargo, el software de protección también facilita que un administrador pueda revertir los cambios y deshacer el daño causado por la infección.

Varios tips adicionales

- Tener un sistema operativo actualizado, preferiblemente 2016 o 2019, parcheado, al día en todos sus complementos.
- Los parches de seguridad del sistema operativo y de los servicios de aplicación deben instalarse de manera conveniente (por ejemplo, 30 días) y de manera consistente con los procedimientos de administración de cambios.
- Los productos que ya no reciben actualizaciones de seguridad del proveedor (por ejemplo, no compatible) no están autorizados.
- Habilitar la notificación automática de nuevos parches si es posible.Instale los últimos paquetes de servicio y revisiones de Microsoft.
- Los administradores del sistema deben establecer y seguir un procedimiento para realizar copias de seguridad periódicas del sistema.
- Las copias de seguridad deben verificarse al menos una vez al mes, ya sea a través de la verificación automatizada, a través de restauraciones de clientes o a través de restauraciones de prueba.
- Los administradores de sistemas deben mantener procedimientos de restauración documentados para los sistemas y los datos de esos sistemas.
- Los medios de copia de seguridad deben estar protegidos del acceso físico no autorizado. Si el medio de copia de seguridad se almacena fuera del sitio, debe estar cifrado o debe tener un proceso documentado para evitar el acceso no autorizado.
- Los sistemas deben configurarse en un entorno de red protegido o mediante un método que garantice que no se pueda acceder al sistema a través de una red potencialmente hostil hasta que esté protegido.
- Los servicios, las aplicaciones y las cuentas de usuario

que no se utilizan deben deshabilitarse o desinstalarse.
- Limite las conexiones a los servicios únicamente a los usuarios autorizados del servicio.
- Los servicios o aplicaciones que se ejecutan en sistemas que manipulan datos confidenciales deben implementar comunicaciones cifradas según lo requieran las necesidades de confidencialidad e integridad.
- (Política de cuentas de usuario)Use contraseñas seguras. Establecer la longitud mínima de la contraseña. Habilitar los requisitos de complejidad de contraseña.
- No almacene contraseñas utilizando cifrado reversible. (Defecto).
- Configurar la política de bloqueo de cuenta.
- Use Windows defender para su versión de Windows server, claro, actualizado.
- Disponga de un firewall por software o por hardware y configúrelo debidamente.
- Verifique que tenga opción de bloqueos por ip.
- Haga el esfuerzo de tener un WAF (pregunte a nuestros asesores por uno)
- Emplee un proxy (nuestra asistencia técnica premium, de pago por horas, puede instalarle uno)
- Cambiar puerto RDP, para prevenir la mayoría de ataques de malware mal escrito.
- Mejorar el nivel de cifrado con TLS
- Otro pequeño truco útil es el nivel de cifrado de la sesión RDP y la implementación forzada de TLS (Seguridad de la capa de transporte). Nivel de seguridad medio o alto inclusive.
- Nivel de cifrado, 3 por lo menos.

Hace unas semanas también Norsk Hydro, uno de los mayores productores de aluminio del mundo, fue infectado por una variedad de de ransomware LockerGoga. Y para que no se crea que esto solo le sucede a empresas comunes y corrientes, La firma de seguridad cibernética Verint también fue golpeada por ransomware en Abril 2019.

Consultar también: Plesk Onyx: SEO, Inteligencia artificial en WordPress, Rendimiento y Seguridad; puede el certificado SSL prevenir ataques XSS