¿Ransomware puede afectar a servidores web Linux ?

¿Ransomware puede afectar a servidores web Linux ? Por supuesto que sí, el sistema operativo solo cambia la forma pero no el fondo del ataque.
Linux es un sistema operativo de código abierto que es muy versátil debido al gran grupo de voluntarios que mantienen y actualizan el popular sistema operativo de código abierto.

Existe una amplia gama de distribuciones de Linux dirigidas a diferentes propósitos y preferencias. Algunos están diseñados para tareas específicas, como la protección de la privacidad o la defensa del perímetro, y hay una gran cantidad de opciones disponibles para los sistemas operativos de escritorio y servidor.

La realidad

Linux ha existido durante décadas, pero solo reclama el 2,36% de la cuota de mercado del sistema operativo de escritorio. Linux es mucho más popular en el back-end, ya que reside en aproximadamente el 11% de los servidores y el 35% de los servidores web.
Algunas formas de malware se van lanza en ristre contra sitios web en Html, Php, cifrando sus contenidos y pidiendo rescate por recuperarlos.
Otras se especializan en «darle duro» al Cpanel, Magento, Mysql, Drupal, WordPress.

IPMI

Hace poco tiempo se descubrió que los dispositivos IPMI mal configurados. Para los no iniciados, IPMI es una interfaz de

administración que está integrada en las placas madre del servidor o en tarjetas complementarias que proporcionan capacidades de administración y monitoreo que son independientes de la CPU, el firmware y el sistema operativo del sistema. Con él, los administradores pueden administrar un servidor de forma remota para hacer cosas como encenderlo y apagarlo, monitorear la información del sistema, acceder a KVM y más. Si bien esto es útil para administrar servidores fuera de las instalaciones en centros de datos de colocación y similares, también ofrece una apertura para los atacantes si no está correctamente bloqueado.

La buena noticia es que protegerse contra tales ataques debería ser bastante sencillo, comenzando por asegurarse de que la contraseña de IPMI no sea la predeterminada. Además, las listas de control de acceso (ACL) deben configurarse para especificar las direcciones IP que tienen acceso a la interfaz IPMI, y también para configurar IPMI para escuchar solo en direcciones IP internas, lo que limitaría el acceso a los administradores dentro del sistema de la organización.

Otras pautas

Para los servidores Linux, podría ser una buena idea proteger con contraseña el gestor de arranque GRUB. Después de obtener acceso a los servidores Linux, los atacantes han estado reiniciando en modo de usuario único para obtener acceso de root antes de descargar la carga útil malintencionada. Como mínimo, la protección con contraseña de GRUB dificultaría los reinicios.

El punto de acceso, generalmente, se remonta a errores de configuración del servidor o al ejecutar versiones obsoletas de software con vulnerabilidades conocidas de ejecución remota de código.
No asuma que pagar el rescate le permitirá descifrar sus datos. No hay garantía de que el autor del ransomware cumpla

su parte del trato.Téngalo muy en cuenta si está implicado en este tipo de situaciones con criptovirus.

La forma más activa de evitar que las variantes de ransomware ingresen a su servidor Linux es cerrar los puertos SSH (shell seguro) y FTP (protocolo de transferencia de archivos) según los expertos.
Estos son dos de los enfoques principales … estos piratas informáticos parecen estar apuntando a ejecutar los scripts de cifrado. El ransomware parece usar un algoritmo base64 que convierte los caracteres en bits, lo que crea un proceso de descifrado extremadamente difícil para recuperar el control.
También es posible que estos ataques se envíen a través de vulnerabilidades básicas de CMS (sistema de administración de contenido). Si los usuarios de Linux utilizan un CMS para administrar el contenido de su sitio web, es posible que esto sirva como una vulnerabilidad en el marco de seguridad del sistema.
Es más común que los cibercriminales encuentren exposiciones en estas aplicaciones aparentemente seguras, lo que les permite realizar cambios drásticos en la configuración de seguridad y permisos de la red.
La mayoría de los sitios web se implementan utilizando un sistema de control de versión de origen que puede volver a implementar una versión limpia del sitio web en poco tiempo.
El único daño potencialmente permanente es en cualquier base de datos del sistema de administración de contenido si se utiliza y no se respalda.

Estos son dos de los enfoques principales … estos piratas informáticos parecen estar apuntando a ejecutar los scripts de cifrado. El ransomware parece usar un algoritmo base64 que convierte los caracteres en bits.

Lo clásico

Para minimizar las posibilidades de acabar infectado por un malware, los procesos a seguir en Linux no varían mucho de los que tendríamos que seguir en Windows:

- Mantener el sistema actualizado para obtener los últimos parches y correcciones a nivel de seguridad.
- Minimizar al máximo la utilización de repositorios de terceros o de fuentes desconocidas, ya que estos pueden contener vulnerabilidades que podrían ser explotadas por los ciberdelincuentes.
- Aplicar siempre los mínimos privilegios necesarios para evitar la exposición de datos a posibles daños y los posibles accesos no autorizados.
- Cambiar las contraseñas administrativas y adoptar unas fuertes y seguras.
- Supervisar y validar de forma activa el tráfico de la red para protegerse de amenazas y detectar el tráfico malicioso.
- Se recomienda el uso de firewalls y otros mecanismos de prevención y detección de intrusiones.
  Realizar copias de seguridad de los datos. Algo simple y que resulta una perogrullada, pero tener una copia de seguridad siempre ayuda a minimizar los daños provocados por un malware (o incluso una avería), más si los datos son irrecuperables tras el incidente.
- Segmentar la red y categorizar los datos.
- Audite la pila de software para detectar vulnerabilidades conocidas que podrían haber permitido la entrada del atacante, y parche según corresponda
- Audite la configuración del sitio para detectar cualquier punto débil

- Deshabilite los servicios que no son críticos y cierre los puertos abiertos;Asegúrese de que las copias de seguridad estén operativas; y
- Realice una prueba de penetración de la huella de la red orientada a Internet.

La mejor manera de estar preparado es asumir que será violado, y luego tomar medidas para asegurar sus servidores y estaciones de trabajo en consecuencia.
Suponga que un atacante está en su red y tiene el control de una estación de trabajo. Luego decida qué datos o recursos de TI querrán robar o cifrar. Luego, tome las medidas adicionales para asegurar esos recursos.

La principal prioridad es encontrar sus datos confidenciales, dicen los expertos. Estos incluyen datos de pacientes, información de clientes y registros financieros. Asegúrese de que estén asegurados y accesibles solo por empleados aprobados. Supervise esos recursos para detectar comportamientos inusuales de archivos, como copias masivas, borrados o cifrado de archivos. Asegúrese de tener un plan de emergencia para reaccionar en minutos.
Estos pasos no evitarán un ataque, la verdad, pero podrían significar la diferencia entre un incidente de seguridad y una violación en toda regla.

Consultar también: Ransomware en Windows server, características y patrones de ataque, qué hacer; OJO TAMBIÉN POST ANTERIOR EN BORRADOR.