10 maneras de proteger su Active Directory

junio 8, 2022
by SentinelOne

Active Directory (AD) es un objetivo de alto valor para los ciberdelincuentes, que a menudo intentan comprometerlo para escalar sus privilegios y ampliar su acceso. Desafortunadamente, AD es tan necesario desde el punto de vista operativo que debe garantizarse el acceso a todos los usuarios de una empresa, y eso complica enormemente su protección. La gravedad del problema queda patente si pensamos que Microsoft afirma que más de 95 millones de cuentas de AD reciben ataques a diario.

Si bien la protección de AD no es fácil, en absoluto se puede decir que sea imposible. Solo hacen faltan las herramientas y tácticas adecuadas. A continuación se incluyen diez consejos que pueden ayudar a las empresas a proteger de manera más eficaz su despliegue de Active Directory frente a algunas de las tácticas de ataques más frecuentes.

1. Prevenga y detecte la enumeración: privilegios, administrador delegado, cuentas de servicios y sesiones de red

Una vez que el ciberdelincuente ha conseguido atravesar las defensas perimetrales y establecerse dentro de la red, llevará a cabo una labor de reconocimiento para identificar recursos potencialmente valiosos y averiguar la manera de apoderarse de ellos. Y una de las mejores formas de hacerlo es a través de AD, ya que pueden disfrazar sus acciones como actividades de trabajo normales y, por tanto, con pocas posibilidades de ser detectados.

La capacidad de detectar y prevenir enumeraciones de privilegios, administradores delegados y cuentas de servicio puede alertar a los responsables de la defensa de la presencia de un ciberdelincuente en una etapa temprana del ciclo de ataque. Desplegar cuentas y credenciales de dominio engañosas en los endpoints también puede confundir a los ciberdelincuentes y permitir a los defensores redirigirlos a señuelos para neutralizarlos.

2. Identifique y corrija las exposiciones de cuentas con privilegios

Los usuarios suelen almacenar credenciales en sus estaciones de trabajo. En ocasiones lo hacen de manera accidental, otras voluntariamente, y generalmente por comodidad. Los ciberdelincuentes lo saben y hacen todo lo posible por apoderarse de esas credenciales almacenadas para conseguir acceder al entorno de red. Un conjunto de credenciales adecuado puede ser extremadamente útil, y los intrusos intentarán siempre escalar sus privilegios y ampliar el acceso.

Las empresas pueden complicar el acceso a la red a los ciberdelincuentes si consiguen identificar las exposiciones de cuentas con privilegios, corregir los errores de configuración y eliminar las credenciales guardadas, las carpetas compartidas y otras vulnerabilidades.

3. Proteja y detecte los ataques de tipo «Golden Ticket» y «Siver Ticket»

Los ataques Pass-the-Ticket (PTT) se encuentran entre las técnicas más eficaces que utilizan los ciberdelincuentes para desplazarse lateralmente por la red y escalar sus privilegios. La estrategia de diseño sin estado de Kerberos facilita el uso ilegítimo, lo que significa que los ciberdelincuentes pueden falsificar fácilmente los vales de autenticación dentro del sistema. «Golden Ticket» y «Silver Ticket» son dos de los tipos de ataques PTT más graves que emplean los ciberdelincuentes para conseguir comprometer dominios y establecer persistencia de dominios.

Para hacer frente a este problema es necesario poder detectar vales de concesión de vales y cuentas de servicios de ordenador de Kerberos vulnerables, que identifiquen y alerten sobre errores de configuración que pudieran dar lugar a ataques PTT. Además, una solución como Singularity Identity puede impedir el uso de vales falsificados en los endpoints.

4. Proteja contra los ataques Kerberoasting, DCSync y DCShadow

Un ataque «Kerberoasting» es una manera sencilla de conseguir acceso con privilegios para los ciberdelincuentes, mientras que los ataques DCSync y DCShadow están centrados en mantener persistencia de dominios dentro de una empresa.

Los defensores necesitan la capacidad de realizar una evaluación permanente de AD que ofrezca análisis en tiempo real de los ataques contra AD y además alerte de los errores de configuración que facilitan estos ataques. Además, una solución que pueda aprovechar la presencia en el endpoint para impedir que los ciberdelincuentes descubran cuentas susceptibles de ataque puede complicar su capacidad para llevar a cabo estas intrusiones.

5. Impida la recopilación de credenciales desde recursos compartidos de dominios

Los ciberdelincuentes suelen buscar contraseñas de texto simple o con cifrado reversible almacenadas en scripts, o archivos de directivas de grupo almacenadas en recursos compartidos de dominios como Sysvol o Netlogon.

Una solución como Ranger AD puede ayudar a detectar estas contraseñas y permitir a los encargados de la defensa corregir las vulnerabilidades antes de que los ciberdelincuentes puedan aprovecharlas. Mecanismos como los que emplea la solución Singularity Identity también pueden desplegar objetos de grupos de directivas Sysvol engañosos en el AD de producción, contribuyendo de esta forma a perturbar la acción del atacante al alejarlo de los activos de producción.

6. Identifique las cuentas con SID con privilegios ocultos

Gracias a la técnica de inyección de identificadores de seguridad (SID) de Windows, los ciberdelincuentes pueden aprovechar el atributo «historial» de SID, y desplazarse lateralmente dentro del entorno de AD y conseguir escalar todavía más sus privilegios.

Para impedirlo es necesario detectar conjuntos de cuentas con valores de SID con privilegios bien conocidas en los informes y el atributo historial de SID.

7. Detecte la delegación de derechos de acceso peligrosos en objetos críticos

La delegación es una función de AD que permite a una cuenta de usuario o de ordenador suplantar otra cuenta. Por ejemplo, cuando un usuario llama a una aplicación web alojada en un servidor web, la aplicación puede imitar las credenciales del usuario para acceder a recursos alojados en un servidor distinto. Cualquier ordenador del dominio con delegación sin restricciones habilitada puede suplantar las credenciales de usuario en cualquier otro servicio del dominio. Desafortunadamente, los ciberdelincuentes pueden aprovecharse de esta función para conseguir acceder a distintas áreas de la red.

La supervisión permanente de vulnerabilidades de AD y las exposiciones de delegación pueden ayudar a los defensores a identificar y corregir estas vulnerabilidades antes de que los ciberdelincuentes puedan aprovecharse de ellas.

8. Identifique las cuentas con privilegios con la delegación habilitada

Hablando de delegación, las cuentas con privilegios configuradas con delegación sin restricciones pueden dar lugar directamente a ataques de Kerberoasting y de Silver Ticket. Las empresas necesitan poder detectar e informar sobre las cuentas con privilegios con delegación habilitada.

Una lista completa de cuentas de usuarios con privilegios, de administradores delegados y de servicios pueden ayudar a los encargados de la defensa a evaluar las vulnerabilidades potenciales. En este caso, la delegación no es directamente algo negativo. A menudo es necesaria por razones operativas, pero los defensores pueden utilizar una herramienta como Singularity Identity para evitar que los ciberdelincuentes descubran esas cuentas.

9. Identifique los usuarios sin privilegios en ACL AdminSDHolder

Los servicios Active Directory Domain Services (AD DS) utilizan el objeto AdminSDHolder y el proceso de propagador de descriptores de seguridad (SDProp) para proteger a usuarios y grupos con privilegios. El objeto AdminSDHolder tiene una lista de control de acceso (ACL) exclusiva, que controla los permisos de las entidades de seguridad que son miembros de grupos de AD con privilegios integrados. Para hacer posible el desplazamiento lateral, los ciberdelincuentes pueden añadir cuentas al objeto AdminSDHolder, lo que les otorga el mismo acceso con privilegios que otras cuentas protegidas.

Las empresas pueden prevenir esta actividad con una herramienta como Ranger AD, que permite detectar y alertar sobre la presencia de cuentas poco habituales dentro de la lista de control de acceso AdminSDHolder.

10. Identifique los cambios recientes en la directiva predeterminada de dominio o la directiva predeterminada de controladores de dominio

En AD, las empresas utilizan directivas de grupo para administrar varias configuraciones funcionales mediante la definición de ajustes de seguridad específicos para el entorno. A menudo consiste en configurar grupos administrativos e incluye scripts de inicio y de apagado. Los administradores estos grupos para establecer requisitos de seguridad definidos por la empresa en cada nivel, instalar software y definir permitidos de archivos y de registro Desafortunadamente, los ciberdelincuentes pueden cambiar estas directivas para conseguir persistencia de dominios dentro la red.

Supervisar los cambios en las directivas predeterminadas de grupo puede ayudar a los defensores a detectar rápidamente a los ciberdelincuentes, reducir los riesgos de seguridad y contribuir a impedir el acceso con privilegios a AD.

Despliegue de las herramientas adecuadas

Conocer las tácticas más comunes que utilizan los ciberdelincuentes para atacar AD puede ayudar a las empresas en sus esfuerzos de protección. Cuando desarrollamos herramientas como Ranger AD y Singularity Identity, tuvimos en cuenta muchos vectores de ataque e identificamos la mejor forma de detectarlos y neutralizarlos.

Con estas herramientas, las empresas actuales pueden identificar eficazmente las vulnerabilidades, detectar de forma temprana la actividad maliciosa y corregir los incidentes de seguridad antes de que los intrusos puedan escalar sus privilegios y convertir un ataque a pequeña escala en una importante violación de la seguridad. Aunque no resulta sencillo proteger AD, gracias a las herramientas específicas de protección disponibles, no es un reto insuperable.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- Protección de Active Directory | Qué es y qué necesita saber