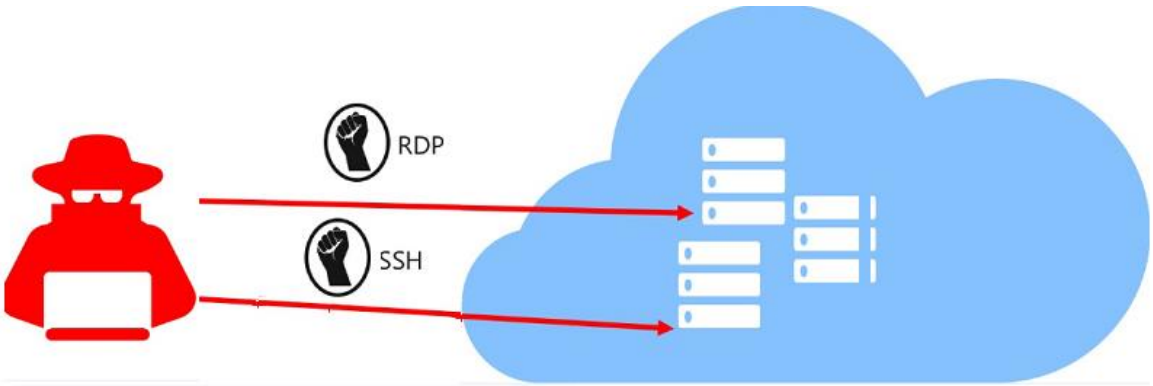
Escenario de ataque

El destino es la fuerza bruta. El hacker persigue a usuarios específicos y pasa por tantas contraseñas como sea posible mediante un diccionario completo o uno que se edite para contraseñas comunes. Un ataque de averiguación de contraseñas aún más específico se produce cuando el hacker selecciona a una persona y realiza investigaciones para determinar si puede adivinar la contraseña del usuario; por ejemplo, intenta detectar nombres de familia a través de publicaciones en redes sociales. Y, a continuación, prueba esas variantes en una cuenta para obtener acceso a ella.

Normalmente, los ataques por fuerza bruta tienen como destino los puertos de administración para obtener acceso a una máquina virtual. Si un atacante tiene éxito, puede tomar el control de la máquina virtual y establecer un punto de apoyo en su entorno. Los equipos con el Protocolo de escritorio remoto (RDP) de Windows expuestos a Internet son un objetivo atractivo para los adversarios porque presentan una manera sencilla y eficaz de obtener acceso a una red. Atacar por fuerza bruta un RDP, un protocolo de comunicaciones de red seguro que proporciona acceso remoto a través del puerto 3389, no requiere un alto nivel de experiencia ni el uso de vulnerabilidades de seguridad. Los atacantes pueden usar muchas herramientas estándar para examinar Internet en busca de posibles víctimas y aprovechar herramientas similares para llevar a cabo el ataque por fuerza bruta.

Los atacantes tienen como destino servidores RDP que usan contraseñas débiles y que no tienen autenticación multifactor, redes privadas virtuales (VPN) ni otras protecciones de seguridad. A través de la fuerza bruta de RDP, los grupos de actores de amenazas pueden obtener acceso a las máquinas de destino y realizar muchas actividades de seguimiento, como ransomware y operaciones de minería de monedas.

En un ataque por fuerza bruta, los adversarios intentan iniciar sesión en una cuenta mediante uno o varios métodos de prueba y error. Muchos inicios de sesión con errores que se producen a lo largo de frecuencias de tiempo muy cortas, normalmente minutos o incluso segundos, suelen asociarse a estos ataques. Un ataque por fuerza bruta también puede implicar que los adversarios intenten acceder a una o varias cuentas mediante nombres de usuario válidos obtenidos del robo de credenciales o el uso de nombres de usuario comunes como "administrador". Lo mismo se mantiene para las combinaciones de contraseñas.



Una manera de reducir el riesgo de sufrir un ataque por fuerza bruta consiste en limitar el tiempo que está abierto un puerto. No es necesario que los puertos de administración estén abiertos en todo momento. Solo deben estar abiertos mientras se está conectado a la máquina virtual, por ejemplo, para realizar tareas de administración o mantenimiento. Cuando se habilita Just-In-Time, Security Center usa las reglas del grupo de seguridad de red (NSG) y Azure Firewall, que restringen el acceso a los puertos de administración para que no puedan ser objeto de ataques.

Microsoft Defender para la nube aprovecha el gráfico de seguridad inteligente de Microsoft para detectar ataques y actuar contra ellos. El gráfico combina la inteligencia cibernética que Microsoft recopila en todos sus servicios junto con los datos del sector para bloquear patrones de ataque conocidos. Microsoft también proporciona el control que necesita para priorizar las alertas y los incidentes que son importantes para su organización. Además, le ofrecemos una visión unificada para el análisis forense y la capacidad de buscar en todos los recursos del equipo. La inteligencia de amenazas se puede visualizar para las técnicas de ataque de tendencia y las regiones geográficas afectadas.

Indicaciones de un ataque

- Recuentos extremos de inicios de sesión con errores de muchos nombres de usuario desconocidos
- Nunca se ha autenticado de forma correcta previamente desde varias conexiones RDP o desde nuevas direcciones IP de origen

Procedimientos para mitigar los ataques de fuerza bruta

- Deshabilitado de la dirección IP pública: uso de un host bastión
- Uso de una VPN de punto a sitio, una VPN de sitio a sitio o Azure ExpressRoute
- Requerir la autenticación en dos fases.
- Uso de contraseñas complejas
- Limitación de la cantidad de tiempo durante el que están abiertos los puertos

---