cpl.thalesgroup.com

THALES
Building a future we can all trust

Cómo los ataques de ransomware se aprovechan de los RDP desprotegidos y qué puede hacer al respecto

Los ataques de ransomware dirigidos a empresas en una variedad de sectores se han disparado durante la primera mitad de 2022. Los delincuentes se están aprovechando de nuestra dependencia de las comunicaciones digitales y el trabajo remoto para fines siniestros. Como resultado, la mayoría de los incidentes de ransomware se pueden atribuir a una cantidad limitada de vectores de intrusión, donde los tres principales son los puntos de conexión del protocolo de escritorio remoto (RDP) mal protegidos, el phishing de correo electrónico y la explotación de las vulnerabilidades de las redes privadas virtuales (VPN) de día cero.

Los informes de Coveware, Emsisoft y Recorded Future destacan que "el RDP se considera el principal vector de ataque de ransomware" y la fuente de la mayoría de los incidentes de ransomware en 2020". Algunos podrían pensar que el RDP es el principal vector de intrusión para ransomware debido a las configuraciones actuales de trabajo desde casa. Sin embargo, esto no es correcto. El RDP ha estado entre los principales vectores de intrusión desde el año pasado, cuando los atacantes de ransomware dejaron de apuntar a los consumidores y, en su lugar, apuntaron a las empresas y la infraestructura crítica.

¿Cuál es la causa subyacente?

El RDP es la tecnología más popular para conectarse a sistemas remotos y, generalmente, se considera una herramienta segura cuando se usa dentro de una red privada. Sin embargo, cuando los puertos del RDP se dejan abiertos en Internet y es posible acceder a ellos con contraseñas simples, son capaces de causar serios problemas de seguridad. Las contraseñas se pueden comprometer fácilmente, allanando el camino para el acceso malicioso y no autorizado a las redes corporativas a través de RDP desprotegidos. El acceso no autorizado a través de los RDP les permite a los atacantes obtener acceso a los servidores corporativos y actuar como plataforma de lanzamiento para los ataques de ransomware.

Hay millones de computadoras con sus puertos RDP expuestos en línea sin ninguna protección, lo que convierte al RDP en un gran vector de ataque para todo tipo de actividades cibernéticas maliciosas y, cada vez más, para los ataques de ransomware. Los delincuentes que buscan explotar estos puntos de acceso pueden encontrarlos de forma gratuita en los "mercados RDP". A partir de ahí, su trabajo se desarrolla como siempre. Buscan contraseñas débiles aprovechando técnicas bien conocidas como la fuerza bruta o la ingeniería social. Una vez que el atacante ha obtenido acceso al sistema objetivo, se enfoca en hacer que la red sea lo más insegura posible.

Una vez que los sistemas de seguridad han sido deshabilitados y la red queda desprotegida, los delincuentes son libres de entregar su paquete malicioso. Esto puede ser cualquier cosa, desde instalar ransomware, implementar registradores de claves, usar máquinas comprometidas para distribuir spam, robar datos confidenciales o instalar puertas traseras para futuros ataques.

Mejores prácticas para mitigar los ataques a los RDP

Como se mencionó anteriormente, los RDP son puntos de acceso para ingresar a las redes corporativas y no deben verse en Internet ni publicarse sin protección. La publicación de escritorios remotos para la comodidad del usuario no justifica el aumento de amenazas a las que están expuestas las organizaciones.

Para las organizaciones que requieren RDP, las siguientes prácticas recomendadas se centran en fortalecer el punto de acceso y son útiles para proteger a los RDP contra ataques de fuerza bruta.

- Como regla general, no publique escritorios remotos desprotegidos en Internet. Si esto es una necesidad absoluta, asegúrese de que el punto de acceso al RDP esté protegido con autenticación de múltiples factores (MFA) para garantizar que solo los usuarios validados puedan ingresar al RDP.
- Utilice puertas de enlace del RDP. Los escritorios remotos deben protegerse detrás de puertas de enlace de proxy inverso para ocultar el puerto RDP estándar 3389. Se accede a las puertas de enlace del RDP a través de conexiones HTTPS (puerto 443) protegidas a través del protocolo de cifrado TLS.
- Aplique la MFA para acceder a la puerta de enlace del RDP. Incluso las contraseñas más seguras pueden verse comprometidas. Si bien no es una panacea, la MFA ofrece una capa adicional de protección al requerir que los usuarios proporcionen al menos dos formas de autenticación para iniciar sesión en una sesión de RDP.
- Aplique la MFA al inicio de sesión de la red. Una vez dentro del escritorio remoto, implemente otra capa de seguridad aplicando la MFA al punto de inicio de sesión de la red.

La manera como SafeNet Trusted Access de Thales ayuda a mitigar los ataques

SafeNet Trusted Access de Thales puede ayudarlo a proteger su entorno comercial contra ataques de ransomware basados en RDP. SafeNet Trusted Access de Thales les permite a las organizaciones asegurar de manera efectiva el acceso remoto a los RDP y a las puertas de enlace del RDP, así como a las aplicaciones heredadas y en la nube adicionales, independientemente del dispositivo de punto final que se utilice. SafeNet Trusted Access ofrece:

- Compatibilidad con una amplia gama de opciones de autenticación, incluida la autenticación adaptativa e incremental, MFA y tokens basados en hardware.
- Políticas de acceso flexibles para todos los sistemas operativos (Windows/Mac/Linux): esto significa que puede usar un único servicio de administración y autenticación de acceso para proteger las aplicaciones basadas en la nube y todos los escritorios remotos, independientemente del sistema operativo que ejecuten.
- Administre de manera centralizada las aplicaciones en la nube y los inicios de sesión en la red desde un único servicio de administración de acceso/MFA.

Acerca de Thales

Las personas en las que usted confía para proteger su privacidad confían en Thales para proteger sus datos. Cuando se trata de seguridad de datos, las organizaciones se enfrentan a un número cada vez mayor de momentos decisivos. Ya sea que se trate de crear una estrategia informática de cifrado, pasarse a la nube o cumplir con las exigencias en materia de cumplimiento, puede confiar en Thales para proteger sus transformaciones digitales.

Tecnología decisiva para momentos decisivos.

Contáctenos: para conocer todas las ubicaciones de las oficinas y la información de contacto, visite cpl.thalesgroup.com/contact-us