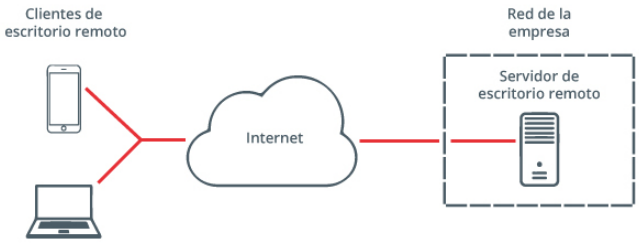
El acceso remoto sigue el modelo lógico de cliente-servidor. El equipo al que queremos acceder hace de «servidor», y el resto de dispositivos que se conecten a él son los «clientes». Cuando se habilita esta funcionalidad se «abre» en el servidor un puerto, que comúnmente es el número 3389. Los puertos pueden entenderse como las vías de entrada y salida de información a Internet. Si una comunicación no se realiza en el puerto correcto, será denegada. Además, habrá que configurar el *router* que da al servidor acceso a Internet, para que acepte las conexiones al escritorio remoto desde fuera de la red interna. Esto último no será necesario si utilizamos una solución VPN para cifrar las comunicaciones entre los equipos cliente y servidor.



Riesgos de utilizar el escritorio remoto

El escritorio remoto de Windows o RDP, además de ser utilizado en el día a día de las empresas, es también uno de los objetivos de los ciberdelincuentes, pudiendo convertirse en un importante riesgo para todas las organizaciones que lo tienen habilitado si no cuenta con las suficientes medidas de seguridad. Es muy frecuente que sea utilizado para infectar con *ransomware*, el *malware* que cifra los archivos y pide un rescate.

¿Cómo atacan RDP los ciberdelincuentes?

Sophos ha publicado recientemente un estudio después de analizar durante un mes los ataques que sufren los servidores RDP accesibles desde Internet. En dicho estudio se utilizaron como señuelos 10 dispositivos (*honeypots*) con RDP habilitado por defecto, ubicados en diferentes zonas geográficas. Estos son algunos datos destacables que se pueden obtener del estudio y que reflejan el interés que presentan este tipo de servicios para los ciberdelincuentes:

- se registraron 4,3 millones de intentos de inicio de sesión fraudulentos en un período de 30 días;
- el primer ataque se produjo tan solo 1 minuto y 20 segundos después de hacer públicos en Internet los *honeypots*;
- todos los *honeypots* fueron atacados una vez transcurridas 15 horas desde su publicación;

- los principales nombres de usuario atacados fueron los que tienen por defecto los sistemas operativos, como administrator, admin, user o ssm-user utilizado en AWS (*Amazon Web Services*);
- fueron atacados tanto usuarios sin privilegios, como administradores;
- la mayoría de ataques centraban su foco en contraseñas débiles.

El estudio muestra que **los ciberdelincuentes utilizan ataques de fuerza bruta**, que consisten en probar múltiples credenciales de acceso, es decir usuario y contraseña, de forma automatizada contra los objetivos. En caso de conseguir acceso, pasan al siguiente objetivo, que generalmente será instalar *malware*.

Además de los ataques de fuerza bruta, otro vector de ataque que pueden utilizar los ciberdelincuentes son las vulnerabilidades descubiertas no parcheadas. El pasado mes de mayo desde Microsoft se publicó un aviso advirtiendo de una vulnerabilidad crítica (CVE-2019-0708), en el escritorio remoto de Windows que afecta a versiones antiguas, aunque todavía muy utilizadas, como Windows 7 o Windows Server 2008, y que permite al atacante instalar *malware* sin que el usuario se percate. Pese a no ser un vector de ataque tan utilizado como la fuerza bruta, estas vulnerabilidades suponen un importante riesgo si no se encuentran debidamente parcheadas.

¿Cuál es el objetivo de los ciberdelincuentes?

Los ciberdelincuentes, una vez que obtienen acceso en el equipo de la víctima, tienen como principal objetivo la instalación de *malware*, pudiendo ser este de varios tipos:

- *Ransomware*, el *malware* que cifra la información y pide un rescate. Este tipo de amenaza ha pasado de propagarse por medio del correo electrónico con ingeniería social, a hacerlo a través de servicios RDP vulnerables.
- *Cryptojacking* que consiste en utilizar los recursos del sistema para minar criptomonedas. El minado de criptomonedas ha desplazado al *ransomware* como amenaza más común y rentable.
- *Malware* que roba información y datos confidenciales, como contraseñas de acceso a otros servicios.
- Infecciones que convierten a tu equipo en un zombi, controlado remotamente por ciberdelincuentes, formando parte de una *botnet.*

¿Por qué lo atacan los ciberdelincuentes?

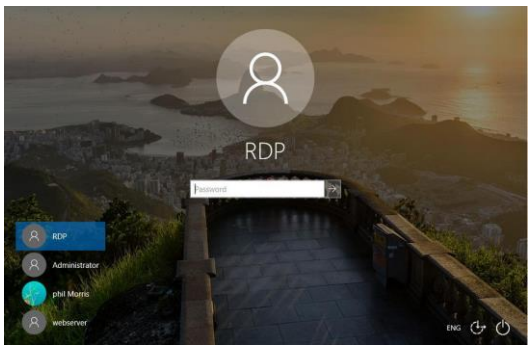
Los ciberdelincuentes tienen su objetivo en este servicio por varios factores:

- Existe un número elevado de dispositivos potencialmente vulnerables. Utilizando buscadores específicos, como Shodan, que permite realizar

búsquedas aplicando diferentes filtros para identificar dispositivos conectados a Internet, nos podemos hacer una idea del número global de equipos con servicios RDP abiertos en Internet. Esto aumenta considerablemente las posibilidades de que uno de ellos sea vulnerable por tener contraseñas débiles, por defecto o por no estar parcheado.

Para realizar la siguiente búsqueda en Shodan, se ha utilizado el filtro «port» indicando el habitualmente utilizado en servidores RDP, el 3389.

Desde Shodan también se pueden ver capturas de pantalla de los servidores de escritorio remoto, lo cual en sí mismo ya puede ser considerado una fuga de información que un ciberdelincuente podría utilizar para futuros ataques.



- La posibilidad de automatización de los ataques. Los ciberdelincuentes utilizan herramientas específicas con las que pueden probar multitud de usuarios y contraseñas en múltiples víctimas. Además pueden utilizar la potencia computacional de las *botnet* para así tener una mayor de posibilidad de éxito.

Recomendaciones de seguridad para el escritorio remoto

Lo primero que se tiene que **valorar es si realmente es necesario utilizar un escritorio remoto en la empresa**, ya que cualquier servicio público en Internet supone un riesgo añadido a la ciberseguridad de la empresa. Si no es necesario conviene deshabilitar el servicio de escritorio remoto. Para ello es recomendable que contactes con el servicio técnico o el administrador de la red.

En caso de ser necesario para las labores de la empresa, se han de tener en cuenta las siguientes consideraciones para que su uso suponga el mínimo riesgo posible.

Sistemas actualizados

El primer aspecto de seguridad en cualquier sistema es que **todo el *software* que se utilice debe estar actualizado a la última versión disponible**. Así, las vulnerabilidades públicas no podrán ser utilizadas para atacar a la organización.

Como ya se indicó, siguen existiendo dispositivos cuyo ciclo de vida ha terminado, como por ejemplo Windows XP o Windows Server 2008, o algunos como Windows 7 que están a punto de terminar. Se debe **evitar utilizar sistemas operativos sin soporte** aunque ante vulnerabilidades tan críticas como la anterior siga recibiendo parches de seguridad.

Redes privadas virtuales

Utilizar redes privadas virtuales o **VPN** como puerta de enlace entre el servidor RDP y el usuario minimizará los riesgos de sufrir un incidente de seguridad. Una VPN crea una conexión cifrada entre ambos dispositivos, por lo que se aumenta considerablemente la privacidad de las comunicaciones. Al igual que sucede con el resto del software, el servidor VPN debe estar actualizado a la última versión.

Esta es la opción que ofrece más garantías de seguridad cuando se tiene que acceder por medio de un escritorio remoto a través de Internet a un equipo de la organización.

Utilizar la combinación VPN más escritorio remoto aumentará el nivel de seguridad, ya que hay una doble barrera hasta la información de la empresa. En caso de que los ciberdelincuentes consigan acceso por medio del servidor VPN, todavía tendrían que conseguir acceso al escritorio remoto.

Nombres de usuario y contraseñas robustas

Como se mostró en el estudio sobre ataques que reciben los escritorios remotos en Internet, muchos se hacen utilizando nombres de usuario genéricos como Administrador, por tanto habrá que **utilizar nombres de usuario que no sean comunes**. Así será más difícil que los ataques de fuerza bruta sean exitosos.

Además es común que los ataques utilicen contraseñas débiles por lo que utilizando una **contraseña robusta lo más larga posible** se reducirá considerablemente la posibilidad de que se produzca un acceso no autorizado. Se deben utilizar nombres de usuario no genéricos y contraseñas robustas, tanto para acceder al servidor VPN, como al escritorio remoto.

Bloqueo de cuenta

Los ataques de fuerza bruta basan su funcionamiento en probar posibles nombres de usuario y contraseña hasta que consiguen el acceso o deciden abandonar el ataque en busca de otro objetivo. Se recomienda aplicar una política de seguridad que **restrinja el acceso del usuario durante un tiempo determinado tras varios intentos no exitosos**. El tiempo de bloqueo aumentará en función del número de intentos no exitosos llegando incluso a bloquear completamente el usuario atacado.

Doble factor de autenticación

Utilizar un sistema de doble factor de autenticación para acceder al escritorio remoto dotará de un plus extra de seguridad a la organización. Para ello, además de tener que conocer el binomio usuario/contraseña, será obligatorio saber un tercer dato (huella, código generado en el momento, etc.). Se utilizarán preferiblemente aplicaciones específicas como mecanismo de doble factor de autenticación en lugar de mensajes SMS, ya que estos son más vulnerables a ataques.

Cambiar el puerto por defecto de RDP

En caso de no utilizar una solución VPN para acceder al escritorio remoto, se recomienda cambiar el puerto utilizado por defecto para conectarse. Comúnmente, la conexión al servicio de escritorio remoto de Windows se hace por medio del puerto 3389. Si se cambia por otro distinto, se dificultará los ataques automatizados que llevan a cabo los ciberdelincuentes. Esto se conoce como seguridad por oscuridad.

Listas de acceso mediante NLA

Probablemente no todos los usuarios de la empresa deben tener acceso al escritorio remoto por lo que se debe limitar este a los estrictamente necesarios. Limitando el

número de usuarios posibles con acceso, se reduce el riesgo de que un ciberdelincuente consiga acceso de forma fraudulenta. Para ello, es recomendable utilizar NLA, por sus siglas en inglés *Network Level Authentication*. Mediante esta tecnología, los usuarios deben autenticarse en la red de la empresa antes de poder hacerlo en el servidor RDP. NLA añade una capa extra de seguridad ante posibles ataques ya que se requiere una doble autenticación. En cualquier caso, debemos mantener la lista de accesos habilitados actualizada, sin olvidar supervisar y monitorizar los accesos remotos.

Reglas del Firewall

En el firewall de la empresa también se recomienda crear reglas específicas para restringir el acceso al servidor de escritorio remoto a un subconjunto de máquinas controlado. Este filtrado se puede hacer por medio de direcciones IP, permitiendo que únicamente accedan las asociadas a los equipos de la empresa.

Utilizar un sistema de escritorio remoto puede ser de gran ayuda a la hora de desempeñar las funciones de trabajo diarias, pero también puede ser la puerta de entrada de los ciberdelincuentes. Proteger su acceso implementando medidas y políticas de seguridad, será vital para evitar ser víctima de un incidente de seguridad.

Referencias

Microsoft. (Mayo 2019). Guía para clientes sobre CVE-2019-0708 | Vulnerabilidad de ejecución de código remoto en los servicios de Escritorio Remoto: 14 de mayo de 2019. 27 de Agosto de 2019, de Microsoft Sitio web: https://support.microsoft.com/es-es/help/4500705/customer-guidance-for-cve-2019-0708

Microsoft. (Mayo 2019). Hoja de datos del ciclo de vida de Windows. 27/08/2019, de Microsoft Sitio web: https://support.microsoft.com/es-es/help/13853/windows-lifecycle-fact-sheet

Incibe. (2019). ¿Es seguro tu escritorio remoto?. 22/08/2019, de Incibe instituto nacional de ciberseguridad Sitio web: https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto