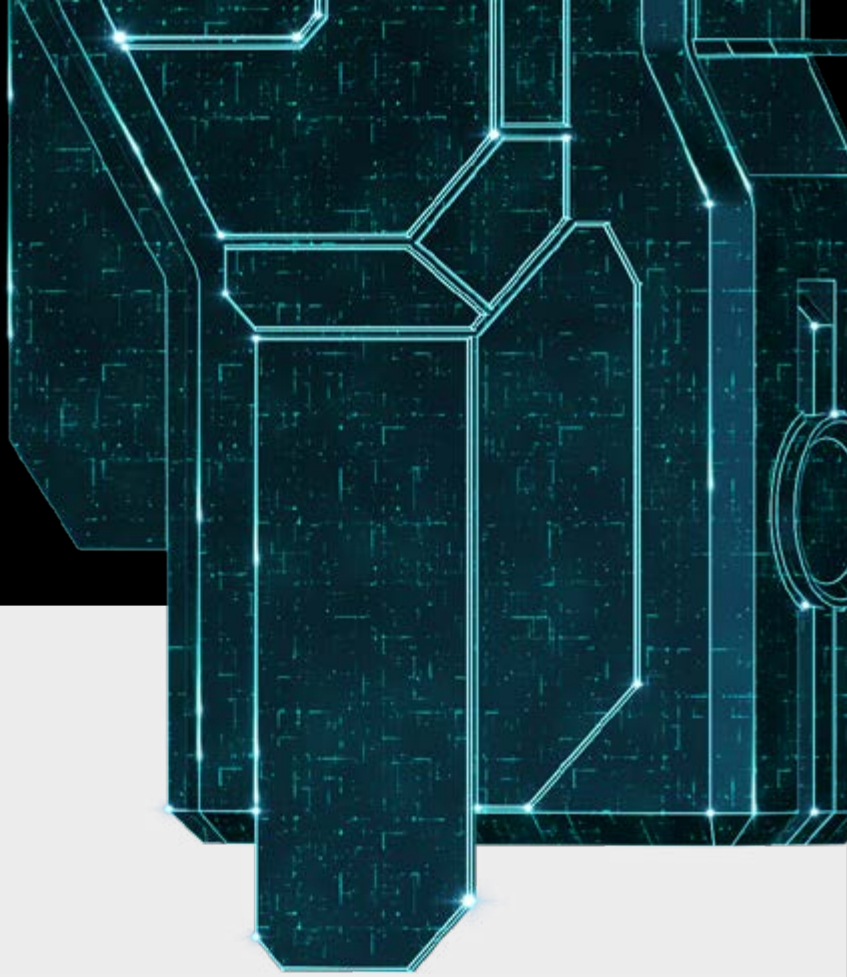
CYBERSECURITY
EXPERTS ON YOUR SIDE



RDP: CONFIGURACIÓN DE SEGURIDAD PARA UN FUTURO REMOTO, PERO NO TAN DISTANTE

Reduzca los riesgos con buenas prácticas, herramientas de autenticación y la base de conocimiento existente.

La pandemia ha forzado a empresas de todo el mundo a implementar el teletrabajo y valerse de todos los medios posibles para continuar con su actividad. En muchos casos, esto implica el uso de la tecnología de **Protocolo de escritorio remoto** (RDP, del inglés), que en los últimos años ha sido objeto de ataques cibernéticos, en especial, cuando los delincuentes encuentran la manera de aprovechar fallas de configuración o contraseñas débiles para obtener acceso a las redes de la compañía.

Una vez adentro, los atacantes tienen vía libre para hacer casi cualquier cosa, por ejemplo, robar propiedad intelectual u otra información confidencial y cifrarla para exigir el pago de un rescate.

AUTOR: Aryeh Goretsky
COLABORADOR: James Shepperd

Abril de 2020

1.

¿Qué hacen los atacantes con el RDP?

En los últimos años, han aumentado la cantidad de incidentes en los que los atacantes se conectaban remoto a los servidores Windows desde Internet mediante el protocolo RDP e iniciaban sesión como administradores. Aquí entran en juego varios vectores de ataque: el aprovechamiento de vulnerabilidades (como BlueKeep CVE-2019-0708), el phishing, credenciales filtradas obtenidas de fugas de datos, el descifrado de contraseñas simples, los ataques por fuerza bruta y el acceso a los sistemas internos mal configurados.

Una vez que los atacantes inician sesión en un servidor como administradores, por lo general, primero realizan una tarea de reconocimiento para determinar quién utiliza el servidor, para qué y cuándo. Luego, inician las acciones maliciosas.

La siguiente no es una lista completa de todo lo que pueden hacer, ni necesariamente implica que van a realizar todas estas acciones. La frecuencia exacta, la secuencia y la naturaleza de lo que harán los atacantes varía drásticamente en cada ataque.

ACTIVIDADES MALICIOSAS MÁS COMUNES:

- borrar los archivos de registro que contienen evidencia de su presencia en el sistema
- deshabilitar los backups y las instantáneas del sistema
- deshabilitar el software de seguridad o configurar exclusiones (que está permitido para los administradores)
- descargar e instalar programas en el servidor
- borrar o sobrescribir copias de seguridad, si es que están accesibles
- extrayendo datos del servidor

TRES DE LAS TAREAS MÁS COMUNES:

- instalar programas de extracción de monedas para generar criptomonedas, como Monero
- instalar ransomware para cifrar contenido y extorsionar a la organización (a menudo se paga con criptomonedas, como el bitcoin)
- en algunos casos, instalar programas de control remoto adicionales para mantener el acceso (persistente) a servidores comprometidos en el caso de que se descubran y finalicen sus actividades RDP.

ACTIVIDAD MALICIOSA NOTABLE Y RECIENTE A TRAVÉS DEL PROTOCOLO RDP

GandCrab, un *ransomware* prolífico que funcionó hasta mayo de 2019, utilizó un modelo de negocio de *ransomware* como servicio (RaaS) en el que los desarrolladores les ofrecían a otros actores maliciosos una participación en el negocio a cambio de propagar aún más su *malware*. **GandCrab** dirigía sus ataques a los Proveedores de servicios gestionados (MSP) que usaban el protocolo RDP para conectarse a sus herramientas de administración remota y así lograba extorsionar a varios clientes a la vez.

Si bien los operadores de **GandCrab** anunciaron su retiro cuando el FBI dio a conocer las claves para descifrar su *ransomware*, nuestros expertos creen que el código fuente de **GandCrab** pudo haber sido vendido a un grupo diferente que ahora ejecuta Sodinokibi, (debido a cambios en el código, su estructura y actualizaciones posteriores). El *ransomware* Sodinokibi apareció justo cuando **GandCrab** comenzó a suspender sus operaciones, prácticamente reemplazando a GandCrab y utilizando tácticas, técnicas y procedimientos similares a los de su predecesor para atacar a los MSP a través del RDP.

Al infectar un proveedor MSP, el *ransomware* logra llegar a todas sus empresas cliente, ya que los MSP poseen las "llaves del reino" para acceder a miles de PYME (y sus socios comerciales) e incluso a algunas grandes corporaciones. En el lado del cliente del MSP, las empresas enfrentan dependencias similares, ya que tanto los equipos como los usuarios individuales dependen de los administradores para obtener ayuda de TI, desde la gestión de licencias e instalación de actualizaciones hasta la seguridad.

LA VULNERABILIDAD DEL RDP CONSTITUYE UN IMPORTANTE FACTOR DE RIESGO

Los ataques realizados a través del protocolo RDP fueron aumentando lenta pero constantemente, y varias organizaciones gubernamentales (como el FBI de los Estados Unidos, el NCSC del Reino Unido, el CCCS de Canadá y el ACSC de Australia, por nombrar algunos) advirtieron sobre sus riesgos.

En mayo de 2019, se detectó la vulnerabilidad de seguridad del protocolo RDP denominada CVE- 2019- 0708 (también conocida como "BlueKeep"), que afecta a Windows 2000, Windows XP, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008 y Windows Server 2008 R2*.

Aunque se trate de sistemas operativos viejos y, en muchos casos, cuentan con soporte limitado o nulo del fabricante, los datos telemétricos sugieren que aún hay muchos sistemas vulnerables en uso.

ESET OFRECE UNA HERRAMIENTA DE DETECCIÓN GRATUITA DE BLUEKEEP (CVE- 2019-0708) QUE AYUDA A IDENTIFICAR LOS SISTEMAS VULNERABLES A TRAVÉS DEL PROTOCOLO RDP. PARA VER LAS INSTRUCCIONES DE USO Y DESCARGAR UNA COPIA,

LEER EL ARTÍCULO

**Tenga en cuenta:* *Al momento de la publicación de este artículo, se informa que la vulnerabilidad no afecta las versiones Windows 8 y Windows Server 2012 (y posteriores).*

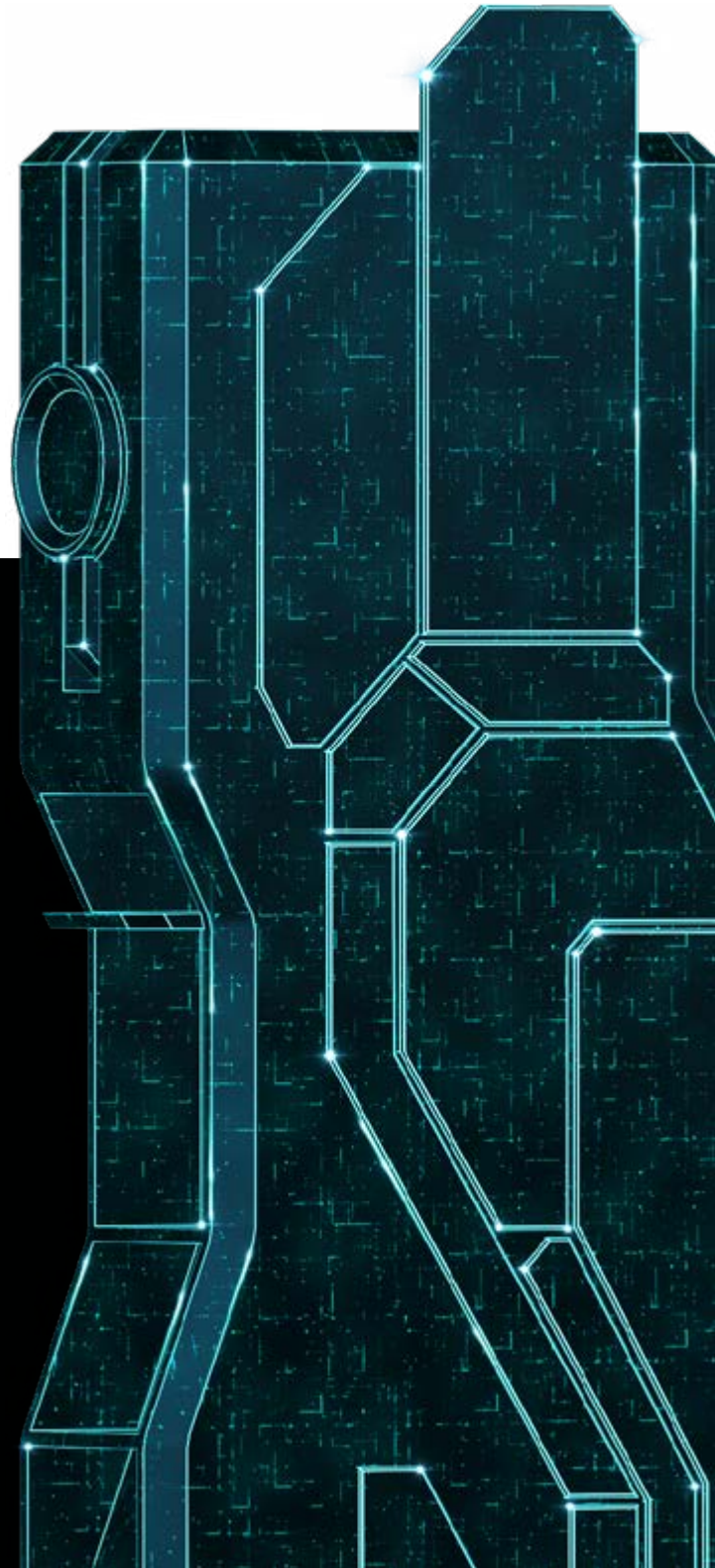
BlueKeep les permite a los atacantes ejecutar código arbitrario en los equipos de sus víctimas. Por más que incluso un atacante individual pueda usar herramientas para automatizar sus ataques y propagarlos en forma generalizada, esta vulnerabilidad en particular tiene la capacidad de comportarse como un gusano, es decir que un ataque podría extenderse automáticamente a través de las redes sin ninguna intervención humana, como ocurrió con los gusanos Win32/Diskcoder.C (también conocido como NotPetya) y Conficker.

El aprovechamiento de las vulnerabilidades que tienen esta capacidad se considera un problema grave. En su guía para clientes sobre vulnerabilidades, Microsoft le ha asignado el nivel de gravedad más alto: Crítico. Y en la Base de datos de vulnerabilidades de los Estados Unidos, la entrada para CVE-2019-0708 se califica con 9,8 puntos de un total de 10. Microsoft publicó un comunicado en su blog donde les recomienda firmemente a los usuarios que instalen los parches que lanzó incluso para los de sistemas operativos obsoletos que ya no cuentan con soporte, como Windows XP y Windows Server 2003. Fue tanta la preocupación sobre la existencia de un exploit con características de gusano que, a principios de junio de 2019, la Agencia de Seguridad Nacional de los Estados Unidos emitió una alerta inusual recomendando la instalación de los parches de Microsoft para corregir la falla.

De todas formas, no se detectó una escalada significativa de la actividad de BlueKeep en las pruebas de penetración llevadas a cabo en equipos de todo el mundo hasta noviembre de 2019, cuando se hicieron públicos los informes masivos sobre el uso del *exploit*, como lo señalaron los medios ZDNet y WIRED.

Según los informes, la mayoría de los ataques no tuvieron éxito: cuando el atacante intentaba usar el *exploit* para la vulnerabilidad BlueKeep, en aproximadamente el 91% de las computadoras vulnerables aparecía un error (los equipos mostraban la pantalla de verificación de errores, también conocida como "pantalla azul de la muerte"). Sin embargo, en el 9% de las computadoras vulnerables restantes, los atacantes instalaron con éxito el *software* para minar la criptomoneda Monero. Aunque al final no fue un ataque de gusano como se esperaba, el grupo criminal igual logró automatizarlo, pero con una tasa muy baja de éxito.

Dado que el tiempo es esencial, nos concentraremos en lo que se debe hacer para proteger las redes ante esta amenaza.



2.

Cómo defenderse de los ataques a través de RDP

En primer lugar, debe evitar conectarse a sus servidores por Internet en forma directa utilizando el RDP, o al menos minimizar su uso siempre que sea posible. Esto puede ser problemático para muchas empresas, en especial ahora que gran parte de los colaboradores trabaja remotamente por la cuarentena.

Recuerde que si aún está usando los sistemas obsoletos Windows Server 2008 o Windows 7 (que dejaron de recibir soporte a partir de enero de 2020) y tiene máquinas con estas plataformas a las que se puede acceder directamente a través de RDP, corre un grave riesgo de ataque y debe tomar medidas correctivas de inmediato. Si usa estas plataformas, su superficie de amenaza se multiplica significativamente, por lo que **debe dejar las recomendaciones que damos a continuación en segundo plano hasta que haya actualizado los sistemas de su empresa a plataformas que reciban el soporte completo de sus respectivos fabricantes.**

Para quienes ya tengan las plataformas actualizadas, la situación no implica que tiene que dejar de usar el RDP de inmediato, sino que debe tomar algunas medidas adicionales para protegerse lo más rápido y exhaustivamente posible. Para ello, hemos creado una tabla con los **12 pasos principales que puede seguir para comenzar a proteger sus computadoras de los ataques basados en RDP.**

12 RECOMENDACIONES PARA PROTEGER EL RDP

En líneas generales, la tabla se basa en el orden de importancia y la facilidad de implementación, pero puede variar según las características específicas de cada organización. En ciertos casos, algunas recomendaciones pueden no ser aplicables o puede resultar más práctico hacerlas en otro orden. También es posible que su organización necesite tomar medidas adicionales.

	RECOMENDACIÓN	MOTIVO
1	Bloquear las conexiones externas a máquinas locales en el puerto 3389 (TCP / UDP) en el firewall perimetral.*	Bloquea por completo el acceso RDP desde Internet.
2	Probar e implementar los parches para la vulnerabilidad CVE-2019-0708 (BlueKeep) y habilitar la Autenticación en el nivel de la red.	Instalar el parche de Microsoft y seguir sus pautas prescriptivas ayuda a proteger los dispositivos contra BlueKeep.
3	Requerir contraseñas complejas para todas las cuentas que puedan iniciar sesión a través del protocolo RDP (más de 15 caracteres, sin frases relacionadas con la empresa, nombres de productos o de usuarios).	Protege ante ataques de adivinación de contraseñas y el uso de credenciales filtradas obtenidas de fugas de datos. Para el atacante es fácil automatizar estas tareas; por eso es fundamental utilizar contraseñas fuertes.
4	Usar contraseñas únicas y derechos de administrador para las cuentas locales que necesiten acceder a los servidores (por ejemplo, el servicio LAPS de Microsoft o algún otro de administración de contraseñas). **Restringir los derechos de acceso al servidor a un grupo limitado de usuarios.*	*(igual que arriba)* Reduce la superficie de ataque de los servidores al limitar la cantidad de usuarios que pueden acceder a ellos.
5	Configurar el nivel de cifrado de la conexión del cliente RDP en "alto", si es posible, sino usar el nivel de cifrado más alto disponible para las conexiones.	Utilice cifrado de 128 bits para todas las comunicaciones entre el cliente y el servidor, de ser posible.

6	Instalar una solución de autenticación en varias fases (MFA), como ESET Secure Authentication (ESA), que sea obligatoria para todas las cuentas que inicien sesión a través del protocolo RDP, así como para todas las cuentas con derechos de administrador.	Requiere una segunda capa de autenticación que los empleados solo puedan obtener desde un teléfono móvil, token u otro mecanismo para iniciar sesión en las computadoras en forma segura.
7	Configurar una puerta de enlace para las conexiones de red privada virtual (VPN) de modo de gestionar todas las conexiones RDP desde fuera de su red local.	Evita las conexiones RDP entre Internet y su red local. Le permite imponer requisitos de identificación y autenticación más fuertes para el acceso remoto a las computadoras.
8	Asegurar, desde el panel de control, que el software de seguridad para endpoints esté usando una contraseña segura no relacionada con las cuentas administrativas y de servicio. ESET Security Management Center (ESMC) permite controlar las políticas en forma fácil y granular, así como crear grupos de computadoras. Además, la consola de ESMC permite el acceso de múltiples usuarios mediante inicios de sesión protegidos por MFA.	Proporciona una capa adicional de protección en caso de que un atacante obtenga acceso a su red como administrador.
9	Habilitar el bloqueo de exploits en el software de seguridad para endpoints: se trata de una tecnología de detección de anomalías no basada en firmas que monitorea el comportamiento de las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia.	Muchos programas de seguridad para endpoints también pueden bloquear las técnicas de los exploits. Verifique que esta funcionalidad esté siempre habilitada.
10	Aislar las computadoras no seguras a las que se deba acceder desde Internet usando el protocolo RDP.	Implemente el aislamiento de red para bloquear las computadoras vulnerables del resto de la red.
11	Reemplazar las computadoras no seguras.	Si una computadora no permite la instalación del parche (para la vulnerabilidad BlueKeep), planifique su reemplazo oportuno.
12	Implementar el bloqueo de direcciones IP según la geolocalización (GeoIP) en la puerta de enlace VPN.	Si el personal y los proveedores se encuentran en un mismo país o dentro de una lista reducida de países, considere bloquear el acceso de los países excluidos de dicha lista para evitar conexiones de atacantes extranjeros.

* **Por defecto, el protocolo RDP opera en el puerto 3389**. *Si lo ha cambiado a un valor diferente, entonces deberá bloquear el puerto modificado.*

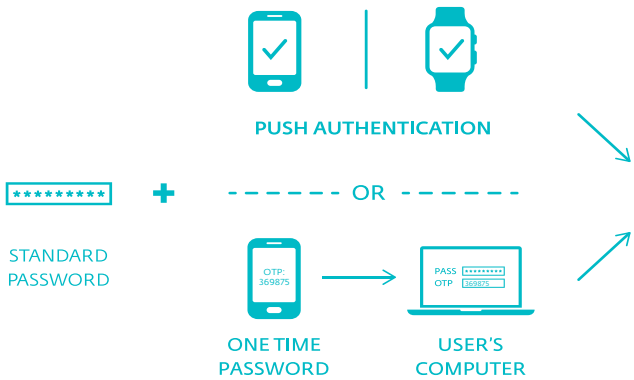
3.
Cómo lo puede ayudar ESET a proteger su RDP

Lo primero es asegurarse de que su software de seguridad para endpoints A. esté actualizado y B. detecte la vulnerabilidad BlueKeep. Luego entran en juego los papeles más granulares de la tecnología en capas. BlueKeep es detectado como RDP / Exploit.CVE- 2019-0708 por el módulo de Protección contra ataques de red de ESET, que es una extensión de la tecnología de firewall de ESET presente en los productos de protección para endpoints de ESET, versión 7 y posteriores.

Otra capa de tecnología crítica para proteger el protocolo RDP es el Bloqueo de exploits de ESET, que monitorea las aplicaciones que suelen ser atacadas por exploits con mayor frecuencia (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.). En lugar de enfocarse solamente en ciertos identificadores de CVE (Vulnerabilidades y Exposiciones Comunes) en particular, se centra en las técnicas de los exploits. Cuando se activa, la amenaza se bloquea de inmediato en la máquina.

Además de las tecnologías, le aconsejamos que implemente procesos adecuados y sencillos para asegurar el RDP. La autenticación en varias fases (MFA) es la más importante porque protege a la organización de las contraseñas fáciles de adivinar y de los ataques por fuerza bruta. Al centrarse en la autenticación del usuario para poder ingresar a un sistema o una plataforma, en este caso el RDP, le permite proteger uno de los sectores más críticos de la empresa para administrar la seguridad de su red y de los usuarios individuales.

La solución MFA ESET Secure Authentication (ESA) protege las comunicaciones vulnerables como el RDP mediante la implementación de la autenticación en varias fases.



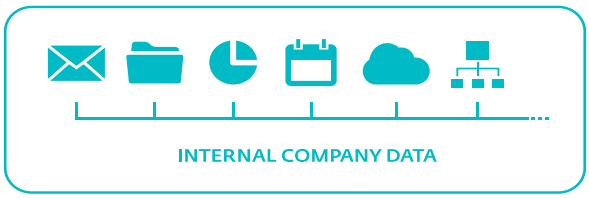
ESA es compatible con todas las redes VPN (que constituyen un mecanismo de protección fundamental para el acceso seguro), así como los inicios de sesión en dispositivos críticos que contienen datos confidenciales y servicios en la nube como Office 365, Google Apps o Dropbox y muchos otros que usan ADFS 3.0 o SAML.

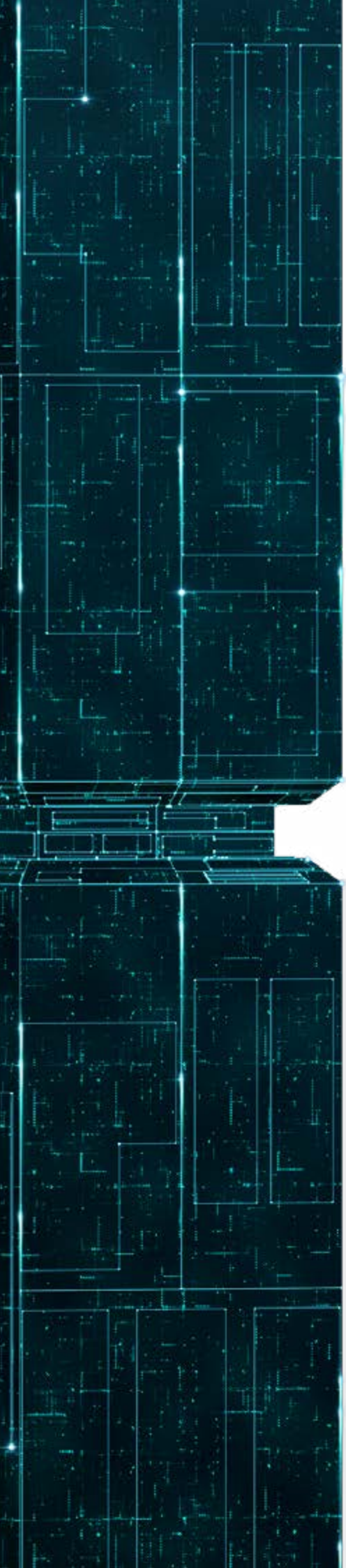
Con la posibilidad de administrarse desde un navegador, ESA fue diseñada para ser compatible con todos los dispositivos iPhone y Android, y con múltiples tipos de autenticadores, incluyendo las notificaciones impulsadas fáciles de usar, las aplicaciones para móviles, los tokens de hardware, las memorias USB de seguridad FIDO y otros métodos personalizados (que se pueden configurar gracias al SDK de ESA). Paralelamente, ESA ayuda a proteger los datos almacenados tanto en la nube como en las instalaciones de la empresa de una manera simple pero potente, y además ayuda a cumplir con los requisitos de normativas como el Reglamento GDPR.

POR EL COVID-19, Y PARA AYUDAR A LAS EMPRESAS A PROTEGER SUS SISTEMAS CRÍTICOS Y DATOS PERSONALES, ESET EXTIENDE EL PERÍODO DE PRUEBA GRATUITA A 90 DÍAS.

MÁS INFORMACIÓN SOBRE ESA

Una vez implementada la MFA, el cifrado del disco completo sería un excelente paso para dar a continuación. El Cifrado de disco completo de ESET (EFDE) proporciona un cifrado potente de los discos, las particiones o las unidades completas del sistema. Se administra en forma nativa desde ESET Security Management Center y ESET Cloud Administrator, mejorando aún más la seguridad de los datos de su organización.





EL CONOCIMIENTO ES PODER, LA SEGURIDAD TAMBIÉN

Se pueden examinar varias técnicas y tácticas de ataques mediante RDP en la base de conocimiento de MITRE ATT&CK® que reúne gran parte de la información sobre ataques en un espacio común. Complementar el uso de las herramientas de detección y respuesta para endpoints (EDR) con esta información, puede ser útil para analizar las amenazas a las que se enfrenta su red. Las herramientas como ESET Enterprise Inspector (EEI) les permiten a los administradores de seguridad examinar las detecciones, encontrar una referencia directa a la base de conocimiento de ATT&CK para obtener más información y configurar alarmas personalizadas para su red.

Respecto a las amenazas transmitidas por RDP, otra posibilidad es que el sistema tenga detecciones (parciales), pero esté desprotegido. Las herramientas de EDR también pueden desempeñar un papel fundamental en escenarios en los que no hay una detección clara del ataque. Por ejemplo, en algunos casos, el exploit BlueKeep bloqueó de inmediato el sistema infectado porque resultó poco confiable. Entonces, para que el exploit de RDP funcione, el atacante debe emparejarlo con otro exploit, por ejemplo, con una vulnerabilidad de divulgación de información (a través de archivos Flash-php) que revela las direcciones de memoria del kernel para que ya no sea necesario adivinarlas. Esto podría reducir la probabilidad de que se bloquee el equipo, ya que el exploit actual utiliza la técnica heap spraying para facilitar la ejecución de código arbitrario. Estos comportamientos típicos de los exploits se pueden detectar con reglas personalizadas creadas dentro de EEI, que en última instancia activan una alarma y llaman la atención del administrador. La inteligencia de red adicional también puede obtenerse mediante pruebas de penetración periódicas y comprobando las conductas sospechosas a través de herramientas SIEM, IPS e IDS.

CONCLUSIÓN

El COVID-19 ha cambiado la forma en que operan las organizaciones para siempre. Las empresas se deben adaptar a las demandas de los colaboradores que ahora trabajan desde su casa; y que posiblemente lo sigan haciendo en el futuro.

Algo que nos ha demostrado esta pandemia es que muchos trabajos que se hacian desde la oficina, ahora se consideran aptos para realizar de forma remota. Para ello, las empresas deben garantizar un acceso seguro a los recursos, y en ESET contamos con soluciones que permiten cubrir estas necesidades.