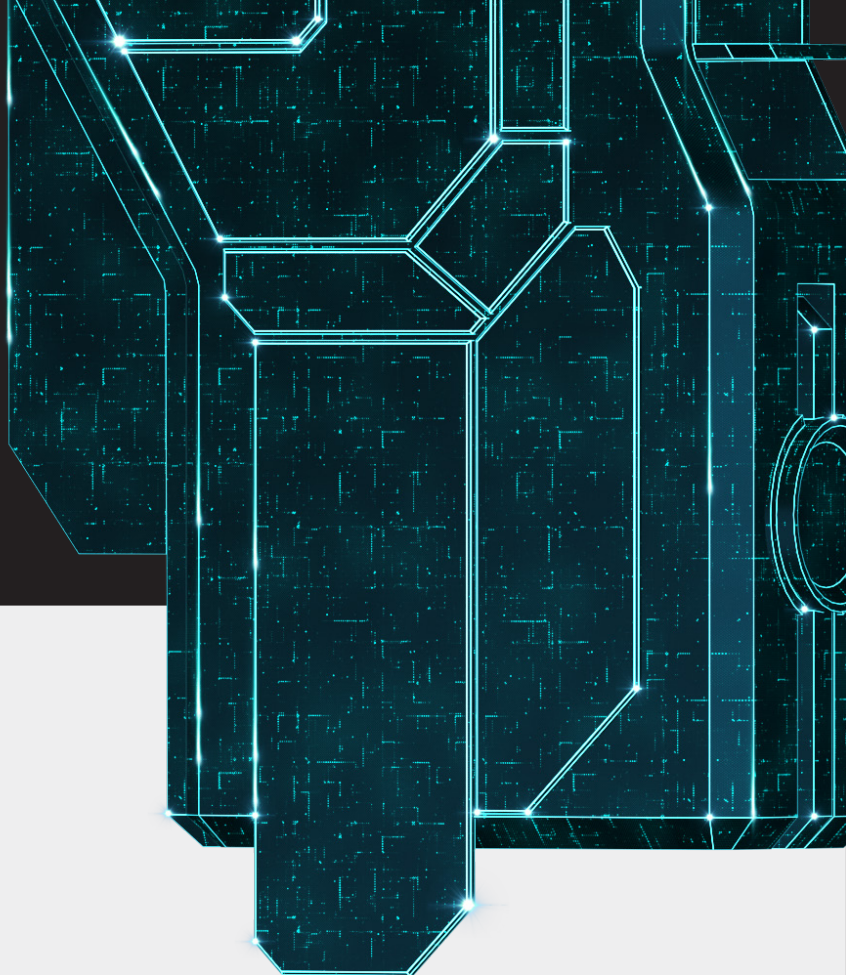




Digital Security
Progress. Protected.



RDP: CONFIGURANDO SEGURIDAD PARA UN FUTURO REMOTO, PERO NO UN FUTURO A DISTANCIA

¿Aprovechando el RDP para gestionar tu red durante una crisis? Entonces asegúrate de limitar tu riesgo con buenas prácticas, herramientas de autenticación y aprovechando la base de conocimientos existente.

La pandemia de la COVID 19 ha empujado a las empresas de todo el mundo a enviar a su plantilla a casa y a potenciar el trabajo a distancia de forma masiva utilizando cualquier medio posible. Esto incluye el uso de la tecnología RDP que en los últimos años ha sido objeto de ataques.

Han surgido numerosos casos, especialmente cuando los atacantes han encontrado la manera de explotar los ajustes mal configurados o las contraseñas débiles para obtener acceso a las redes de la empresa.

Una vez dentro, los atacantes tienen una puerta abierta para hacer casi cualquier cosa, incluyendo, por ejemplo, el robo de propiedad intelectual u otra información sensible y cifrarla para pedir un rescate.

AUTOR: Aryeh Goretsky
COLABORADOR: James Shepperd

Abril 2020

1.

¿Qué hacen los atacantes con el RDP?

En los últimos años, ESET ha visto un número creciente de incidentes en los que los atacantes se conectaban remotamente a servidores Windows desde Internet utilizando RDP y se registraban como administrador del equipo. Esto implica varios vectores que incluyen: vulnerabilidades (como BlueKeep CVE-2019-0708), phishing, robo de credenciales, difusión de contraseñas, fuerza bruta o acceso mal configurado a sistemas internos.

Una vez que los atacantes se conectan a un servidor como administrador, suelen realizar un análisis para determinar para qué se utiliza el servidor, por quién y cuándo se utiliza. Entonces pueden empezar a realizar acciones maliciosas.

Esta no es una lista completa de todo lo que pueden hacer, ni necesariamente van a realizar todas estas actividades. La frecuencia exacta, la secuencia y la naturaleza de lo que harán los atacantes varía mucho.

LAS ACTIVIDADES MALICIOSAS MÁS COMUNES QUE HEMOS VISTO INCLUYEN:

- borrar los archivos de registro que contengan pruebas de su presencia en el sistema
- desactivar las copias de seguridad programadas y las instantáneas
- desactivar el software de seguridad o configurar exclusiones en el mismo (lo cual está permitido para administradores)
- descargar e instalar varios programas en el servidor
- borrar o sobrescribir las copias de seguridad antiguas, si son accesibles
- exfiltrar datos del servidor

TRES DE LAS MÁS COMUNES SON:

- instalar programas de minería de monedas con el fin de generar criptomonedas, como Monero
- la instalación de ransomware con el fin de extorsionar a la empresa, a menudo para ser pagado usando criptomoneda, como bitcoin
- en algunos casos, los atacantes pueden instalar software de control remoto adicional para mantener el acceso (persistencia) a los servidores comprometidos en caso de que sus actividades RDP sean descubiertas y terminadas

ACTIVIDAD MALICIOSA NOTABLE Y RECIENTE DE RDP

Un prolífico ransomware, GandCrab, que operó hasta mayo de 2019, utilizó un modelo de negocio de ransomware como servicio (RaaS) en el que los desarrolladores aprovecharon una serie de autores maliciosos afiliados para seguir distribuyendo el malware. GandCrab, en particular, se dirigía a los MSPs que utilizaban RDP para conectarse a sus herramientas de gestión remota y extorsionar a varios clientes a la vez.

Aunque los responsables del ransomware GandCrab anunciaron su retirada después de que el FBI publicara las claves para descifrar su ransomware, nuestros expertos creen que el código fuente de GandCrab puede haber sido vendido a un grupo diferente que ahora está ejecutando Sodinokibi, (debido a los cambios en el código, su estructura y sus posteriores actualizaciones). El ransomware Sodinokibi apareció justo cuando GandCrab empezó a suspender sus operaciones, esencialmente sustituyendo a GandCrab y utilizando tácticas, técnicas y procedimientos similares a los de su predecesor para atacar a los MSPs a través de RDP.

La conexión con los MSPs también es notable para las empresas, ya que los MSPs tienen las "llaves que conducen al reino" de miles de PYMES (y de las relaciones comerciales de esas PYMES), e incluso de algunas empresas. Del lado del cliente MSP, las empresas se enfrentan a dependencias similares, ya que tanto los equipos como los usuarios individuales dependen de los administradores para que les ayuden en todo, desde las licencias y las actualizaciones hasta la seguridad.

LA VULNERABILIDAD DE LA RDP ABRE UNA GRAN PUERTA AL RIESGO

Los ataques a través de RDP han ido aumentando lenta, pero constantemente, y han sido objeto de una serie de avisos gubernamentales del FBI, el NCSC del Reino Unido, el CCCS de Canadá y el ACSC de Australia, por nombrar algunos.

En mayo de 2019 se abrieron las compuertas con la llegada de CVE-2019-0708, alias "BlueKeep", una vulnerabilidad de seguridad en RDP 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 puede tratarse de sistemas heredados y, en la mayoría de los casos, ya no reciben soporte o solo tienen un soporte limitado por parte del proveedor, la telemetría sugiere que habrá muchos sistemas vulnerables todavía en uso.

La vulnerabilidad BlueKeep permite a los atacantes ejecutar un código de programa arbitrario en los ordenadores de sus víctimas. Aunque incluso los atacantes individuales pueden ser una amenaza generalizada utilizando herramientas automatizadas para los ataques, esta vulnerabilidad es "wormable", lo que significa que un ataque podría propagarse automáticamente a través de las redes sin ninguna intervención de los usuarios, al igual que los gusanos Win32 / Diskcoder.C (aka NotPetya) y Conficker en el pasado.

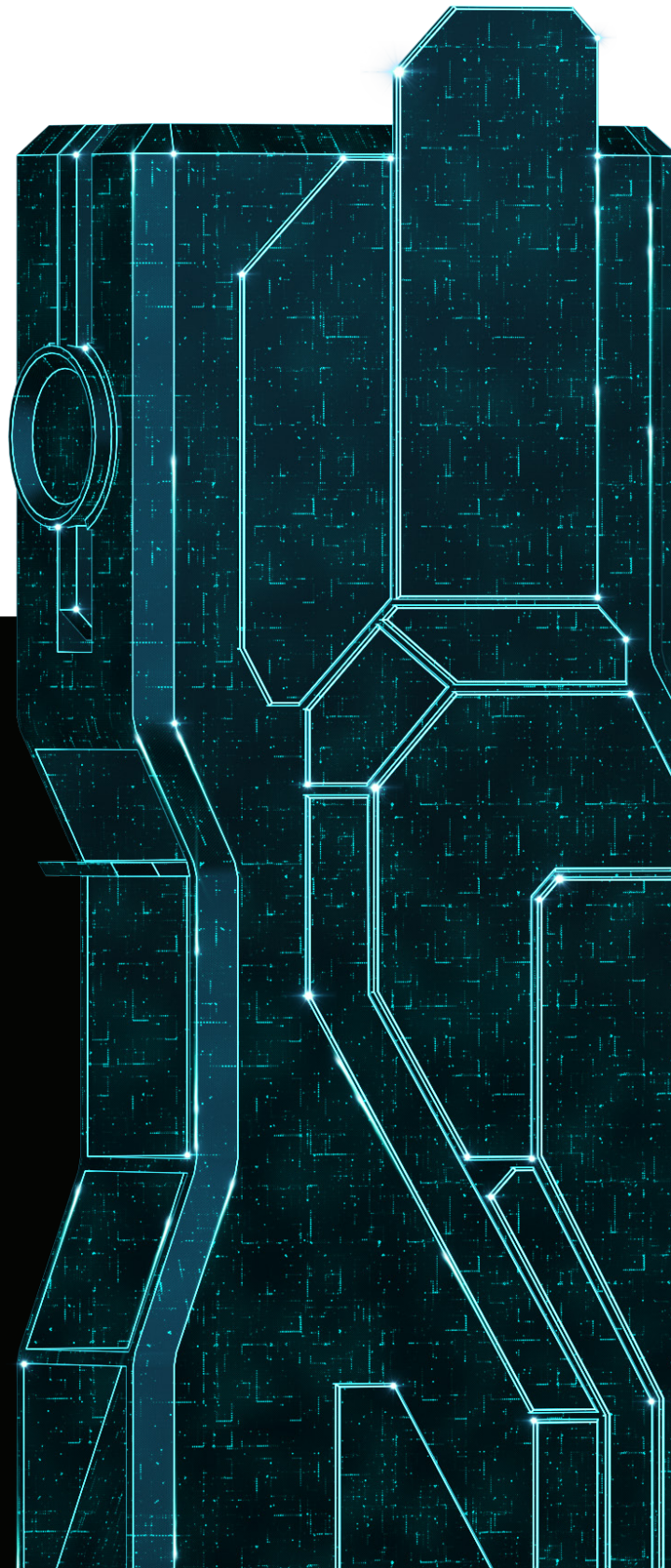
ESET OFRECE UNA HERRAMIENTA DE DETECCIÓN GRATUITA BLUEKEEP (CVE-2019-0708) PARA AYUDAR A IDENTIFICAR LOS SISTEMAS VULNERABLES A LA EXPLOTACIÓN MEDIANTE RDP. PARA OBTENER INSTRUCCIONES SOBRE SU USO Y DESCARGAR UNA COPIA

**Nota: Las versiones de Windows 8 y Windows Server 2012 y posteriores no están siendo afectadas en el momento de la publicación.*

La explotación de las vulnerabilidades que pueden convertirse en gusanos se considera generalmente un problema grave. Microsoft ha asignado a la vulnerabilidad su nivel de gravedad más alto, Crítico, en su guía publicada para los clientes, y en la Base de Datos Nacional de Vulnerabilidad del gobierno de los Estados Unidos, la entrada de CVE-2019-0708 tiene una puntuación de 9,8 sobre 10. Microsoft publicó entrada en su blog en la que recomendaba encarecidamente a los usuarios que instalaran sus parches, incluidos los de los sistemas operativos no compatibles, como Windows XP y Windows Server2003. La preocupación por un exploit de tipo gusano era tan alta que, a principios de junio de 2019, la Agencia de Seguridad Nacional de los Estados Unidos emitió un insólito aviso en el que recomendaba la instalación de los parches de Microsoft para el citado fallo.

Mientras se hacían las rondas en varios conjuntos de pentesting en todo el mundo, no se reportaron escaladas importantes en la actividad de BlueKeep hasta noviembre de 2019, cuando los informes masivos de uso del exploit se hicieron públicos, como señalaron ZDNet y WIRED. Según los informes, los ataques fueron menos que exitosos, ya que alrededor del 91% de los ordenadores vulnerables se bloquean con un error de parada (también conocido como verificación de errores o pantalla azul de la muerte) cuando el atacante intenta explotar la vulnerabilidad BlueKeep. Sin embargo, en el 9% restante de los ordenadores vulnerables, estos atacantes instalaron con éxito el software de minería de criptomonedas Monero. Aunque no se trata del temido ataque con gusanos, el grupo criminal automatizó la explotación, aunque sin un alto porcentaje de éxito.

Dado que el tiempo es esencial, evitemos una descripción demasiado detallada de la vulnerabilidad y centrémonos en lo que debe hacerse para proteger las redes contra esta amenaza.



2.

Defensa contra los atacantes de RDP

Entonces, ¿qué puedes hacer? Bueno, lo primero es dejar de conectarte directamente a tus servidores a través de Internet utilizando RDP o al menos minimizarlo siempre que sea posible. Esto puede ser problemático para muchas empresas, especialmente ahora que muchos empleados pueden estar trabajando remotamente bajo varios regímenes de cuarentena.

Insistamos, si todavía estás ejecutando Windows Server 2008 o Windows 7 (que ya no son soportados a partir de enero de 2020) y tienes máquinas ejecutando estas plataformas que son directamente accesibles a través de RDP, entonces estás en grave riesgo de ataque y debes tomar medidas de solución inmediatamente. Al ejecutar estas plataformas, tu superficie de amenaza se ha multiplicado por un factor sustancial, y **las recomendaciones que figuran a continuación deberían pasar a un segundo plano para que tu empresa se actualice a las plataformas que están totalmente soportadas por sus respectivos proveedores.**

Para aquellos que ejecutan plataformas actualizadas, la situación no significa que haya que dejar de usar inmediatamente RDP, sino que hay que tomar medidas adicionales para asegurarlo cuanto antes y de la forma más completa posible. Para ello, hemos creado una tabla con **los 12 principales pasos que puedes dar para empezar a proteger tus equipos de los ataques basados en RDP.**



12 RECOMENDACIONES PARA ASEGURAR LA RDP

Esta tabla se basa, a grandes rasgos, en el orden de importancia y la facilidad de aplicación, pero puede variar en función de tu empresa. Algunas pueden no ser aplicables o puede ser más práctico hacerlas en un orden diferente. Es posible que tu empresa tenga que tomar medidas adicionales.

	RECOMENDACIÓN	RAZÓN
1	No permitir las conexiones externas a las máquinas locales en el puerto 3389 (TCP / UDP) en el cortafuegos*	Bloquea por completo el acceso a RDP desde Internet.
2	Probar y aplicar parches para la vulnerabilidad CVE-2019-708(BlueKeep) y habilitar la autenticación a nivel de red lo antes posible.	Instalar el parche de Microsoft y seguir sus directrices prescriptivas ayuda a garantizar que los dispositivos estén protegidos contra la vulnerabilidad BlueKeep.
3	Para todas las cuentas a las que se pueda acceder a través de RDP, exige contraseñas complejas (es obligatoria una frase de contraseña larga que contenga más de 15 caracteres sin frases relacionadas con la empresa, los nombres de los productos o los usuarios).	Protege contra los ataques de suplantación de contraseñas y credenciales. Es increíblemente fácil automatizarlos y aumentar la longitud de las contraseñas, las hace exponencialmente más resistentes a los ataques.
4	Para acceder a los servidores, utiliza contraseñas únicas para las cuentas locales con derechos de administrador (por ejemplo, utilizando LAPS o un servicio de gestión de contraseñas sólido) <i>* También: restringe los derechos de acceso al servidor a un grupo limitado de usuarios.</i>	(como arriba) Reduce la superficie de ataque de los servidores limitando el número de usuarios que pueden acceder a ellos.
5	Establece el nivel de cifrado de la conexión del cliente RDP en "alto," si es posible. Si no, utiliza el nivel de cifrado más alto disponible para las conexiones.	Utiliza una encriptación de 128 bits para todas las comunicaciones cliente-servidor, si es posible.

6

Instala una solución de autenticación multifactor (MFA), como [ESET Secure Authentication \(ESA\)](#), y la requiere para todas las cuentas a las que pueden iniciar sesión a través de RDP, así como para todas las cuentas de administrador.

Requiere una segunda capa de autenticación solo disponible para los empleados a través del teléfono móvil, token u otro mecanismo para iniciar sesión en los ordenadores.

7

Instala una pasarela de red privada virtual (VPN) para intermediar todas las conexiones RDP desde fuera de tu red local.

Impide las conexiones RDP entre Internet y tu red local. Te permite imponer requisitos de identificación y autenticación más estrictos para el acceso remoto a los ordenadores.

8

A través de tu panel de seguridad, asegúrate de que tu software de seguridad de equipos protegidos por contraseña está utilizando una contraseña fuerte no relacionada con cuentas administrativas y de servicio. ESET PROTECT On-Prem permite un control de políticas fácil y granular y la creación de varios grupos de ordenadores. Al mismo tiempo, ESET PROTECT On-Prem permite el multiarrendamiento y es accesible mediante inicios de sesión protegidos por MFA.

Proporciona una capa adicional de protección en caso de que un atacante obtenga acceso de administrador a tu red.

9

Habilitar el bloqueo de exploits en el software de seguridad de equipos, que es una tecnología de detección de anomalías no basada en firmas que monitoriza el comportamiento de las aplicaciones más comunes.

Muchos programas de seguridad para equipos también pueden bloquear las técnicas de explotación. Comprueba que esta funcionalidad está activada.

10

Aísla cualquier ordenador inseguro al que haya que acceder desde Internet utilizando RDP.

Implementar el aislamiento de la red para bloquear los ordenadores vulnerables del resto de la red.

11

Sustituir los ordenadores inseguros.

Si un ordenador no puede ser parcheado (contra la vulnerabilidad BlueKeep), planifica su sustitución a tiempo.

12

Considera la posibilidad de implementar el bloqueo de GeolP en la puerta de enlace de la VPN.

Si el personal y los proveedores se encuentran en el mismo país, o entre una lista corta de países, considera la posibilidad de bloquear el acceso desde los países excluidos para evitar las conexiones de los atacantes extranjeros.

3.

Cómo ayuda ESET a proteger tu RDP

Un buen primer paso es asegurarte de que tu software de seguridad para equipos está actualizado y detecta la vulnerabilidad BlueKeep. A continuación, hay una función más granular para la tecnología en capas. BlueKeep se detecta como RDP / Exploit. CVE- 2019- 0708 por el módulo Network Attack Protection de ESET, que es una extensión de la tecnología de cortafuegos de ESET presente en los [productos de protección de equipos de ESET](#), versión 7 y superior.

Otra capa de tecnología fundamental para proteger el RDP es ESET Exploit Blocker, que monitoriza las aplicaciones típicamente explotables (navegadores, lectores de documentos, clientes de correo electrónico, Flash, Java, etc.). En lugar de dirigirse únicamente a identificadores CVE concretos, se centra en las técnicas de explotación. Cuando se activa, la amenaza se bloquea inmediatamente en la máquina.

Paralelamente a la tecnología, te recomendamos que pongas en marcha procesos adecuados que sean lo más fáciles de usar posible, procesos que en última instancia se benefician de herramientas fáciles de usar. Dado que la seguridad del RDP requiere varios pasos (de procedimiento), la autenticación multifactor fácil de usar (MFA) es quizás la más crucial porque actúa como protección contra las contraseñas fácilmente adivinadas o forzadas. Al centrarse en la autenticación de un sistema o plataforma, en este caso RDP, protege uno de los sistemas más críticos que tiene en la empresa para gestionar la seguridad tanto de la red como de los usuarios individuales.

Nuestra solución MFA [ESET Secure Authentication \(ESA\)](#) protege las comunicaciones vulnerables, como el Protocolo de Escritorio Remoto, añadiendo una autenticación multifactor.



Una solución como ESA es compatible con todas las VPN (en sí misma una salvaguarda crítica que asegura el acceso), los inicios de sesión en dispositivos críticos que contienen datos sensibles y los servicios en la nube como Microsoft 365, Google Apps o Dropbox y muchos otros que utilizan ADFS 3.0 o SAML.

Gestionado de forma centralizada desde el navegador, ESA fue diseñado para funcionar en todos los iPhones y dispositivos Android, y también funciona bien con múltiples tipos de autenticadores, incluyendo notificaciones push fáciles de usar, aplicaciones móviles, tokens de hardware, claves de seguridad FIDO y otros métodos personalizados (a través del SDK de ESA). Paralelamente ESA ayuda a asegurar tanto los datos de la empresa como la nube de una manera simple, pero potente, también ayuda a cumplir con los requisitos de cumplimiento de regulaciones como GDPR.

DURANTE LA PANDEMIA DE LA COVID-19, PARA AYUDAR A LAS EMPRESAS A PROTEGER EFICAZMENTE SUS SISTEMAS CRÍTICOS Y SUS DATOS PERSONALES, ESET AMPLÍA A 90 DÍAS LA PRUEBA GRATUITA HABITUAL DE ESA.

LEER EL RESUMEN DE LA SOLUCIÓN ESET

Por último, añadir el [cifrado de disco completo](#) como seguimiento de MFA es también un gran paso. ESET Full Disk Encryption (EFDE) proporciona un potente cifrado de los discos del sistema, las particiones o las unidades completas. Se gestiona de forma autónoma a través de las consolas de gestión de [ESET PROTECT \(on-prem\)](#) y [ESET PROTECT](#), mejorando aún más la seguridad de los datos de tu empresa.





EL CONOCIMIENTO ES PODER... TAMBIÉN LA SEGURIDAD TOTAL

También se pueden examinar varias técnicas y tácticas de RDP en la base de conocimientos de MITRE ATT&CK®. Aunque los investigadores de muchos proveedores hacen referencia a ella, la base de conocimientos ATT&CK aporta gran parte de estos conocimientos a un espacio compartido. Aprovechar las herramientas ATT&CK y (EDR) puede ser muy útil para examinar en detalle las amenazas a las que se enfrenta tu red. Herramientas como [ESET Enterprise Inspector](#) (EEI) permiten a los administradores de seguridad examinar las detecciones, consultar directamente la biblioteca de recursos de ATT&CK para obtener más información y establecer alarmas personalizadas para tu red.

Otra posibilidad con las amenazas transmitidas por RDP es tener detecciones (parciales), pero seguir sin protección. El EDR también puede desempeñar un papel en escenarios en los que no se produzcan detecciones claras. Por ejemplo, en algunos casos el exploit BlueKeep bloqueó inmediatamente el sistema objetivo porque resultó ser poco fiable. Por lo tanto, para que el exploit RDP funcione puede ser necesario emparejarlo con otro exploit, como una vulnerabilidad de divulgación de información (por ejemplo, a través de archivos Flash - php) que revele las direcciones de memoria del kernel para que ya no sea necesario adivinarlas. Esto podría reducir la probabilidad de una caída, ya que el exploit actual realiza una gran descarga de almacenamiento libre de datos. Estos comportamientos asociados pueden ser marcados con reglas personalizadas creadas dentro de EEI, activando finalmente una alarma y llamando la atención del administrador. También se puede obtener información adicional sobre la red mediante pruebas de intrusión periódicas y la comprobación de comportamientos sospechosos a través de SIEM, IPS, IDS.

CONCLUSIÓN

La COVID-19 ha cambiado la forma de trabajar de las empresas, no solo temporalmente durante el transcurso de la pandemia, sino para siempre. Los empresarios deben adaptarse no solo a las exigencias de los empleados que trabajan desde casa ahora, sino también en el futuro.

Una de las cosas que la pandemia nos ha mostrado es que muchos trabajos y tareas que antes se consideraban que requerían empleados en la oficina ahora se considerarán candidatos óptimos para el trabajo a distancia. Pero, para que eso ocurra, los trabajadores remotos necesitan tener un acceso seguro a la oficina. ESET ofrece una variedad de soluciones que pueden ayudar a las empresas a proporcionar un acceso seguro a los recursos corporativos.