FlexPod, la solución a ransomware

FlexPod

NetApp
October 30, 2025

Tabla de contenidos

FlexPod, la solución a ransomware

TR-4802: FlexPod, la solución para ransomware

Arvind Ramakrishnan, NetApp

En colaboración con: 

Para comprender el ransomware, es necesario en primer lugar comprender algunos puntos clave sobre la criptografía. Los métodos criptográficos permiten el cifrado de datos con una clave secreta compartida (cifrado de clave simétrica) o un par de claves (cifrado de claves asimétrico). Una de estas claves es una clave pública ampliamente disponible y la otra es una clave privada no revelada.

El ransomware es un tipo de malware basado en la criptovirología, que es el uso de criptografía para crear software malicioso. Este malware puede utilizar tanto el cifrado simétrico como el cifrado de claves asimétricas para bloquear los datos de una víctima y exigir un rescate para proporcionar la clave para descifrar los datos de la víctima.

¿Cómo funciona el ransomware?

Los siguientes pasos describen cómo el ransomware utiliza la criptografía para cifrar los datos de la víctima sin ningún ámbito para su descifrado o recuperación por parte de la víctima:

1. El atacante genera un par de claves como en el cifrado de claves asimétricas. La clave pública generada se coloca dentro del malware y el malware se libera.
2. Después de que el malware haya entrado en el equipo o sistema de la víctima, genera una clave simétrica aleatoria utilizando un generador de números pseudoorandom (PRNG) o cualquier otro algoritmo viable de generación de números aleatorios.
3. El malware utiliza esta clave simétrica para cifrar los datos de la víctima. Finalmente, cifra la clave simétrica mediante el uso de la clave pública del atacante que se incrustó en el malware. El resultado de este paso es un cifrado asimétrico de la clave simétrica cifrada y el texto cifrado simétrico de los datos de la víctima.
4. El malware borra los datos de la víctima y la clave simétrica que se utilizó para cifrar los datos, sin así dejar margen para la recuperación.
5. La víctima se muestra ahora el texto cifrado asimétrico de la clave simétrica y un valor de rescate que debe pagarse para obtener la clave simétrica que se utilizó para cifrar los datos.
6. La víctima paga el rescate y comparte el cifrado asimétrico con el atacante. El atacante descifra el cifrado con su clave privada, lo que da como resultado la clave simétrica.
7. El atacante comparte esta clave simétrica con la víctima, que se puede utilizar para descifrar todos los datos y, por tanto, recuperarse del ataque.

Retos

Individuos y organizaciones se enfrentan a los siguientes retos cuando son atacados por ransomware:

- El desafío más importante es que se cobra un costo inmediato en la productividad de la organización o del individuo. Toma tiempo para volver a un estado de normalidad, porque todos los archivos importantes deben ser recuperados, y los sistemas deben ser asegurados.
- Podría llevar a una filtración de datos que contenga información confidencial y confidencial de clientes o clientes, y provocar una situación de crisis que una organización querría evitar claramente.
- Existe una gran posibilidad de que los datos entren en las manos equivocadas o se eliminen por completo, lo que conduce a un punto de retorno nulo que podría ser desastroso para las organizaciones y los individuos.
- Después de pagar el rescate, no hay garantía de que el atacante proporcionará la clave para restaurar los datos.
- No hay garantías de que el atacante se abstenga de transmitir los datos delicados a pesar de pagar el rescate.
- En las grandes empresas, identificar la laguna que llevó a un ataque de ransomware es una tarea tediosa, y asegurar todos los sistemas implica un gran esfuerzo.

¿Quién está en riesgo?

Cualquiera puede ser atacado por ransomware, incluidos individuos y organizaciones grandes. Las organizaciones que no aplican medidas y prácticas de seguridad bien definidas son aún más vulnerables a esos ataques. El efecto del ataque en una organización grande puede ser varias veces mayor de lo que un individuo podría soportar.

El ransomware representa aproximadamente el 28 % de todos los ataques de malware. En otras palabras, más de uno de cada cuatro incidentes de malware es un ataque de ransomware. El ransomware puede propagarse automática e indiscriminadamente a través de Internet y, cuando hay un lapso de seguridad, puede entrar en los sistemas de la víctima y continuar extendiéndose a otros sistemas conectados. Los atacantes tienden a dirigirse a personas u organizaciones que realizan un gran uso compartido de archivos, tienen una gran cantidad de datos confidenciales y críticos o a mantener una protección inadecuada frente a ataques.

Los atacantes tienden a centrarse en los siguientes objetivos potenciales:

- Universidades y comunidades estudiantiles
- Oficinas y organismos gubernamentales
- Hospitales
- De Estados Unidos

Esta no es una lista exhaustiva de objetivos. Usted no puede considerarse seguro de los ataques si se encuentra fuera de una de estas categorías.

¿Cómo se introduce el ransomware en un sistema o se distribuye?

Existen varias formas en las que el ransomware puede entrar en un sistema o propagarse a otros sistemas. En el mundo actual, casi todos los sistemas están conectados entre sí a través de Internet, LAN, WAN, etc. La cantidad de datos que se generan e intercambian entre estos sistemas no hace más que aumentar.

Algunos de los métodos más comunes mediante los que se puede distribuir el ransomware incluyen métodos que utilizamos diariamente para compartir o acceder a los datos:

- Correo electrónico

- Redes P2P
- Descargas de archivos
- Redes sociales
- Dispositivos móviles
- Conectarse a redes públicas no seguras
- Acceso a direcciones URL Web

Consecuencias de la pérdida de datos

Las consecuencias o los efectos de la pérdida de datos pueden ser más amplios de lo que las organizaciones podrían anticipar. Los efectos pueden variar en función de la duración del tiempo de inactividad o del período de tiempo durante el cual una organización no tiene acceso a sus datos. Cuanto más dure el ataque, mayor será el efecto sobre los ingresos, la Marca y la reputación de la organización. Una organización también puede enfrentarse a problemas legales y a una fuerte disminución de la productividad.

A medida que estas cuestiones continúan persistiéndose con el tiempo, comienzan a magnificar y podrían terminar cambiando la cultura de una organización, dependiendo de cómo responda al ataque. En el mundo actual, la información se propaga rápidamente y las noticias negativas sobre una organización podrían causar un daño permanente a su reputación. Una organización podría enfrentarse a enormes sanciones por pérdida de datos, lo que podría desembocar en el cierre de un negocio.

Efectos financieros

Según un informe reciente "Informe de McAfee", Los costos globales incurridos por el crimen cibernético son aproximadamente 600 mil millones de dólares, lo que representa aproximadamente el 0.8% del PIB global. Cuando esta cantidad se compara con la creciente economía mundial de internet de 4.2 billones de dólares, equivale a un impuesto del 14% sobre el crecimiento.

El ransomware asume una parte importante de este coste financiero. En 2018, los costos incurridos debido a los ataques de ransomware fueron aproximadamente de $8 mil millones—una cantidad que se prevé que alcanzará los $11.5 mil millones en 2019.

¿Cuál es la solución?

La recuperación a partir de un ataque de ransomware con un tiempo de inactividad mínimo solo es posible gracias a la implementación de un plan de recuperación ante desastres proactivo. Tener la capacidad para recuperarse de un ataque es bueno, pero evitar un ataque es ideal.

Aunque hay varios frentes que se deben revisar y reparar para evitar un ataque, el componente central que permite prevenir o recuperar de un ataque es el centro de datos.

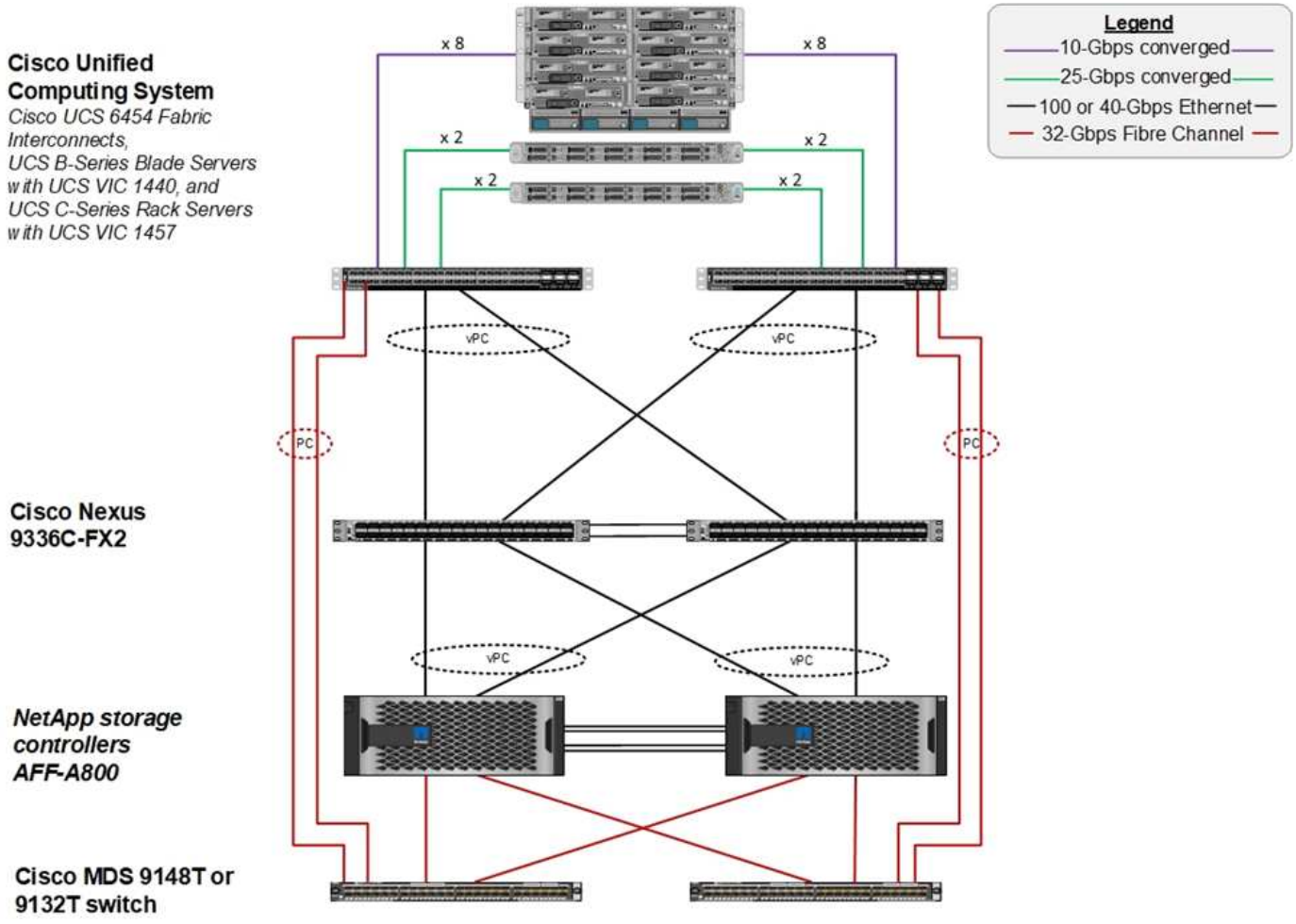
El diseño del centro de datos y las funciones que proporciona para proteger los puntos finales de red, informática y almacenamiento tienen un papel fundamental a la hora de crear un entorno seguro para las operaciones cotidianas. Este documento muestra cómo las funciones de una infraestructura de cloud híbrido de FlexPod pueden ayudar a lograr una recuperación de datos rápida en caso de ataque, y también pueden ayudar a evitar ataques.

Información general de FlexPod

FlexPod es una arquitectura prediseñada, integrada y validada que combina servidores Cisco Unified Computing System (Cisco UCS), la familia de switches Cisco Nexus,

switches estructurales Cisco MDS y cabinas de almacenamiento de NetApp en una sola arquitectura flexible. Las soluciones FlexPod están diseñadas para ofrecer alta disponibilidad sin puntos únicos de error, a la vez que mantienen la rentabilidad y la flexibilidad del diseño necesarias para acomodar una amplia variedad de cargas de trabajo. Un diseño de FlexPod puede admitir diferentes hipervisores y servidores con configuración básica, y también puede dimensionarse y optimizarse según los requisitos de carga de trabajo de los clientes.

La siguiente figura muestra la arquitectura de FlexPod y destaca claramente la alta disponibilidad en todas las capas de la pila. Los componentes de la infraestructura de almacenamiento, red y computación se configuran de forma que las operaciones se pueden conmutar al respaldo instantáneamente al partner superviviente en caso de que uno de los componentes falle.



Una ventaja importante para un sistema FlexPod es que está diseñado, integrado y validado para varias cargas de trabajo. Se publican guías detalladas de diseño e instalación para cada validación de soluciones. Estos documentos incluyen las prácticas recomendadas que debe emplear para que las cargas de trabajo se ejecuten sin problemas en FlexPod. Estas soluciones se han creado con los mejores productos de informática, red y almacenamiento de su clase y con una gran cantidad de funciones centradas en la seguridad y el endurecimiento de toda la infraestructura.

"El índice de inteligencia de amenazas X-Force de IBM" estados, “error humano responsable de dos tercios de los registros comprometidos, incluido un aumento histórico del 424% en infraestructura de nube mal configurada”.

Con un sistema FlexPod, puede evitar una configuración incorrecta de su infraestructura mediante los libros de estrategia de Ansible que realizan una configuración integral de la infraestructura de acuerdo con las mejores prácticas descritas en los diseños validados por Cisco (CVD) y las arquitecturas verificadas de NetApp (NVA).

Medidas de protección contra ransomware

En esta sección se describen las funciones clave del software de gestión de datos ONTAP de NetApp y las herramientas para Cisco UCS y Cisco Nexus que puede usar para proteger y recuperar datos de forma efectiva de ataques de ransomware.

Almacenamiento: ONTAP de NetApp

El software ONTAP ofrece muchas funciones útiles para la protección de datos, la mayoría de las cuales son gratuitas para los clientes que tienen un sistema ONTAP. Puede utilizar las siguientes funciones en todo momento para proteger los datos de los ataques:

- **Tecnología Snapshot de NetApp.** una copia snapshot es una imagen de solo lectura de un volumen que captura el estado de un sistema de archivos en un momento dado. Estas copias ayudan a proteger los datos sin afectar el rendimiento del sistema y, al mismo tiempo, no ocupan mucho espacio de almacenamiento. NetApp recomienda crear un programa para la creación de copias Snapshot. Usted también debe mantener un largo período de retención porque algunos malware pueden permanecer inactivos y luego reactivar semanas o meses después de una infección. En caso de ataque, es posible revertir el volumen utilizando una copia snapshot que se había realizado antes de la infección.
- **Tecnología SnapRestore de NetApp.** el software de recuperación de datos SnapRestore es extremadamente útil para la recuperación de datos dañados o para revertir únicamente el contenido del archivo. SnapRestore no revierte los atributos de un volumen; es mucho más rápido de lo que puede conseguir un administrador al copiar los archivos de la copia snapshot al sistema de archivos activo. La velocidad a la que se pueden recuperar los datos resulta útil cuando se deben recuperar muchos archivos lo antes posible. En caso de ataque, este eficiente proceso de recuperación ayuda a que el negocio vuelva a estar online rápidamente.
- **La tecnología SnapCenter de NetApp.** el software SnapCenter utiliza funciones de backup y replicación basadas en almacenamiento de NetApp para proporcionar una protección de datos coherente con las aplicaciones. Este software se integra con aplicaciones empresariales y proporciona flujos de trabajo específicos para aplicaciones y bases de datos para satisfacer las necesidades de los administradores de aplicaciones, bases de datos e infraestructuras virtuales. SnapCenter proporciona una plataforma empresarial fácil de usar para coordinar y administrar de un modo seguro la protección de datos en aplicaciones, bases de datos y sistemas de archivos. Su capacidad de proporcionar protección de datos coherente con las aplicaciones es fundamental durante la recuperación de datos, ya que facilita la restauración de las aplicaciones a un estado coherente con mayor rapidez.
- **La tecnología SnapLock de NetApp.** SnapLock proporciona un volumen para finalidades especiales en el que los archivos se pueden almacenar y poner en un estado en el que no se pueden borrar ni sobrescribir. Los datos de producción del usuario que se encuentran en un volumen FlexVol se pueden duplicar o realizar copias vault en un volumen SnapLock mediante la tecnología SnapMirror o SnapVault de NetApp, respectivamente. Los archivos del volumen de SnapLock, el volumen en sí y su agregado de alojamiento no se pueden eliminar hasta que finalice el período de retención.
- **Tecnología FPolicy de NetApp.** Utilice el software FPolicy para evitar ataques al desactivar las operaciones en archivos con extensiones específicas. Es posible activar un evento de FPolicy para operaciones de archivos específicas. El evento está ligado a una política, que llama al motor que necesita utilizar. Puede configurar una política con un conjunto de extensiones de archivo que potencialmente puedan contener ransomware. Cuando un archivo con una extensión no permitida intenta realizar una

operación no autorizada, FPolicy impide que esa operación se ejecute.

Red: Cisco Nexus

El software Cisco NX OS admite la función NetFlow que permite una detección mejorada de anomalías y seguridad de la red. NetFlow captura los metadatos de cada conversación de la red, las partes implicadas en la comunicación, el protocolo utilizado y la duración de la transacción. Una vez agregada y analizado la información, puede proporcionar una visión del comportamiento normal.

Los datos recopilados también permiten la identificación de patrones de actividad cuestionables, como el malware que se propaga a través de la red, lo que de otra manera puede pasar desapercibida.

NetFlow utiliza flujos para proporcionar estadísticas para la supervisión de la red. Un flujo es un flujo unidireccional de paquetes que llega a una interfaz de origen (o VLAN) y tiene los mismos valores para las claves. Una clave es un valor identificado para un campo dentro del paquete. Puede crear un flujo utilizando un registro de flujo para definir las claves únicas para su flujo. Puede exportar los datos que NetFlow recopila para sus flujos utilizando un exportador de flujo a un colector NetFlow remoto, como Cisco StealtWatch. StealtWatch utiliza esta información para la supervisión continua de la red y proporciona información forense de respuesta a incidentes y detección de amenazas en tiempo real si se produce un brote de ransomware.

Computación: Cisco UCS

Cisco UCS es el extremo de computación en una arquitectura de FlexPod. Puede usar varios productos de Cisco que pueden ayudar a proteger esta capa de la pila en el nivel del sistema operativo.

Puede implementar los siguientes productos clave en la capa informática o de aplicación:

- **Cisco Advanced Malware Protection (AMP) para endpoints.** compatible con los sistemas operativos Microsoft Windows y Linux, esta solución integra capacidades de prevención, detección y respuesta. Este software de seguridad evita infracciones, bloquea el malware en el punto de entrada y supervisa y analiza continuamente la actividad de los archivos y procesos para detectar, contener y resolver rápidamente amenazas que puedan evadir las defensas de primera línea.

  El componente de Protección de actividad maliciosa (MAP) de AMP supervisa continuamente todas las actividades de los extremos y proporciona detección en tiempo de ejecución y bloqueo del comportamiento anormal de un programa en ejecución en el punto final. Por ejemplo, cuando el comportamiento del punto final indica ransomware, los procesos ofensor se terminan, lo que impide el cifrado del punto final y detiene el ataque.

- **Cisco Advanced Malware Protection for Email Security.** los correos electrónicos se han convertido en el vehículo principal para propagar malware y llevar a cabo ciberataques. En promedio, aproximadamente 100 mil millones de correos electrónicos se intercambian en un solo día, lo que proporciona a los atacantes un excelente vector de penetración en los sistemas de los usuarios. Por lo tanto, es absolutamente esencial defender contra esta línea de ataque.

  AMP analiza correos electrónicos para amenazas tales como exploits de día cero y malware sigiloso ocultos en archivos adjuntos maliciosos. También utiliza la inteligencia de URL líder en el sector para combatir enlaces maliciosos. Proporciona a los usuarios protección avanzada contra el phishing espear, el ransomware y otros ataques sofisticados.

- **Sistema de prevención de intrusiones de próxima generación (NGIPS).** Cisco Firepower NGIPS se puede implementar como un dispositivo físico en el centro de datos o como un dispositivo virtual en VMware (NGIPSv para VMware). Este sistema altamente eficaz de prevención de intrusiones proporciona un rendimiento fiable y un costo total de propiedad bajo. La protección contra amenazas se puede ampliar con licencias de suscripción opcionales para proporcionar funciones de AMP, visibilidad y control de

aplicaciones y filtrado de URL. La virtualización de NGIPS inspecciona el tráfico entre equipos virtuales (VM) y facilita la implementación y gestión de soluciones de NGIPS en sitios con recursos limitados, lo que aumenta la protección tanto para activos físicos como virtuales.

Proteja y recupere datos en FlexPod

En esta sección se describe cómo se pueden recuperar los datos de un usuario final en caso de un ataque y cómo se pueden prevenir los ataques mediante un sistema FlexPod.

Resumen de banco

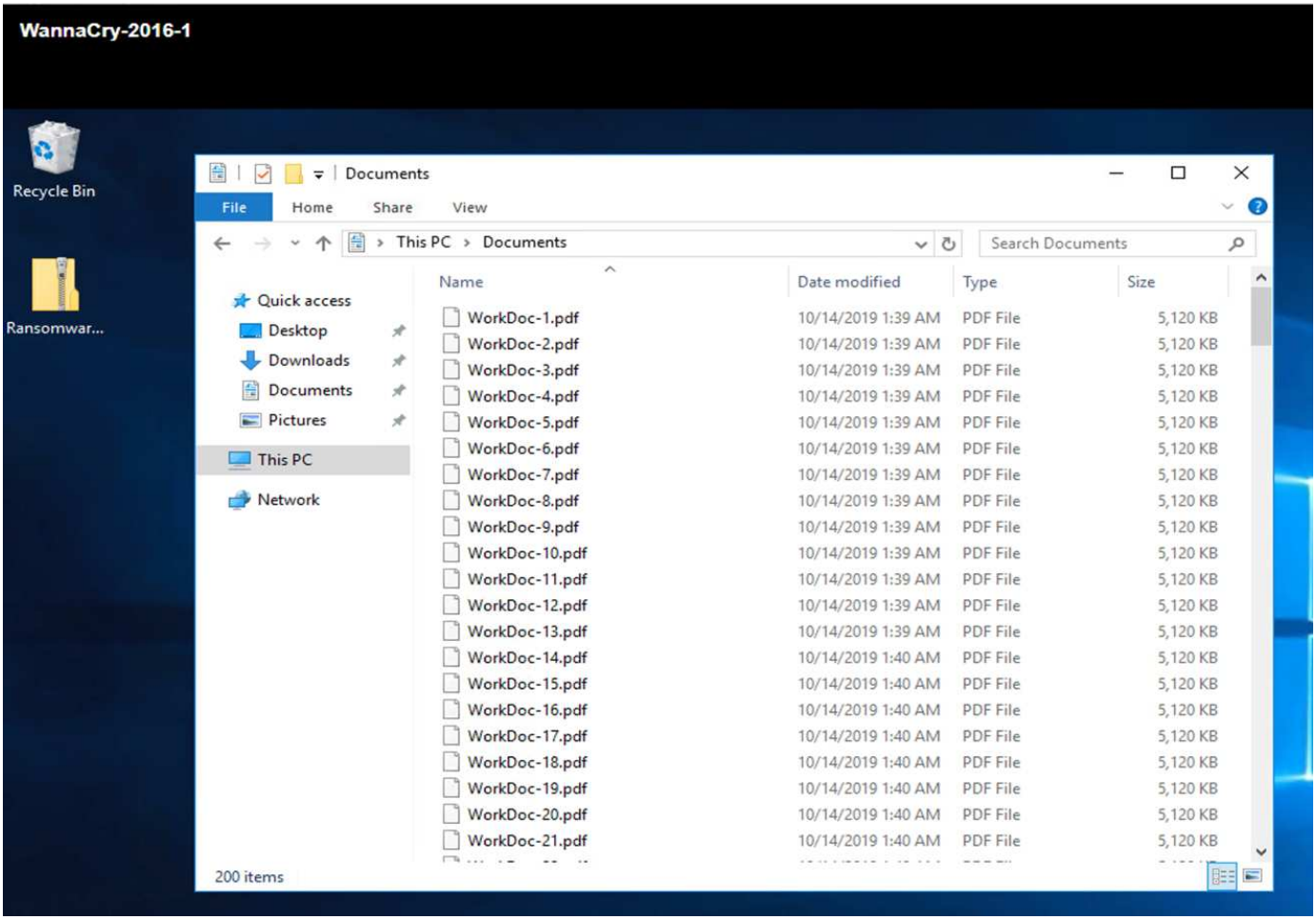
Para presentar la detección, la corrección y la prevención de FlexPod, se creó un banco de pruebas basado en las directrices especificadas en el último CVD de plataforma disponible en el momento en el que se escribió este documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS de cuarta generación y NetApp AFF A-Series CVD".

Se puso en marcha un equipo virtual con Windows 2016, que proporcionaba un recurso compartido CIFS del software ONTAP de NetApp, en la infraestructura de VMware vSphere. A continuación, se configuró FPolicy de NetApp en el recurso compartido de CIFS para evitar la ejecución de archivos con ciertos tipos de extensiones. El software SnapCenter de NetApp también se puso en marcha para gestionar las copias Snapshot de los equipos virtuales de la infraestructura para proporcionar copias Snapshot coherentes con las aplicaciones.

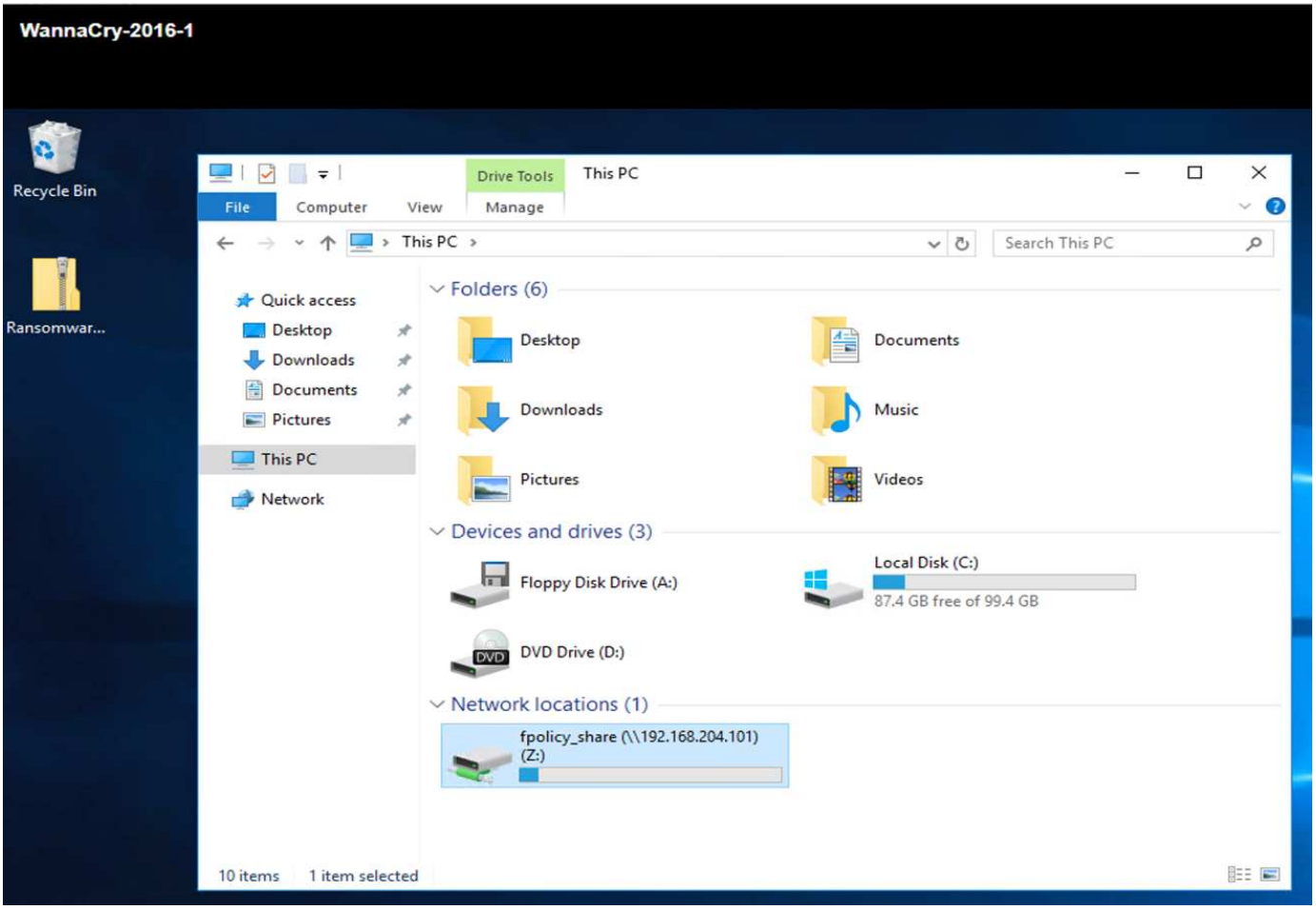
Estado del equipo virtual y sus archivos antes de un ataque

En esta sección se muestra el estado de los archivos antes de un ataque a la máquina virtual y al recurso compartido CIFS que se le ha asignado.

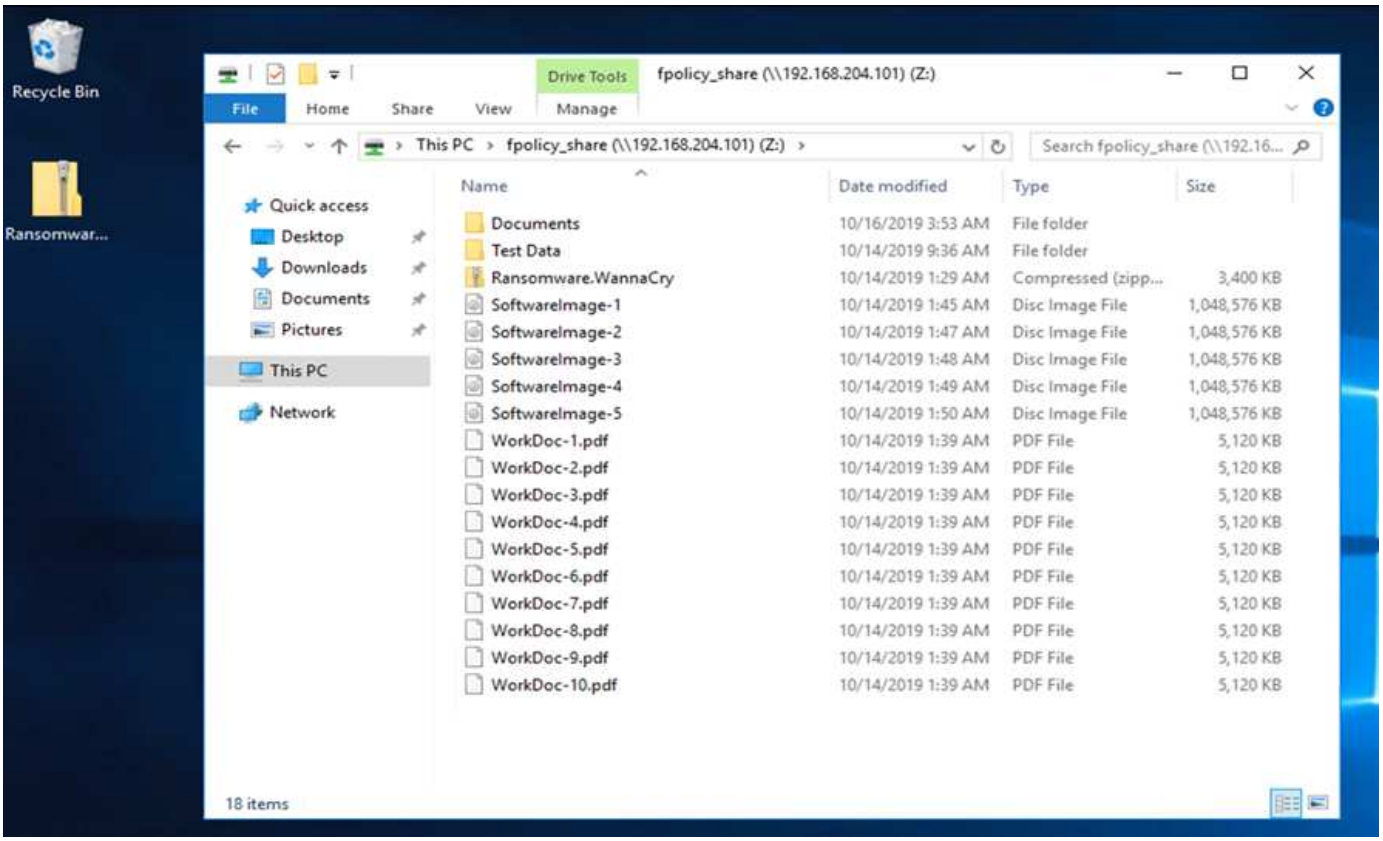
La carpeta Documentos del equipo virtual tenía un conjunto de archivos PDF que todavía no han sido cifrados por el malware WannaCry.



La siguiente captura de pantalla muestra el recurso compartido de CIFS asignado a la máquina virtual.



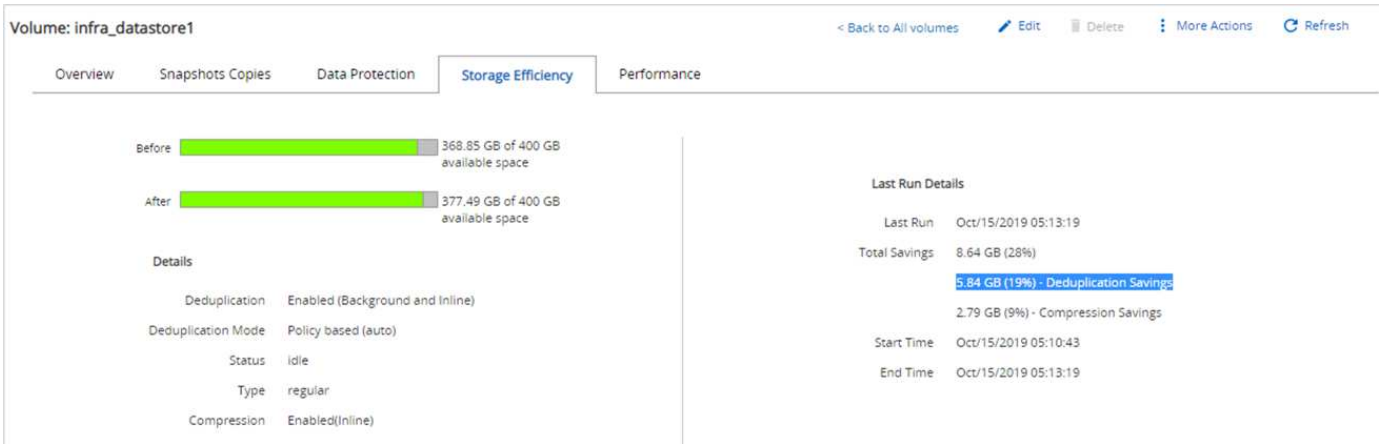
La siguiente captura de pantalla muestra los archivos del recurso compartido CIFS `fpolicy_share` Que todavía no han sido cifrados por el malware WannaCry.



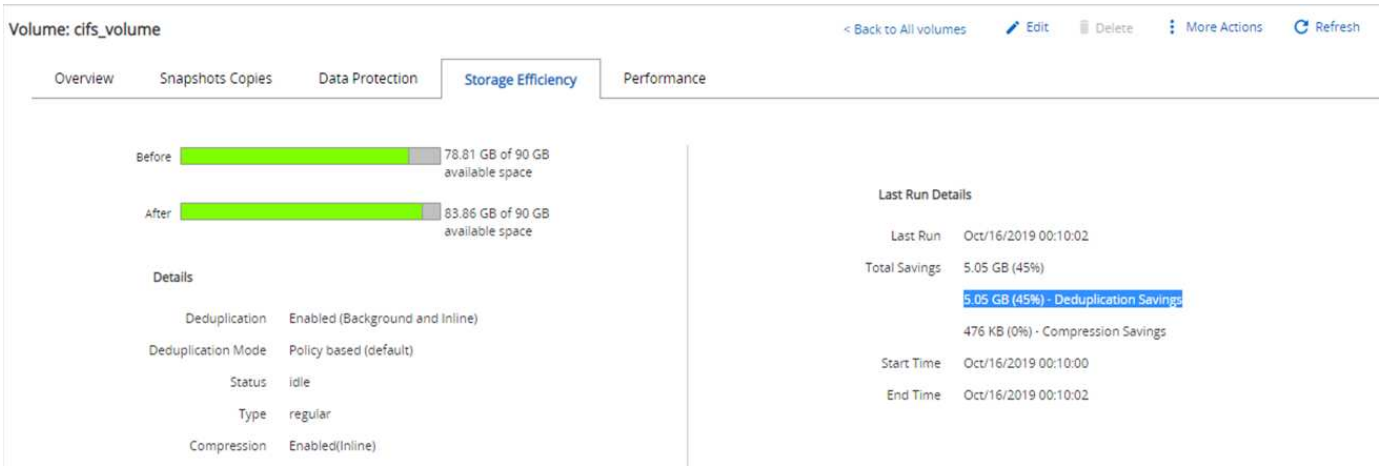
Información sobre deduplicación y copias snapshot antes de un ataque

Los detalles de la eficiencia del almacenamiento y el tamaño de la copia Snapshot antes de un ataque se indican y se utilizan como referencia durante la fase de detección.

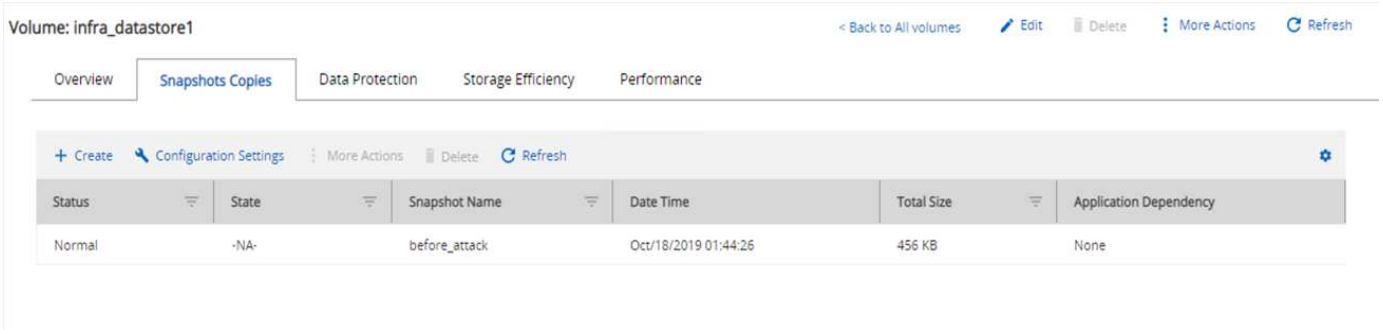
Se obtuvo un ahorro del 19% en el almacenamiento, gracias a la deduplicación en el volumen que alojaba el equipo virtual.



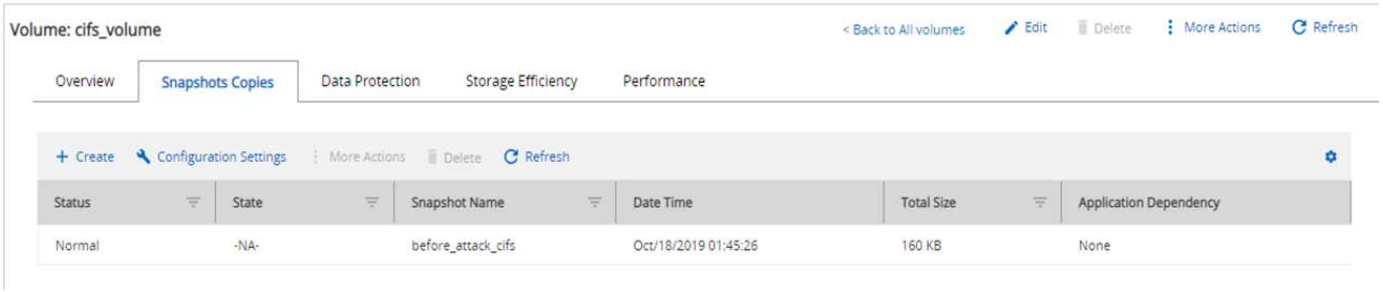
Se obtuvo un ahorro del 45% gracias a la deduplicación en la unidad CIFS `fpolicy_share`.



Se observó un tamaño de copia snapshot de 456 KB para el volumen donde se alojaba el equipo virtual.



Se observó un tamaño de copia Snapshot de 160 KB para el recurso compartido de CIFS `fpolicy_share`.



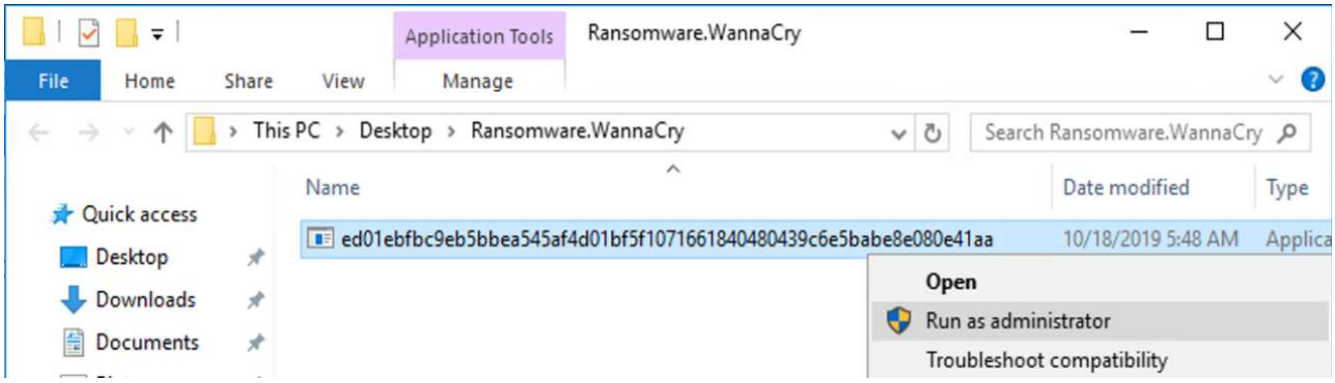
Infección de WannaCry en VM y recursos compartidos de CIFS

En esta sección, mostramos cómo se introdujo el malware de WannaCry en el entorno de FlexPod y los posteriores cambios en el sistema que se observaron.

Los pasos siguientes muestran cómo se introdujo el binario de malware WannaCry en el equipo virtual:

1. Se extrajo el malware protegido.

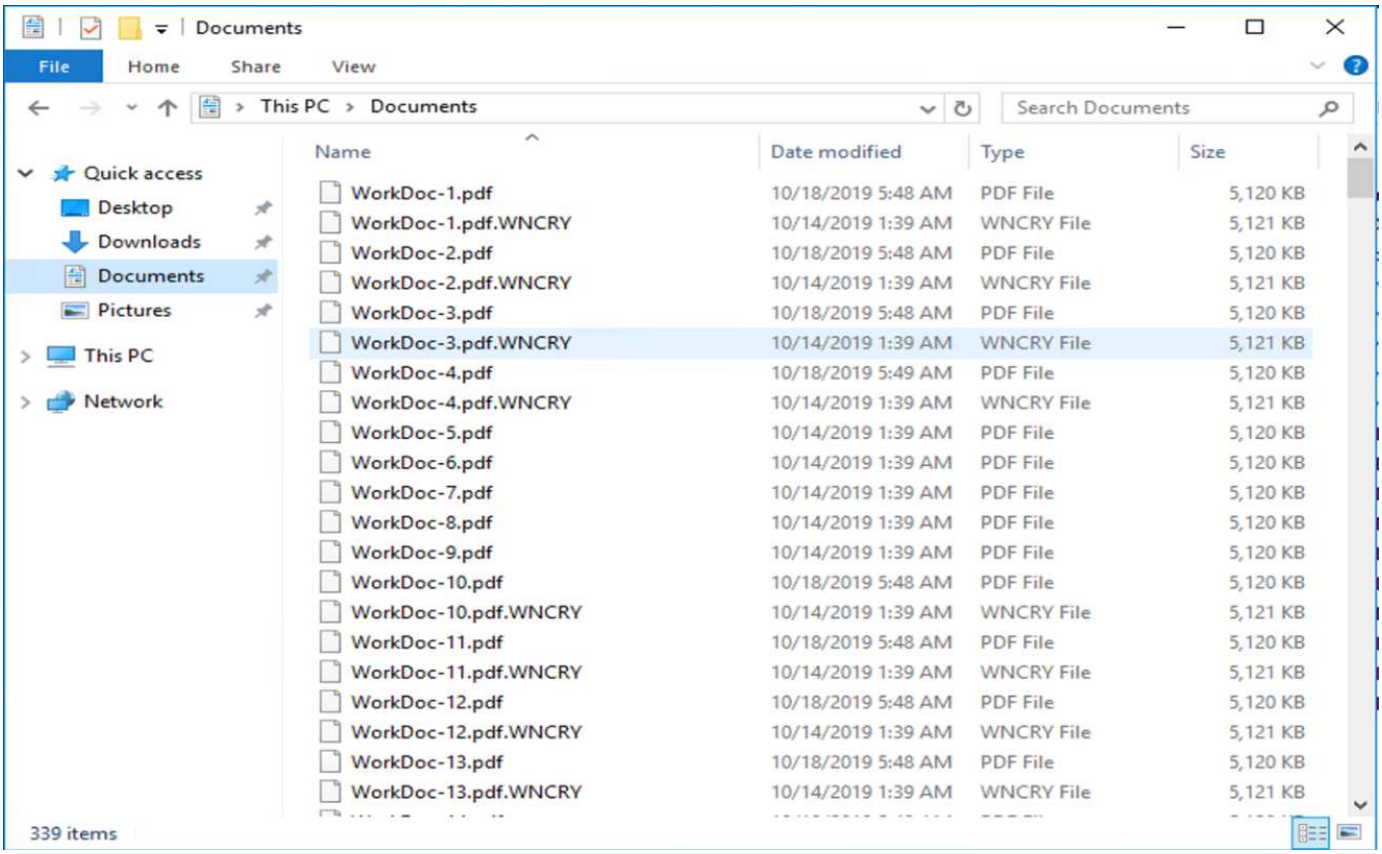
2. Se ejecutó el binario.



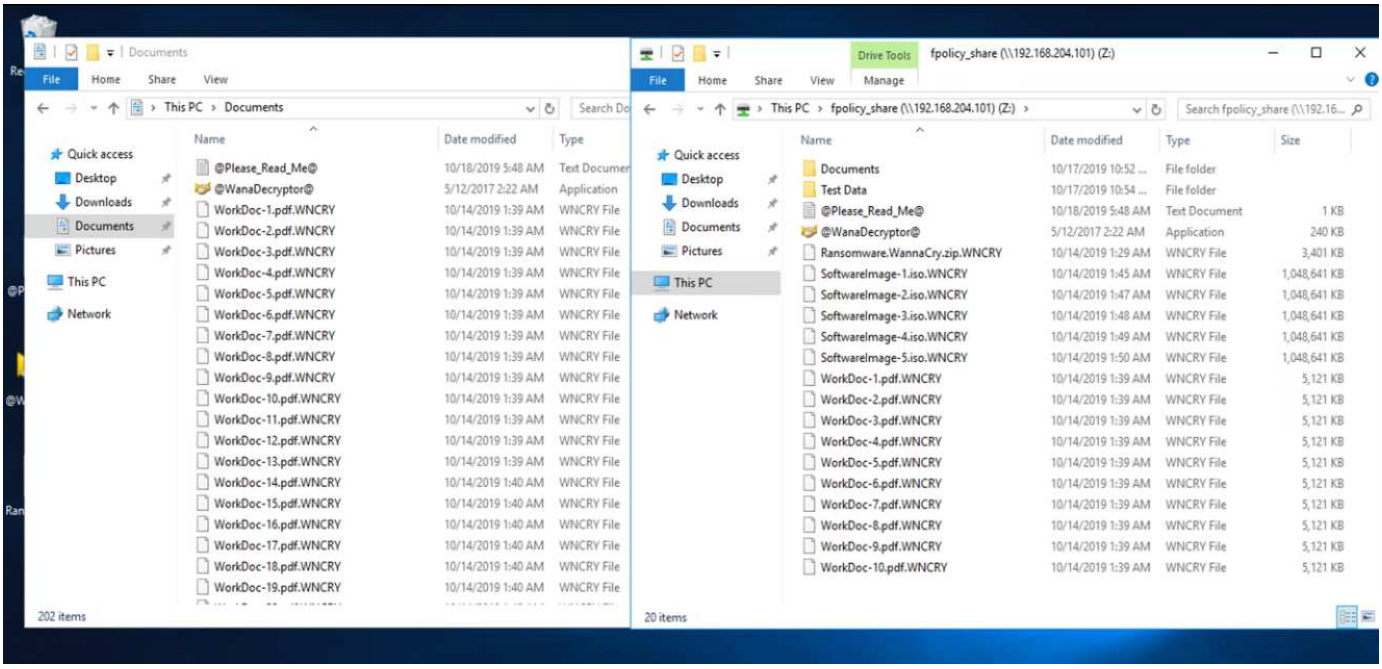
Caso 1: WannaCry cifra el sistema de archivos dentro del equipo virtual y el recurso compartido CIFS asignado

El sistema de archivos local y el recurso compartido CIFS asignado fueron cifrados por el malware WannaCry.

El malware comienza a cifrar archivos con extensiones WNCRY.



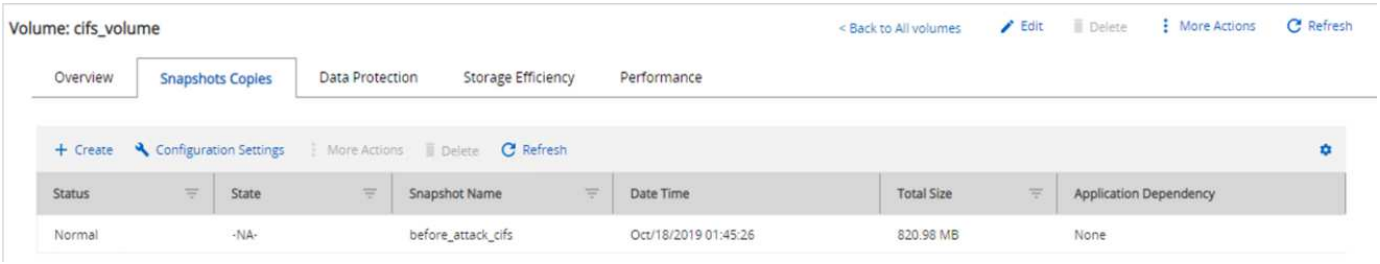
El malware cifra todos los archivos del equipo virtual local y del recurso compartido asignado.



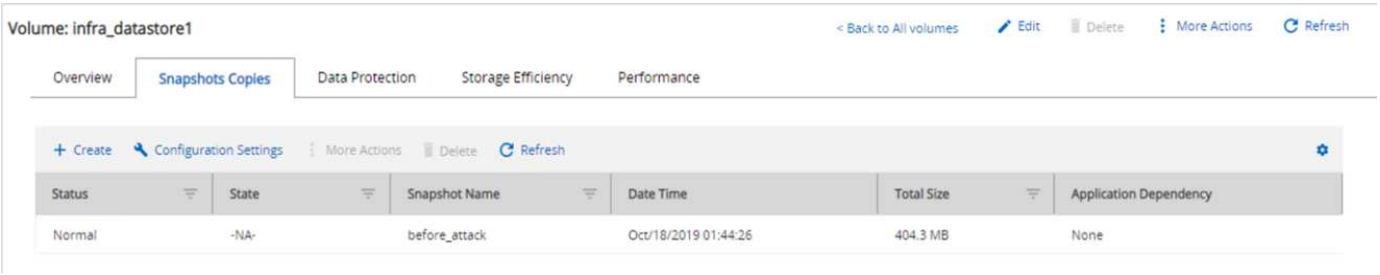
Detección

Desde el momento en que el malware comenzó a cifrar los archivos, se activó un aumento exponencial del tamaño de las copias snapshot y una reducción exponencial del porcentaje de eficiencia del almacenamiento.

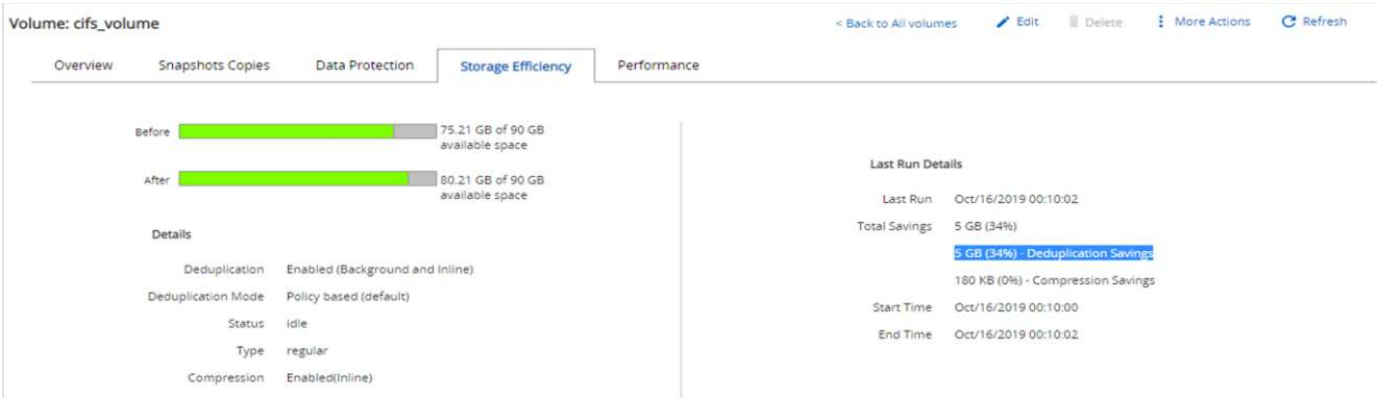
Se detectó un aumento espectacular del tamaño de snapshot a 820,98 MB para el volumen que aloja la unidad CIFS durante el ataque.



Hemos detectado un aumento en el tamaño de la copia snapshot a 404,3 MB para el volumen donde se aloja la máquina virtual.



La eficiencia de almacenamiento para el volumen que aloja la unidad CIFS se redujo a un 34 %.



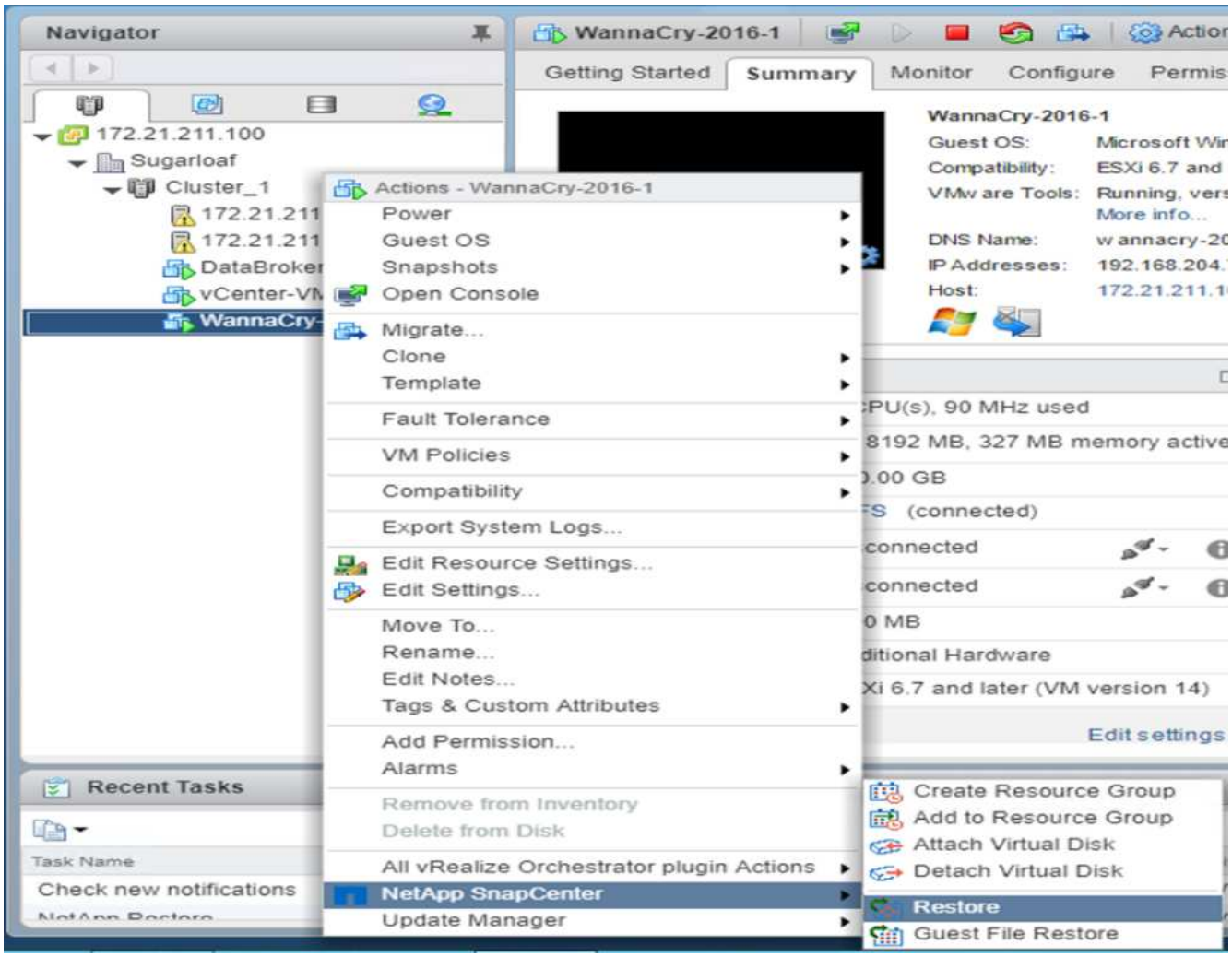
Reparación

Restaurar el equipo virtual y el recurso compartido CIFS asignado mediante una copia Snapshot limpia creada antes del ataque

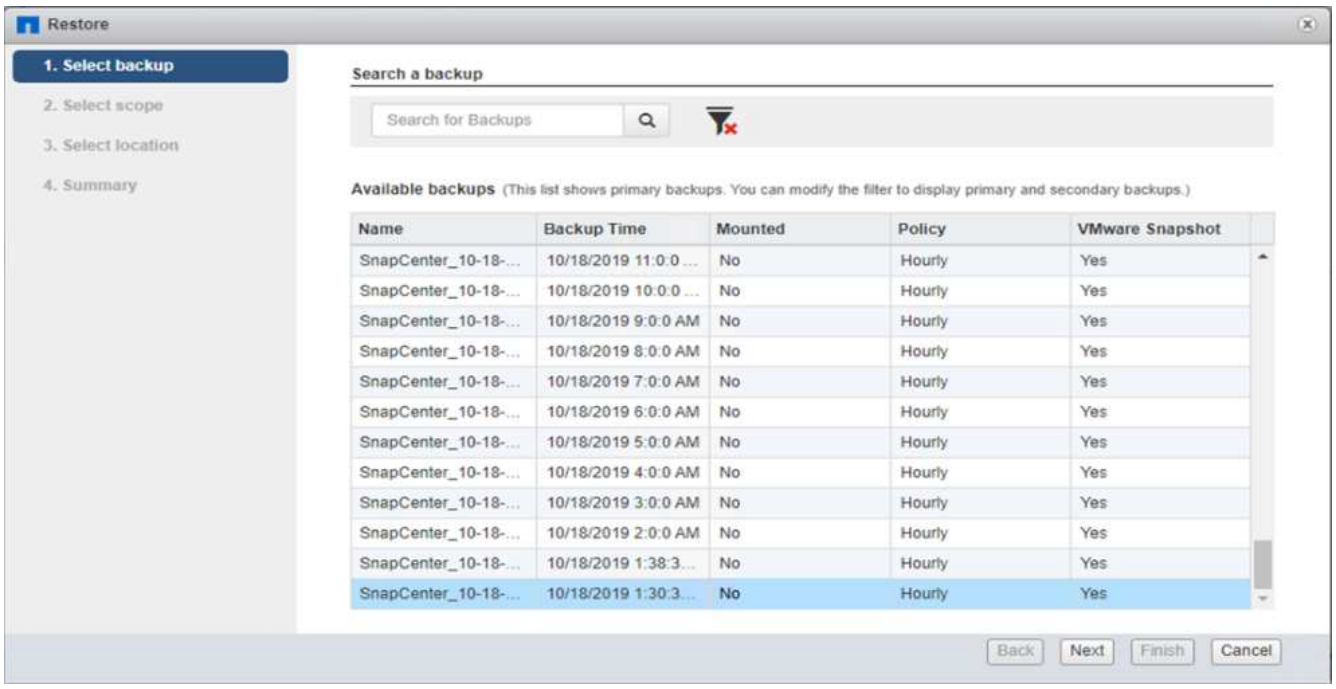
Restaurar VM

Para restaurar el equipo virtual, complete los siguientes pasos:

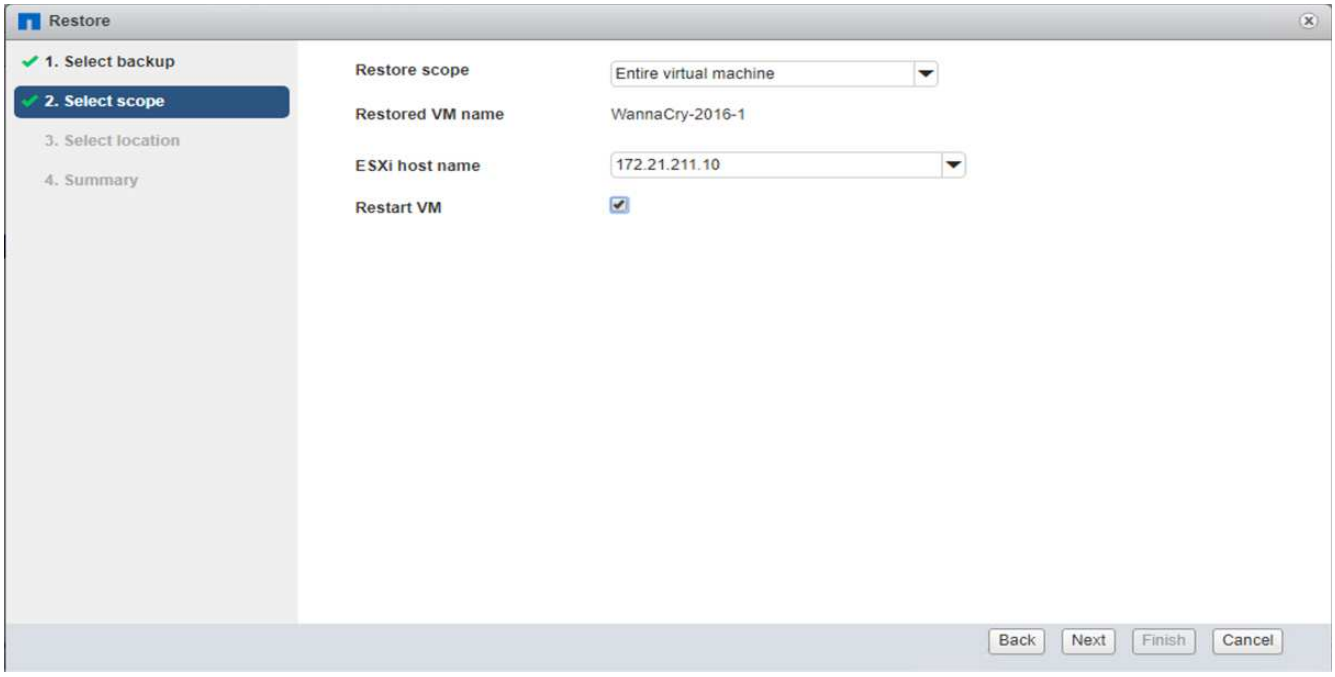
1. Use la copia Snapshot que creó con SnapCenter para restaurar la máquina virtual.



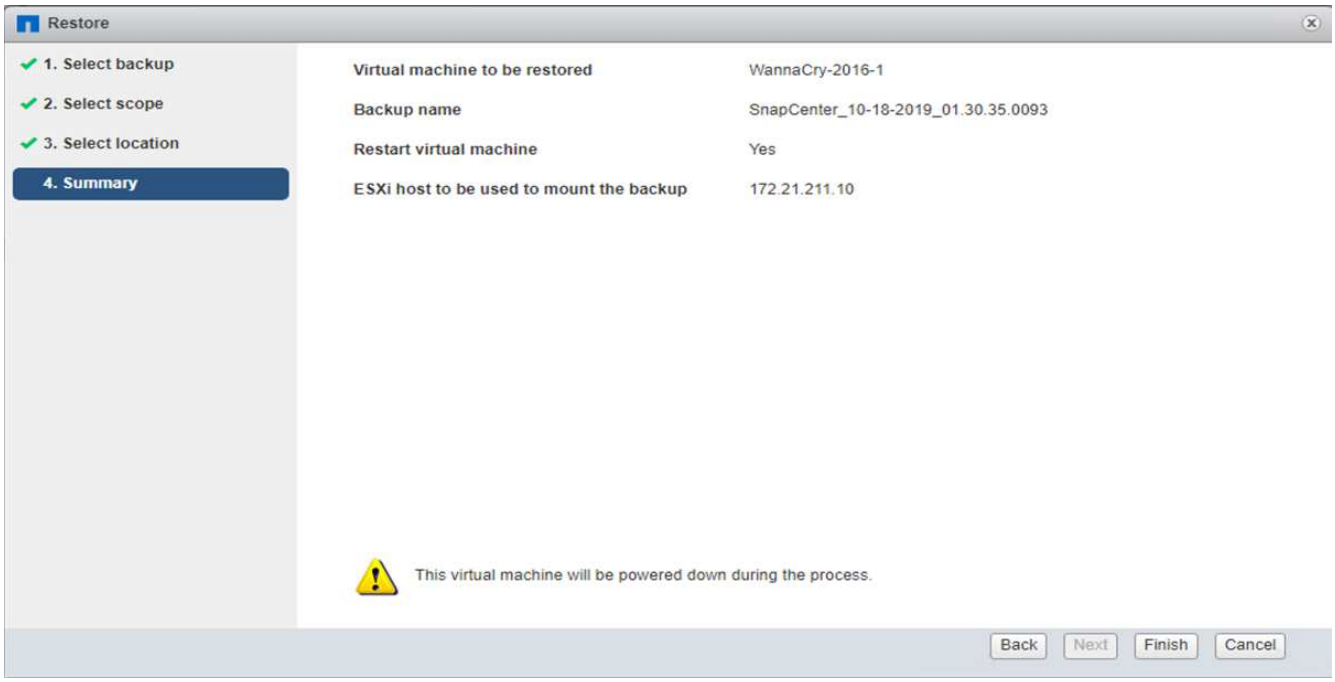
2. Seleccione la copia de Snapshot coherente con VMware que desee restaurar.



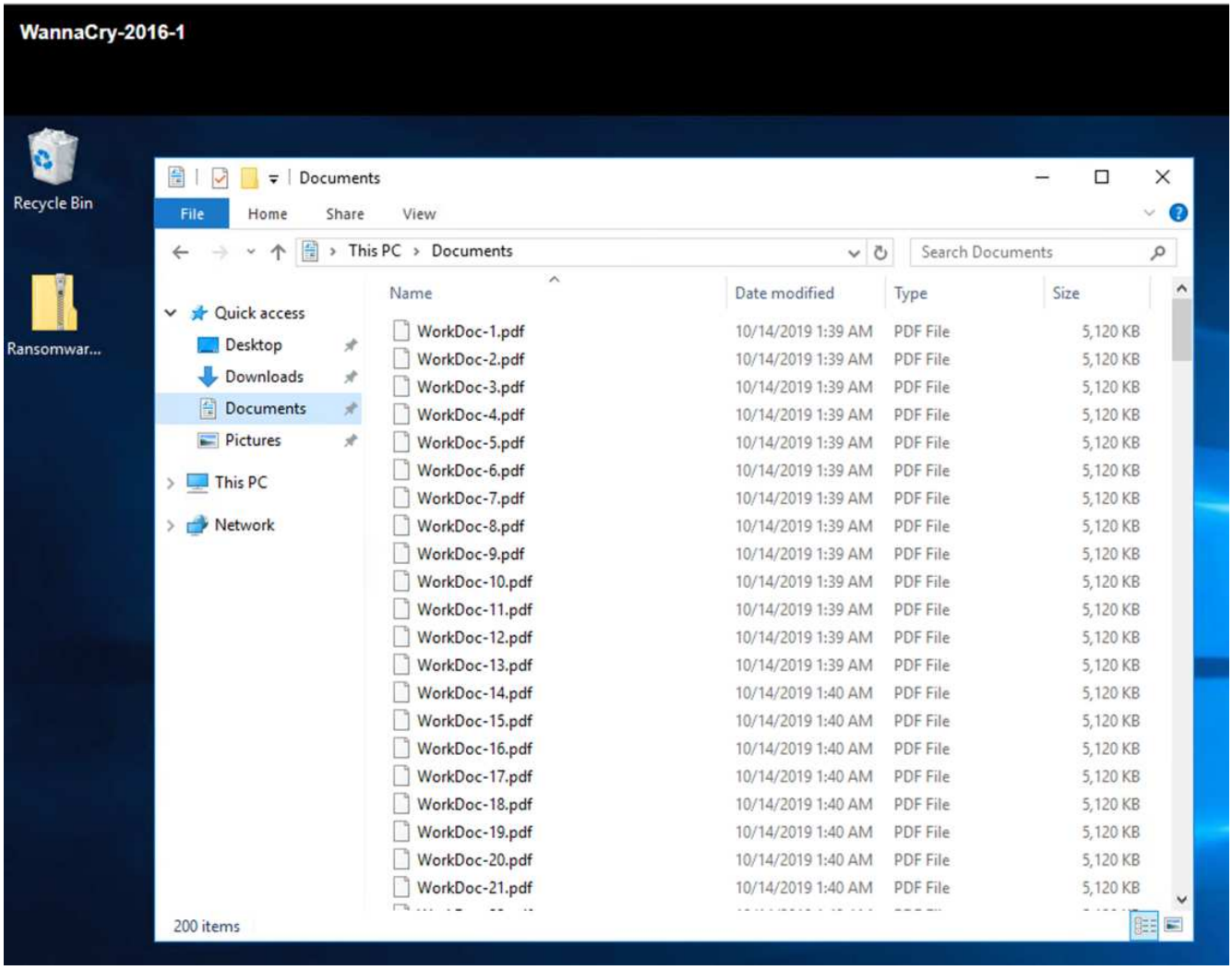
3. Toda la máquina virtual se restaura y se reinicia.



4. Haga clic en Finalizar para iniciar el proceso de restauración.



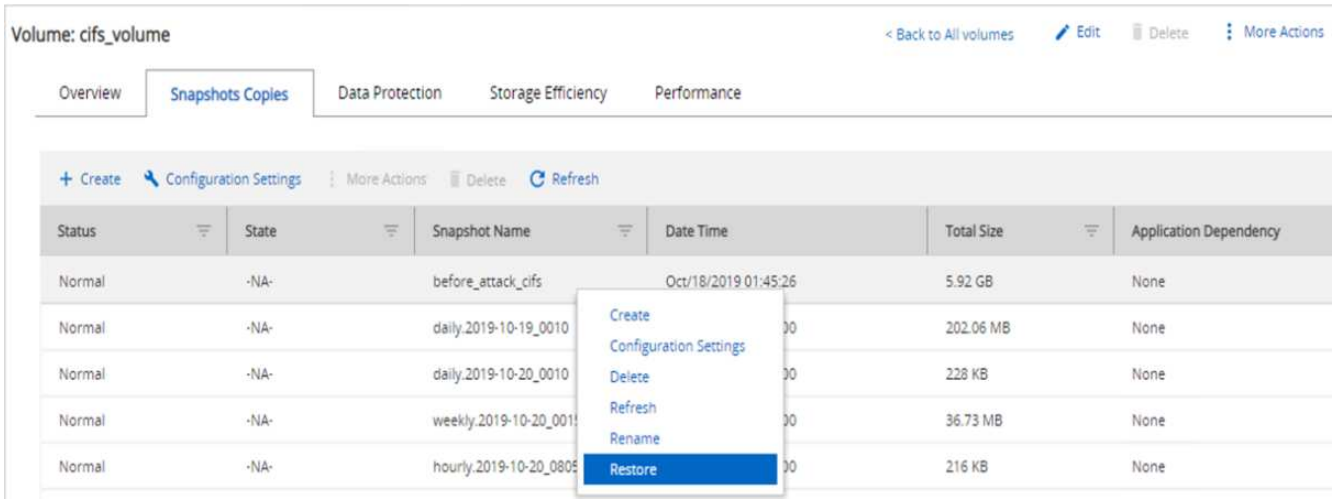
5. Se restauran el equipo virtual y sus archivos.



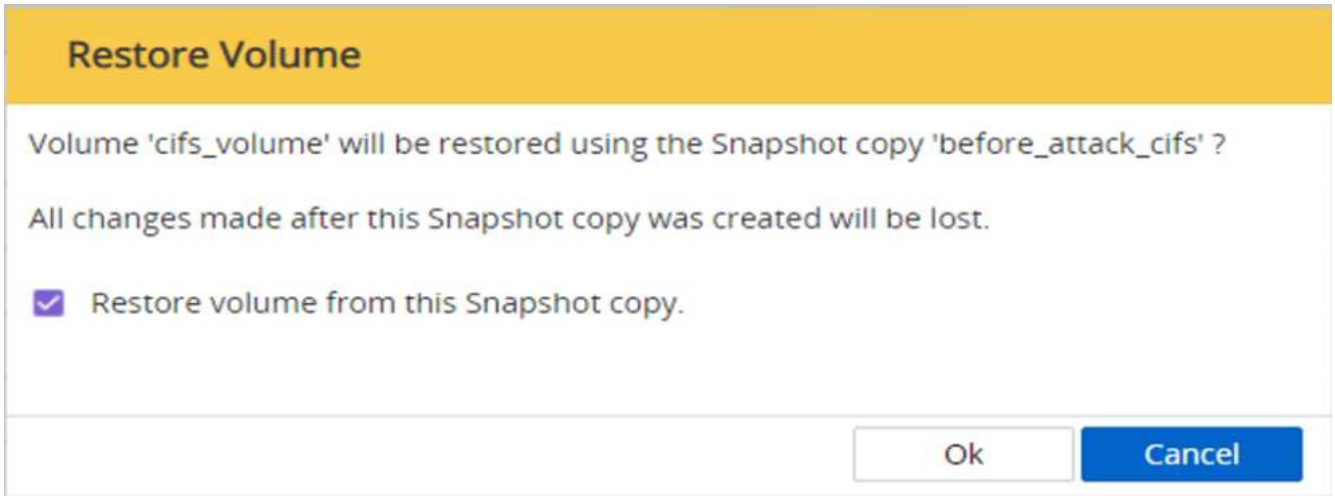
Restaurar recurso compartido CIFS

Para restaurar el recurso compartido CIFS, realice los siguientes pasos:

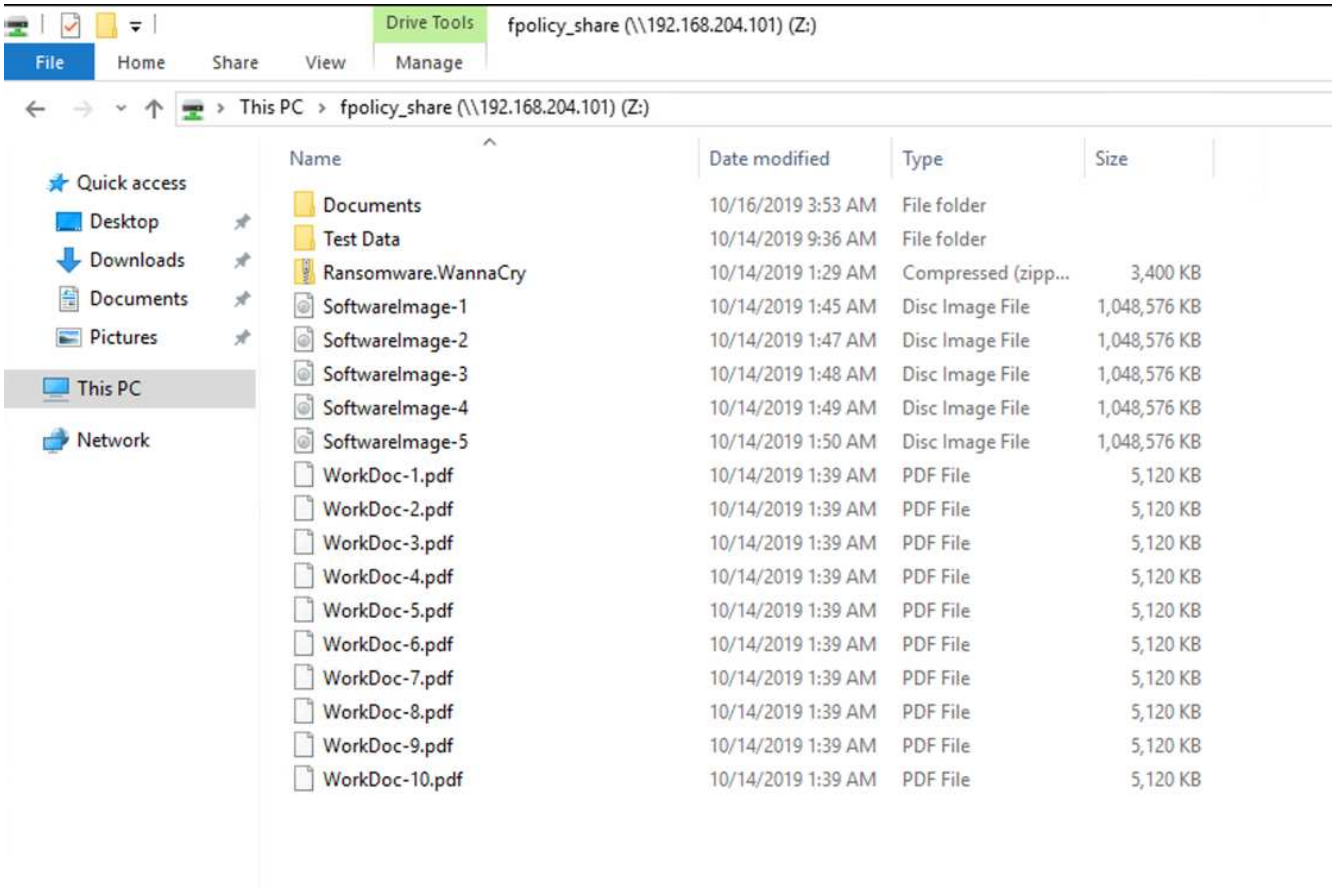
1. Utilice la copia snapshot del volumen que haya tomado antes del ataque para restaurar el recurso compartido.



2. Haga clic en OK para iniciar la operación de restauración.



3. Vea el recurso compartido CIFS después de la restauración.



Caso 2: WannaCry cifra el sistema de archivos dentro del equipo virtual e intenta cifrar el recurso compartido CIFS asignado que está protegido mediante FPolicy

Prevención

Configurar FPolicy

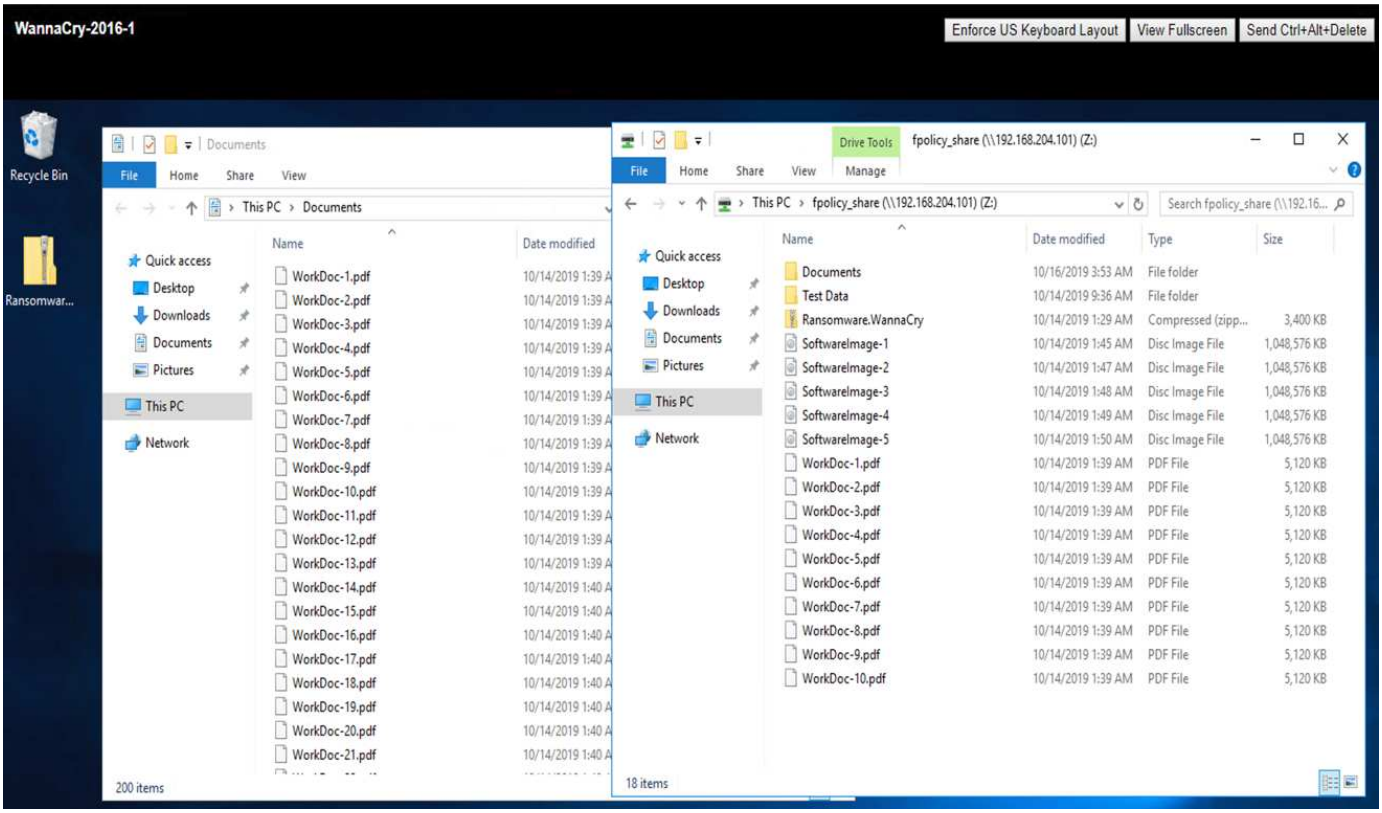
Para configurar FPolicy en el recurso compartido de CIFS, ejecute los siguientes comandos en el clúster de

ONTAP:

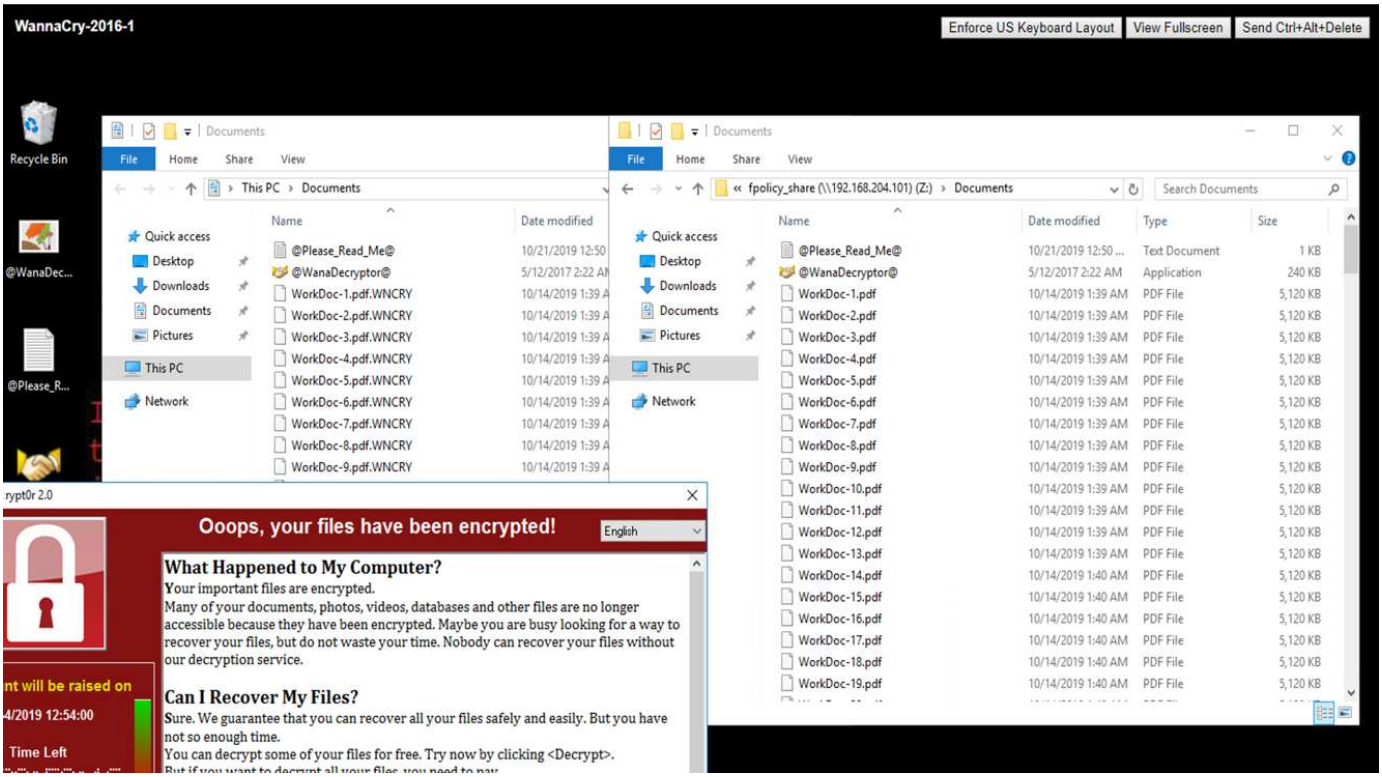
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -vserver infra_svm -policy-name
Ransomware_policy -shares-to-include fpolicy_share -file-extensions-to
-include WNCRY,Locky,ad4c
vserver fpolicy enable -vserver infra_svm -policy-name Ransomware_policy
-sequence-number 1
```

Con esta directiva, los archivos con extensiones WNCRY, Locky y ad4c no pueden realizar las operaciones de archivo crear, cambiar el nombre, escribir o abrir.

Ver el estado de los archivos antes del ataque: Están sin cifrar y en un sistema limpio.



Los archivos del equipo virtual están cifrados. El malware WannaCry intenta cifrar los archivos en el recurso compartido de CIFS, pero FPolicy evita que afecten a los archivos.



Continuar las operaciones de negocios sin pagar el rescate

Las funcionalidades de NetApp descritas en este documento le ayudan a restaurar los datos en cuestión de minutos después de un ataque y a evitar ataques en primer lugar, de tal modo que pueda continuar con sus operaciones empresariales sin impedimentos.

Es posible establecer una programación de copias Snapshot para cumplir el objetivo de punto de recuperación (RPO) deseado. Las operaciones de restauración basadas en copias de Snapshot son muy rápidas; por lo tanto, se puede lograr un objetivo de tiempo de recuperación (RTO) muy bajo.

Por encima de todo, usted no tiene que pagar cualquier rescate como resultado de un ataque, y usted puede rápidamente volver a las operaciones regulares.

Conclusión

El ransomware es un producto de la delincuencia organizada, y los atacantes no operan con la ética. Pueden abstenerse de proporcionar la clave para el descifrado incluso después de recibir el rescate. La víctima no solo pierde sus datos, sino también una cantidad importante de dinero, y se enfrenta a las consecuencias asociadas con la pérdida de datos de producción.

Según a "Artículo de Forbes", sólo el 19% de las víctimas de ransomware obtienen sus datos después de pagar el rescate. Por lo tanto, los autores recomiendan no pagar un rescate en caso de un ataque porque hacerlo refuerza la fe del atacante en su modelo de negocios.

Las operaciones de backup y restauración de datos juegan un papel importante de la recuperación de ransomware. Por lo tanto, deben incluirse como parte integral de la planificación empresarial. La implementación de estas operaciones se debe presupuestar para que no exista ningún compromiso en las

funcionalidades de recuperación en caso de ataque.

La clave está en seleccionar el partner tecnológico correcto en este viaje. FlexPod proporciona la mayoría de las funcionalidades necesarias de forma nativa sin coste adicional en un sistema FAS all-flash.

Reconocimientos

El autor desea agradecer a las siguientes personas su apoyo en la creación de este documento:

- Jorge Gómez Navarrete, NetApp
- Ganesh Kamath, NetApp

Información adicional

Si quiere más información sobre el contenido de este documento, consulte los siguientes documentos o sitios web:

- Software Snapshot de NetApp

  "https://www.netapp.com/us/products/platform-os/snapshot.aspx"

- Gestión de backups de SnapCenter

  "https://www.netapp.com/us/products/backup-recovery/snapcenter-backup-management.aspx"

- Cumplimiento de normativas para datos de SnapLock

  "https://www.netapp.com/us/products/backup-recovery/snaplock-compliance.aspx"

- Documentación de productos de NetApp

  "https://www.netapp.com/us/documentation/index.aspx"

- Cisco Advanced Malware Protection (AMP)

  "https://www.cisco.com/c/en/us/products/security/advanced-malware-protection/index.html"

- Cisco StealtWatch

  "https://www.cisco.com/c/en_in/products/security/stealthwatch/index.html"

Información de copyright

Información de la marca comercial