FlexPod, la soluzione per il ransomware

FlexPod

NetApp
March 25, 2024

Sommario

FlexPod, la soluzione per il ransomware

TR-4802: FlexPod, la soluzione per il ransomware

Arvind Ramakrishnan, NetApp

In collaborazione con: 

Per comprendere il ransomware, è necessario prima comprendere alcuni punti chiave sulla crittografia. I metodi crittografici consentono la crittografia dei dati con una chiave segreta condivisa (crittografia a chiave simmetrica) o con una coppia di chiavi (crittografia a chiave asimmetrica). Una di queste chiavi è una chiave pubblica ampiamente disponibile e l'altra è una chiave privata non divulgata.

Ransomware è un tipo di malware basato sulla crittografia, ovvero l'utilizzo della crittografia per la creazione di software dannoso. Questo malware può utilizzare la crittografia a chiave simmetrica e asimmetrica per bloccare i dati della vittima e richiedere un riscatto per fornire la chiave per decrittare i dati della vittima.

Come funziona il ransomware?

I seguenti passaggi descrivono come ransomware utilizza la crittografia per crittografare i dati della vittima senza alcun scopo per la decifratura o il ripristino da parte della vittima:

1. L'utente malintenzionato genera una coppia di chiavi come nella crittografia a chiave asimmetrica. La chiave pubblica generata viene inserita nel malware e il malware viene quindi rilasciato.
2. Una volta che il malware è entrato nel computer o nel sistema della vittima, genera una chiave simmetrica casuale utilizzando un generatore di numeri pseudocasuali (PRNG) o qualsiasi altro algoritmo di generazione di numeri casuali.
3. Il malware utilizza questa chiave simmetrica per crittografare i dati della vittima. Infine, crittografa la chiave simmetrica utilizzando la chiave pubblica dell'utente malintenzionato incorporata nel malware. L'output di questo passo è un testo cifrato asimmetrico della chiave simmetrica crittografata e il testo cifrato simmetrico dei dati della vittima.
4. Il malware azzera (cancella) i dati della vittima e la chiave simmetrica utilizzata per crittografare i dati, senza lasciare spazio per il ripristino.
5. La vittima ora mostra il testo cifrato asimmetrico della chiave simmetrica e un valore di riscatto che deve essere pagato per ottenere la chiave simmetrica utilizzata per crittografare i dati.
6. La vittima paga il riscatto e condivide il testo cifrato asimmetrico con l'autore dell'attacco. L'utente malintenzionato decrittografa il testo crittografato con la propria chiave privata, che determina la chiave simmetrica.
7. L'utente malintenzionato condivide questa chiave simmetrica con la vittima, che può essere utilizzata per decrittare tutti i dati e quindi per ripristinarli dall'attacco.

Sfide

Individui e organizzazioni devono affrontare le seguenti sfide quando vengono attaccati dal ransomware:

- La sfida più importante è che richiede un costo immediato sulla produttività dell'organizzazione o dell'individuo. Ci vuole tempo per tornare a uno stato di normalità, perché tutti i file importanti devono essere riconquistati e i sistemi devono essere protetti.
- Potrebbe portare a una violazione dei dati che contiene informazioni riservate e riservate che appartengono a clienti o clienti e che porta a una situazione di crisi che un'organizzazione vorrebbe chiaramente evitare.
- Esiste un'ottima probabilità che i dati entrino nelle mani sbagliate o vengano cancellati completamente, il che porta a un punto di non ritorno che potrebbe essere disastroso per le organizzazioni e gli individui.
- Dopo aver pagato il riscatto, non vi è alcuna garanzia che l'utente malintenzionato fornisca la chiave per ripristinare i dati.
- Non vi è alcuna garanzia che l'utente malintenzionato si asterrà dalla trasmissione dei dati sensibili nonostante il pagamento del riscatto.
- Nelle grandi imprese, identificare la lacuna che ha portato a un attacco ransomware è un compito noioso e la protezione di tutti i sistemi richiede un notevole impegno.

Chi è a rischio?

Chiunque può essere attaccato da ransomware, inclusi individui e grandi organizzazioni. Le organizzazioni che non implementano procedure e misure di sicurezza ben definite sono ancora più vulnerabili a tali attacchi. L'effetto dell'attacco su un'organizzazione di grandi dimensioni può essere più grande di quanto un individuo potrebbe sopportare.

Ransomware rappresenta circa il 28% di tutti gli attacchi di malware. In altre parole, più di un malware su quattro è un attacco ransomware. Il ransomware può diffondersi automaticamente e indiscriminatamente attraverso Internet e, in caso di mancanza di sicurezza, può entrare nei sistemi della vittima e continuare a diffondersi ad altri sistemi connessi. Gli autori degli attacchi tendono a rivolgersi a persone o organizzazioni che eseguono una grande quantità di file sharing, dispongono di molti dati sensibili e critici o mantengono una protezione inadeguata contro gli attacchi.

Gli autori degli attacchi tendono a concentrarsi sui seguenti potenziali obiettivi:

- Università e comunità studentesche
- Uffici governativi e agenzie
- Ospedali
- Banche

Questo non è un elenco completo di obiettivi. Non puoi considerarti al sicuro dagli attacchi se ti trovi al di fuori di una di queste categorie.

In che modo il ransomware entra in un sistema o si diffonde?

Esistono diversi modi in cui il ransomware può entrare in un sistema o diffondersi in altri sistemi. Nel mondo odierno, quasi tutti i sistemi sono connessi tra loro tramite Internet, LAN, WAN e così via. La quantità di dati che vengono generati e scambiati tra questi sistemi è solo in aumento.

Alcuni dei modi più comuni con cui il ransomware può diffondersi includono metodi che utilizziamo quotidianamente per condividere o accedere ai dati:

- E-mail
- Reti P2P

- Download di file
- Social network
- Dispositivi mobili
- Connessione a reti pubbliche non sicure
- Accesso agli URL Web

Conseguenze della perdita di dati

Le conseguenze o gli effetti della perdita di dati possono arrivare più ampiamente di quanto le organizzazioni potrebbero prevedere. Gli effetti possono variare a seconda della durata del downtime o del periodo di tempo durante il quale un'organizzazione non ha accesso ai propri dati. Quanto più dura l'attacco, tanto maggiore sarà l'effetto sui ricavi, sul marchio e sulla reputazione dell'organizzazione. Un'organizzazione può anche affrontare problemi legali e un drastico calo della produttività.

Poiché questi problemi continuano a persistere nel tempo, iniziano ad ingrandirsi e potrebbero finire per cambiare la cultura di un'organizzazione, a seconda di come risponde all'attacco. Nel mondo di oggi, le informazioni si diffondono rapidamente e le notizie negative su un'organizzazione potrebbero causare danni permanenti alla sua reputazione. Un'organizzazione potrebbe affrontare enormi sanzioni per la perdita di dati, che potrebbe portare alla chiusura di un'azienda.

Effetti finanziari

Secondo un recente "Report McAfee", I costi globali sostenuti a causa della criminalità informatica sono pari a circa 600 miliardi di dollari, pari a circa il 0.8% del PIL globale. Quando questo importo viene confrontato con la crescente economia mondiale di Internet di 4.2 trilioni di dollari, equivale a una tassa del 14% sulla crescita.

Ransomware prende una quota significativa di questo costo finanziario. Nel 2018, i costi sostenuti per gli attacchi ransomware sono stati di circa 8 miliardi di dollari—, un importo previsto per raggiungere i 11.5 miliardi di dollari nel 2019.

Qual è la soluzione?

Il ripristino da un attacco ransomware con downtime minimo è possibile solo implementando un piano di disaster recovery proattivo. Avere la capacità di recuperare da un attacco è un bene, ma prevenire un attacco è l'ideale.

Sebbene vi siano diversi fronti che è necessario rivedere e correggere per prevenire un attacco, il componente principale che consente di prevenire o ripristinare da un attacco è il data center.

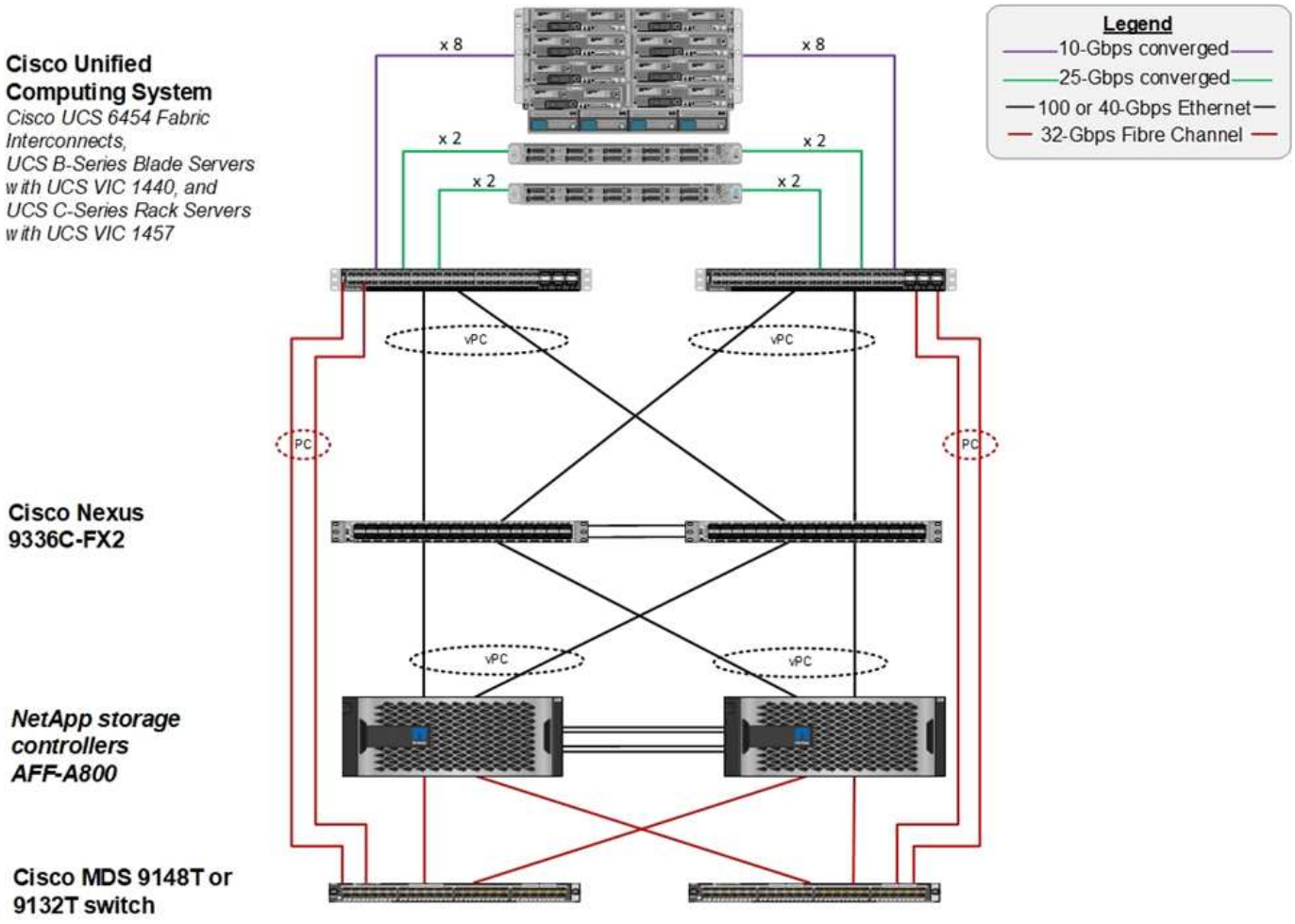
Il design del data center e le funzionalità che offre per proteggere gli end-point di rete, calcolo e storage svolgono un ruolo fondamentale nella creazione di un ambiente sicuro per le operazioni quotidiane. Questo documento mostra in che modo le funzionalità di un'infrastruttura di cloud ibrido FlexPod possono contribuire al rapido ripristino dei dati in caso di attacco e possono anche contribuire a prevenire del tutto gli attacchi.

Panoramica di FlexPod

FlexPod è un'architettura pre-progettata, integrata e validata che combina i server Cisco Unified Computing System (Cisco UCS), la famiglia di switch Cisco Nexus, gli switch Cisco MDS Fabric e gli storage array NetApp in un'unica architettura flessibile. Le soluzioni FlexPod sono progettate per l'alta disponibilità senza singoli punti di errore,

mantenendo al contempo convenienza e flessibilità di progettazione per supportare un'ampia varietà di carichi di lavoro. Un design FlexPod può supportare diversi hypervisor e server bare metal e può anche essere dimensionato e ottimizzato in base ai requisiti dei carichi di lavoro del cliente.

La figura seguente illustra l'architettura FlexPod e evidenzia chiaramente l'alta disponibilità in tutti i livelli dello stack. I componenti dell'infrastruttura di storage, rete e calcolo sono configurati in modo che le operazioni possano eseguire il failover istantaneo al partner sopravvissuto in caso di guasto di uno dei componenti.



Un vantaggio importante per un sistema FlexPod è la sua pre-progettazione, integrazione e validazione per diversi carichi di lavoro. Vengono pubblicate guide dettagliate di progettazione e implementazione per ogni convalida della soluzione. Questi documenti includono le Best practice da adottare per consentire ai carichi di lavoro di essere eseguiti senza problemi su FlexPod. Queste soluzioni sono costruite con i migliori prodotti di calcolo, rete e storage e una serie di funzionalità che si concentrano sulla sicurezza e la protezione avanzata dell'intera infrastruttura.

"L'X-Force Threat Intelligence Index di IBM" afferma: "Errore umano responsabile di due terzi dei record compromessi, compreso un salto storico del 424% nell'infrastruttura cloud non configurata correttamente".

Con un sistema FlexPod, è possibile evitare di configurare in modo errato l'infrastruttura utilizzando l'automazione attraverso i playbook Ansible che eseguono una configurazione end-to-end dell'infrastruttura in base alle Best practice descritte in Cisco Validated Designs (CVD) e NetApp Verified Architectures (NVA).

Misure di protezione ransomware

In questa sezione vengono descritte le funzionalità principali del software di gestione dei dati NetApp ONTAP e gli strumenti per Cisco UCS e Cisco Nexus che è possibile utilizzare per proteggere e ripristinare in modo efficace dagli attacchi ransomware.

Storage: NetApp ONTAP

Il software ONTAP offre molte funzionalità utili per la protezione dei dati, la maggior parte delle quali è gratuita per i clienti che dispongono di un sistema ONTAP. È possibile utilizzare le seguenti funzionalità in qualsiasi momento per proteggere i dati dagli attacchi:

- **Tecnologia NetApp Snapshot.** Una copia Snapshot è un'immagine di sola lettura di un volume che acquisisce lo stato di un file system in un momento specifico. Queste copie aiutano a proteggere i dati senza alcun effetto sulle prestazioni del sistema e, allo stesso tempo, non occupano molto spazio di storage. NetApp consiglia di creare una pianificazione per la creazione di copie Snapshot. È inoltre necessario mantenere un lungo periodo di conservazione, in quanto alcuni malware possono andare in stato di inattività e quindi riattivarsi settimane o mesi dopo un'infezione. In caso di attacco, è possibile eseguire il rollback del volume utilizzando una copia Snapshot acquisita prima dell'infezione.
- **La tecnologia NetApp SnapRestore.** il software di ripristino dei dati SnapRestore è estremamente utile per eseguire il ripristino dalla corruzione dei dati o per ripristinare solo il contenuto del file. SnapRestore non ripristina gli attributi di un volume, ma è molto più veloce di quanto un amministratore possa ottenere copiando i file dalla copia Snapshot al file system attivo. La velocità con cui è possibile recuperare i dati è utile quando molti file devono essere ripristinati il più rapidamente possibile. In caso di attacco, questo processo di recovery altamente efficiente consente di ripristinare rapidamente il business online.
- **Tecnologia NetApp SnapCenter.** il software SnapCenter utilizza le funzioni di backup e replica basate su storage NetApp per fornire una protezione dei dati coerente con l'applicazione. Questo software si integra con le applicazioni aziendali e fornisce flussi di lavoro specifici per applicazioni e database per soddisfare le esigenze degli amministratori di applicazioni, database e infrastrutture virtuali. SnapCenter offre una piattaforma aziendale di facile utilizzo per coordinare e gestire in modo sicuro la protezione dei dati tra applicazioni, database e file system. La sua capacità di fornire una protezione dei dati coerente con l'applicazione è fondamentale durante il ripristino dei dati, perché semplifica il ripristino delle applicazioni a uno stato coerente più rapidamente.
- **Tecnologia NetApp SnapLock.** SnapLock offre un volume speciale in cui i file possono essere memorizzati e impegnati in uno stato non cancellabile e non riscrivibile. I dati di produzione dell'utente che risiedono in un volume FlexVol possono essere mirrorati o archiviati in un volume SnapLock, rispettivamente tramite NetApp SnapMirror o la tecnologia SnapVault. I file nel volume SnapLock, nel volume stesso e nel relativo aggregato di hosting non possono essere cancellati fino alla fine del periodo di conservazione.
- **Tecnologia NetApp FPolicy.** Usa il software FPolicy per prevenire gli attacchi impedendo operazioni su file con estensioni specifiche. È possibile attivare un evento FPolicy per operazioni di file specifiche. L'evento è legato a una policy, che richiama il motore che deve utilizzare. È possibile configurare un criterio con una serie di estensioni di file che potrebbero contenere ransomware. Quando un file con un'estensione non consentita tenta di eseguire un'operazione non autorizzata, FPolicy impedisce l'esecuzione di tale operazione.

Rete: Cisco Nexus

Il software Cisco NX OS supporta la funzione NetFlow che consente un rilevamento avanzato delle anomalie e della sicurezza della rete. NetFlow acquisisce i metadati di ogni conversazione sulla rete, le parti coinvolte nella comunicazione, il protocollo utilizzato e la durata della transazione. Una volta aggregate e analizzate le

informazioni, possono fornire informazioni dettagliate sul comportamento normale.

I dati raccolti consentono inoltre l'identificazione di modelli di attività dubbi, come la diffusione di malware nella rete, che altrimenti potrebbero passare inosservati.

NetFlow utilizza i flussi per fornire statistiche per il monitoraggio della rete. Un flusso è un flusso unidirezionale di pacchetti che arriva su un'interfaccia di origine (o VLAN) e ha gli stessi valori per le chiavi. Una chiave è un valore identificato per un campo all'interno del pacchetto. Si crea un flusso utilizzando un record di flusso per definire le chiavi univoche per il flusso. È possibile esportare i dati raccolti da NetFlow per i flussi utilizzando un'esportazione di flusso in un NetFlow Collector remoto, ad esempio Cisco Stealthwatch. Stealthwatch utilizza queste informazioni per il monitoraggio continuo della rete e fornisce analisi forensi in tempo reale per il rilevamento delle minacce e la risposta agli incidenti in caso di scoppio di ransomware.

Calcolo: Cisco UCS

Cisco UCS è l'endpoint di calcolo in un'architettura FlexPod. È possibile utilizzare diversi prodotti Cisco per proteggere questo livello dello stack a livello di sistema operativo.

È possibile implementare i seguenti prodotti chiave a livello di elaborazione o applicazione:

- **Cisco Advanced malware Protection (AMP) per endpoint.** supportata sui sistemi operativi Microsoft Windows e Linux, questa soluzione integra funzionalità di prevenzione, rilevamento e risposta. Questo software di sicurezza previene le violazioni, blocca il malware nel punto di ingresso e monitora e analizza continuamente le attività di file e processi per rilevare, contenere e rimediare rapidamente alle minacce che possono eludere le difese front-line.

  Il componente di protezione delle attività dannose (MAP) di AMP monitora continuamente tutte le attività degli endpoint e fornisce il rilevamento in fase di esecuzione e il blocco del comportamento anomalo di un programma in esecuzione sull'endpoint. Ad esempio, quando il comportamento degli endpoint indica ransomware, i processi in errore vengono terminati, impedendo la crittografia degli endpoint e arrestando l'attacco.

- **Cisco Advanced malware Protection for Email Security.** le email sono diventate il mezzo principale per diffondere malware e per eseguire cyber-attacchi. In media, circa 100 miliardi di e-mail vengono scambiate in un solo giorno, il che fornisce agli autori degli attacchi un eccellente vettore di penetrazione nei sistemi degli utenti. Pertanto, è assolutamente essenziale difendersi da questa linea di attacco.

  AMP analizza le e-mail per individuare minacce come exploit zero-day e malware furtivo nascosto in allegati dannosi. Utilizza inoltre l'intelligence URL leader del settore per combattere i collegamenti dannosi. Offre agli utenti una protezione avanzata contro il phishing, il ransomware e altri attacchi sofisticati.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco firepower NGIPS può essere implementato come appliance fisica nel data center o come appliance virtuale su VMware (NGIPSv per VMware). Questo sistema di prevenzione delle intrusioni altamente efficace offre performance affidabili e un basso costo totale di proprietà. La protezione dalle minacce può essere estesa con licenze di abbonamento opzionali per fornire AMP, visibilità e controllo delle applicazioni e funzionalità di filtraggio degli URL. I NGIPS virtualizzati ispezionano il traffico tra macchine virtuali (VM) e semplificano l'implementazione e la gestione delle soluzioni NGIPS in siti con risorse limitate, aumentando la protezione per risorse fisiche e virtuali.

Proteggere e ripristinare i dati su FlexPod

Questa sezione descrive come è possibile ripristinare i dati di un utente finale in caso di attacco e come è possibile prevenire gli attacchi utilizzando un sistema FlexPod.

Panoramica testbed

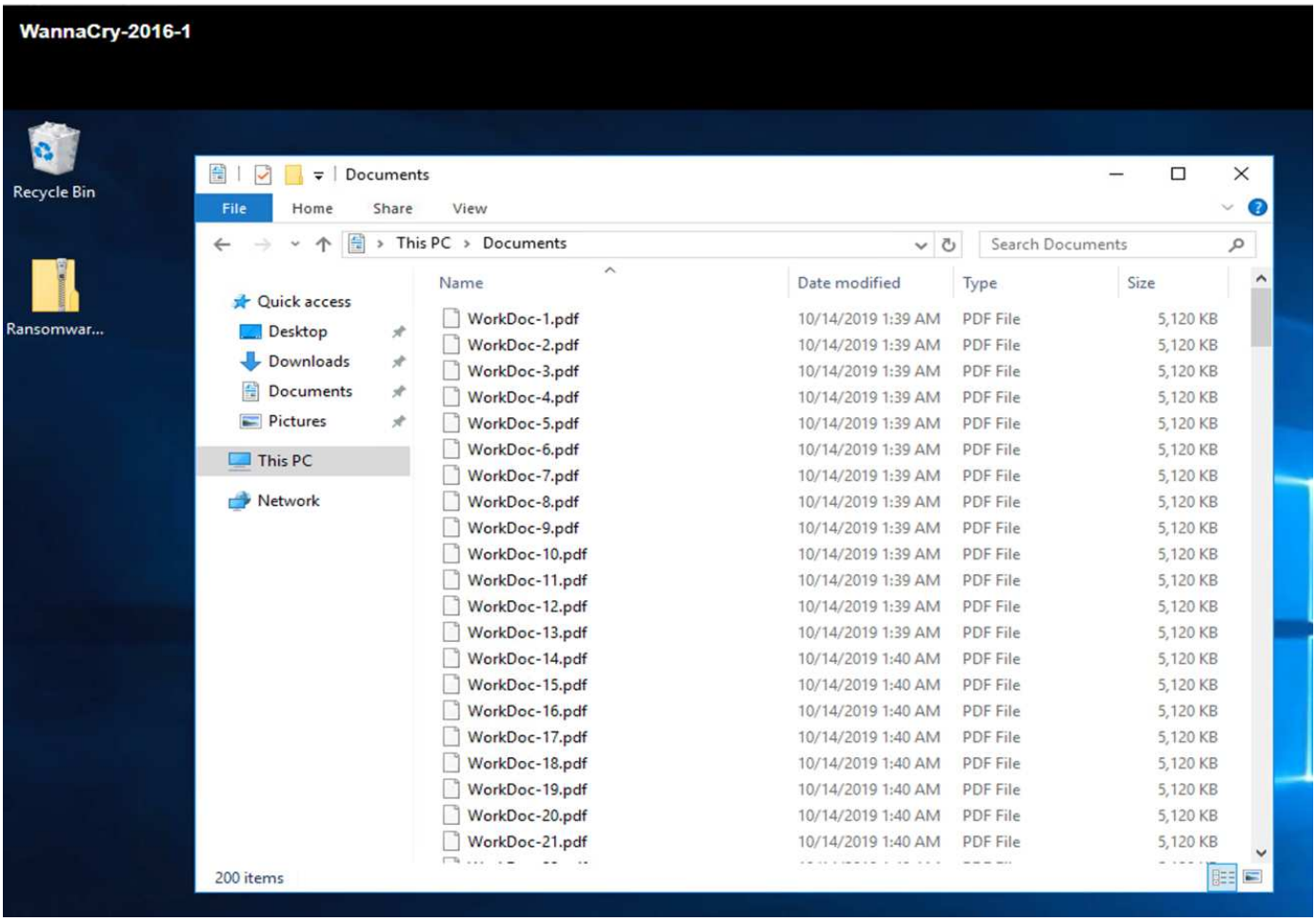
Per mostrare il rilevamento, la correzione e la prevenzione di FlexPod, è stato creato un testbed basato sulle linee guida specificate nell'ultima piattaforma CVD disponibile al momento della stesura del presente documento: "FlexPod Datacenter con VMware vSphere 6.7 U1, Cisco UCS 4a generazione e NetApp AFF A-Series CVD".

Una macchina virtuale Windows 2016, che forniva una condivisione CIFS dal software NetApp ONTAP, è stata implementata nell'infrastruttura VMware vSphere. Quindi, NetApp FPolicy è stato configurato sulla condivisione CIFS per impedire l'esecuzione di file con determinati tipi di estensione. Il software NetApp SnapCenter è stato implementato anche per gestire le copie Snapshot delle macchine virtuali nell'infrastruttura per fornire copie Snapshot coerenti con l'applicazione.

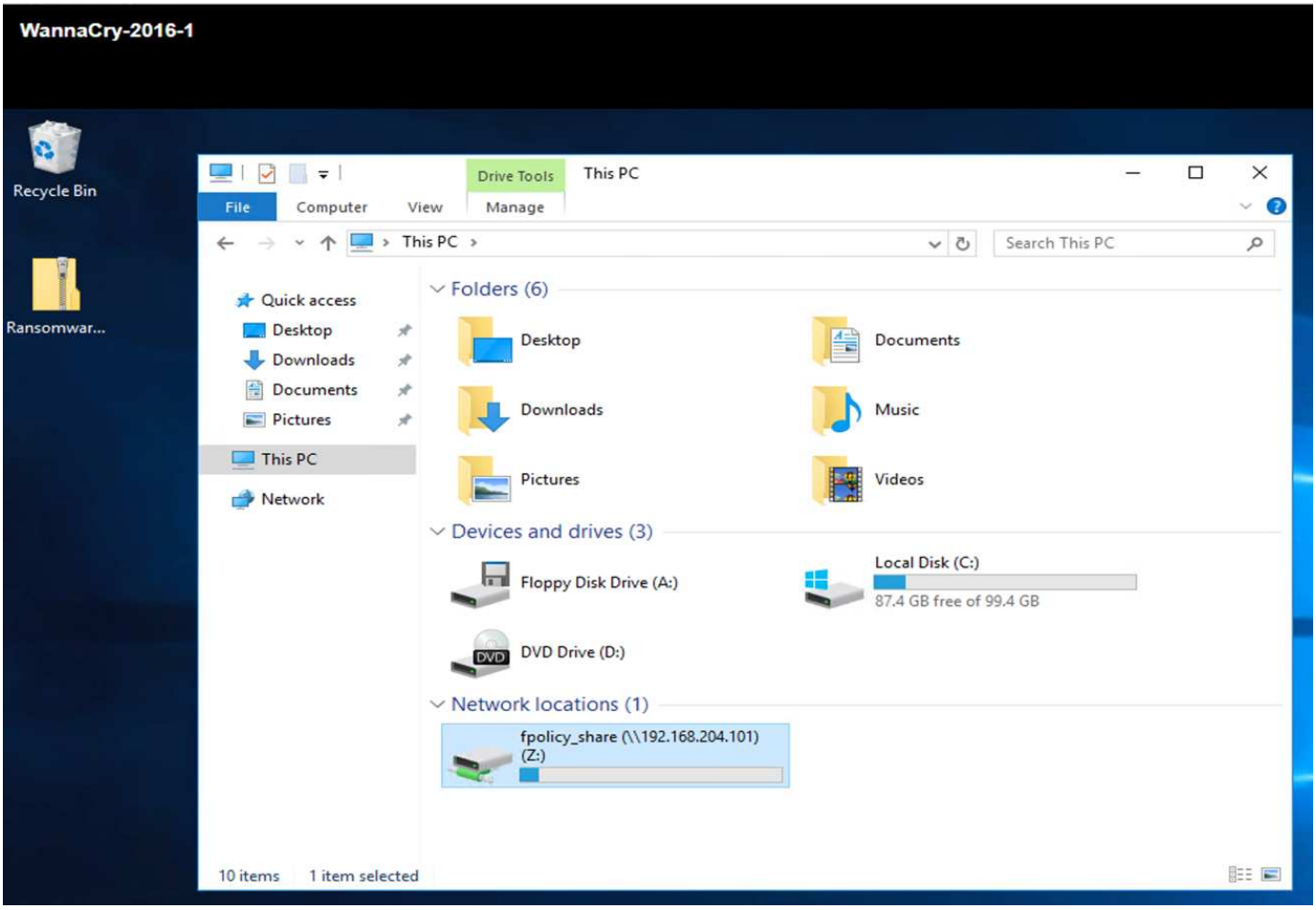
Stato della macchina virtuale e dei relativi file prima di un attacco

Questa sezione mostra lo stato dei file prima di un attacco alla macchina virtuale e la condivisione CIFS ad essa mappata.

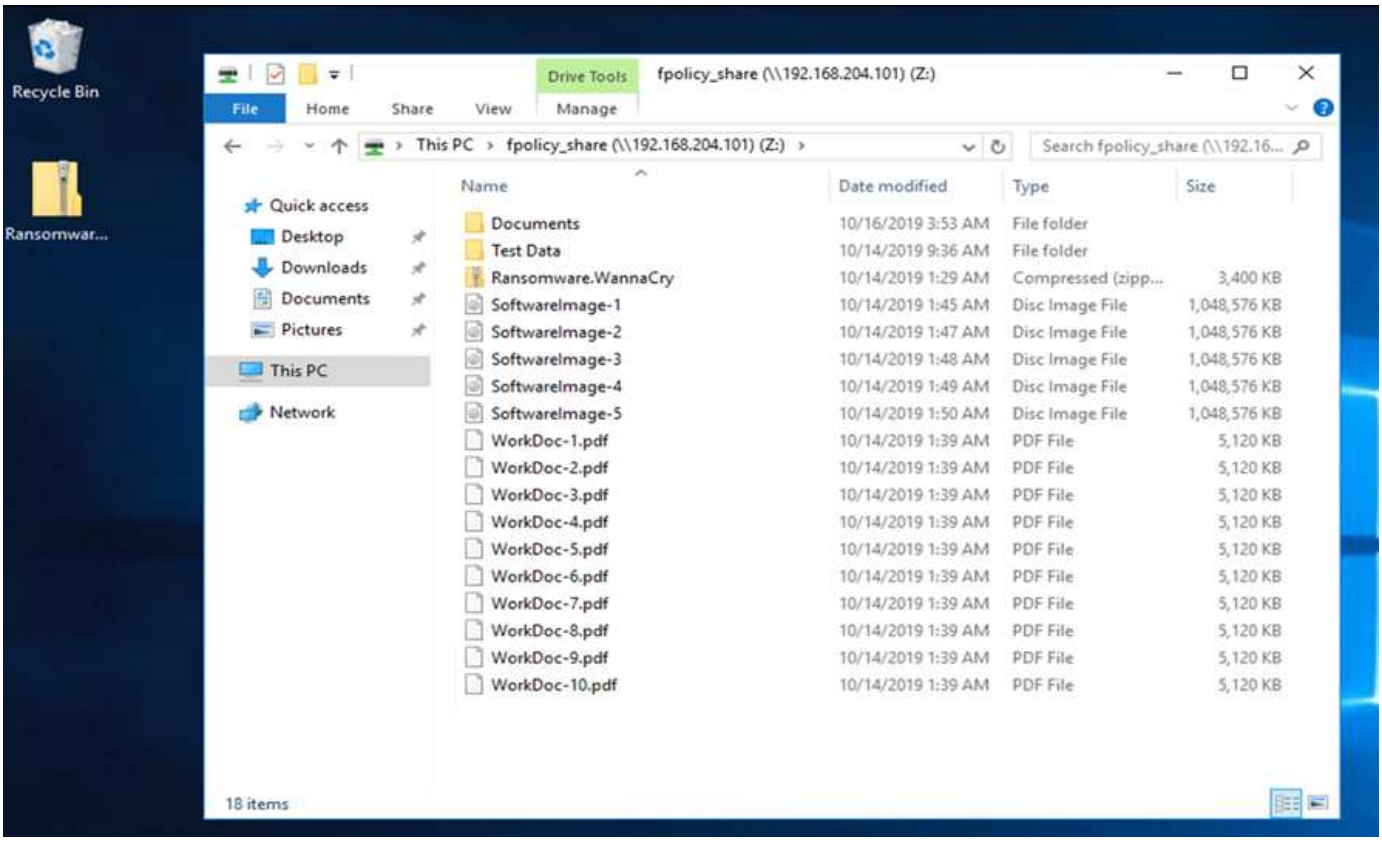
La cartella documenti della macchina virtuale aveva un set di file PDF che non sono stati ancora crittografati dal malware WannaCry.



La seguente schermata mostra la condivisione CIFS mappata alla macchina virtuale.



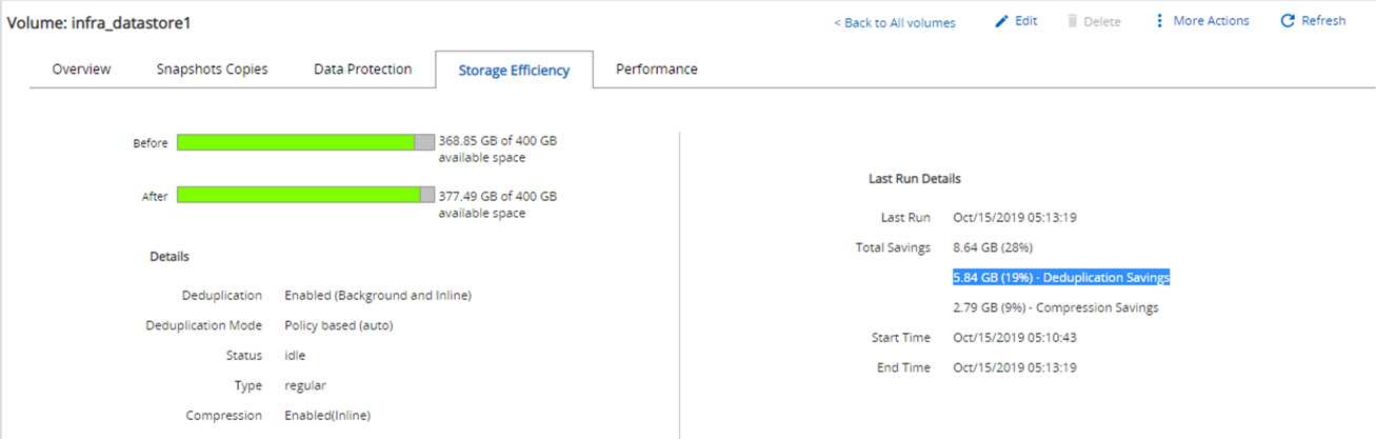
La seguente schermata mostra i file sulla condivisione CIFS `fpolicy_share` Che non sono ancora stati crittografati dal malware WannaCry.



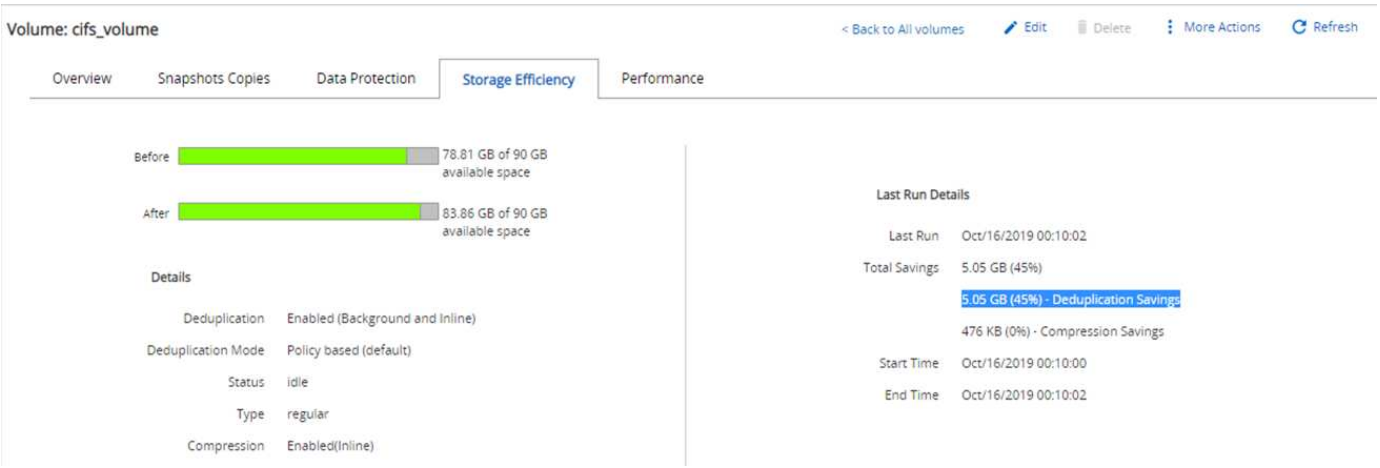
Deduplica e informazioni Snapshot prima di un attacco

I dettagli sull'efficienza dello storage e le dimensioni della copia Snapshot prima di un attacco vengono indicati e utilizzati come riferimento durante la fase di rilevamento.

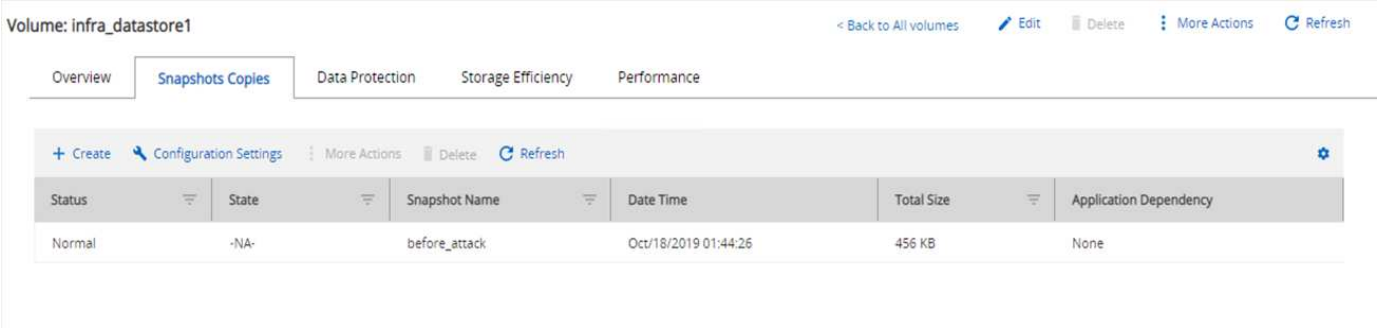
Grazie alla deduplica sul volume che ospita la macchina virtuale, sono stati ottenuti risparmi dello storage del 19%.



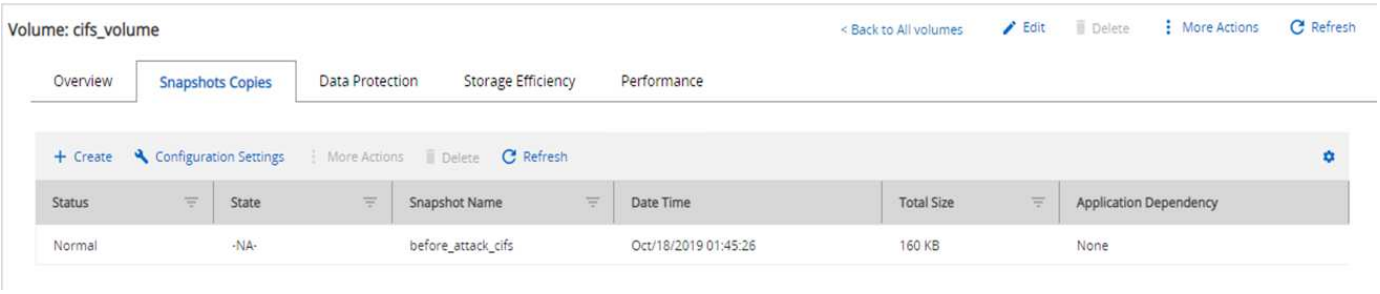
Con la deduplica sulla condivisione CIFS sono stati ottenuti risparmi dello storage del 45% `fpolicy_share`.



È stata rilevata una dimensione della copia Snapshot di 456 KB per il volume che ospita la macchina virtuale.



Per la condivisione CIFS è stata osservata una dimensione della copia Snapshot di 160 KB `fpolicy_share`.



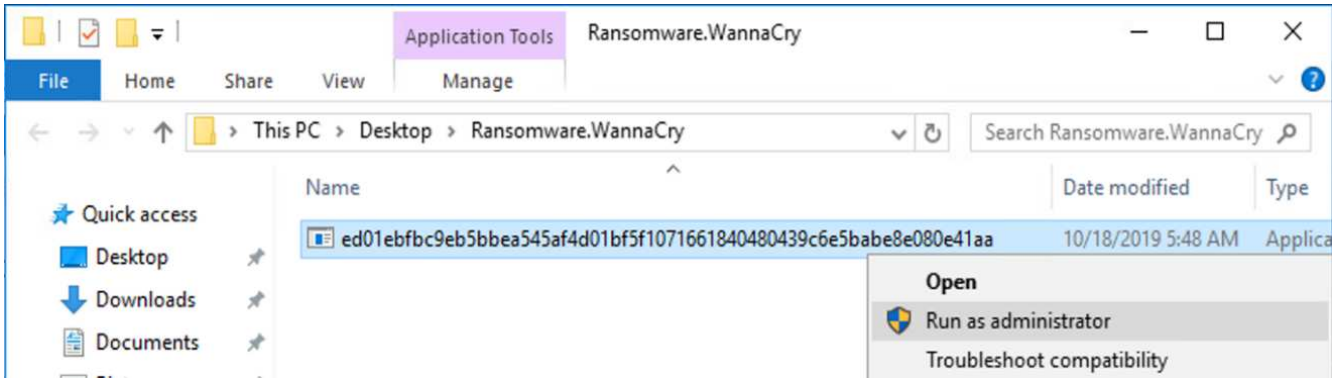
Infezione WannaCry su VM e condivisione CIFS

In questa sezione viene illustrato come il malware WannaCry è stato introdotto nell'ambiente FlexPod e le successive modifiche apportate al sistema.

I seguenti passaggi dimostrano come il malware binario WannaCry è stato introdotto nella macchina virtuale:

1. Il malware protetto è stato estratto.

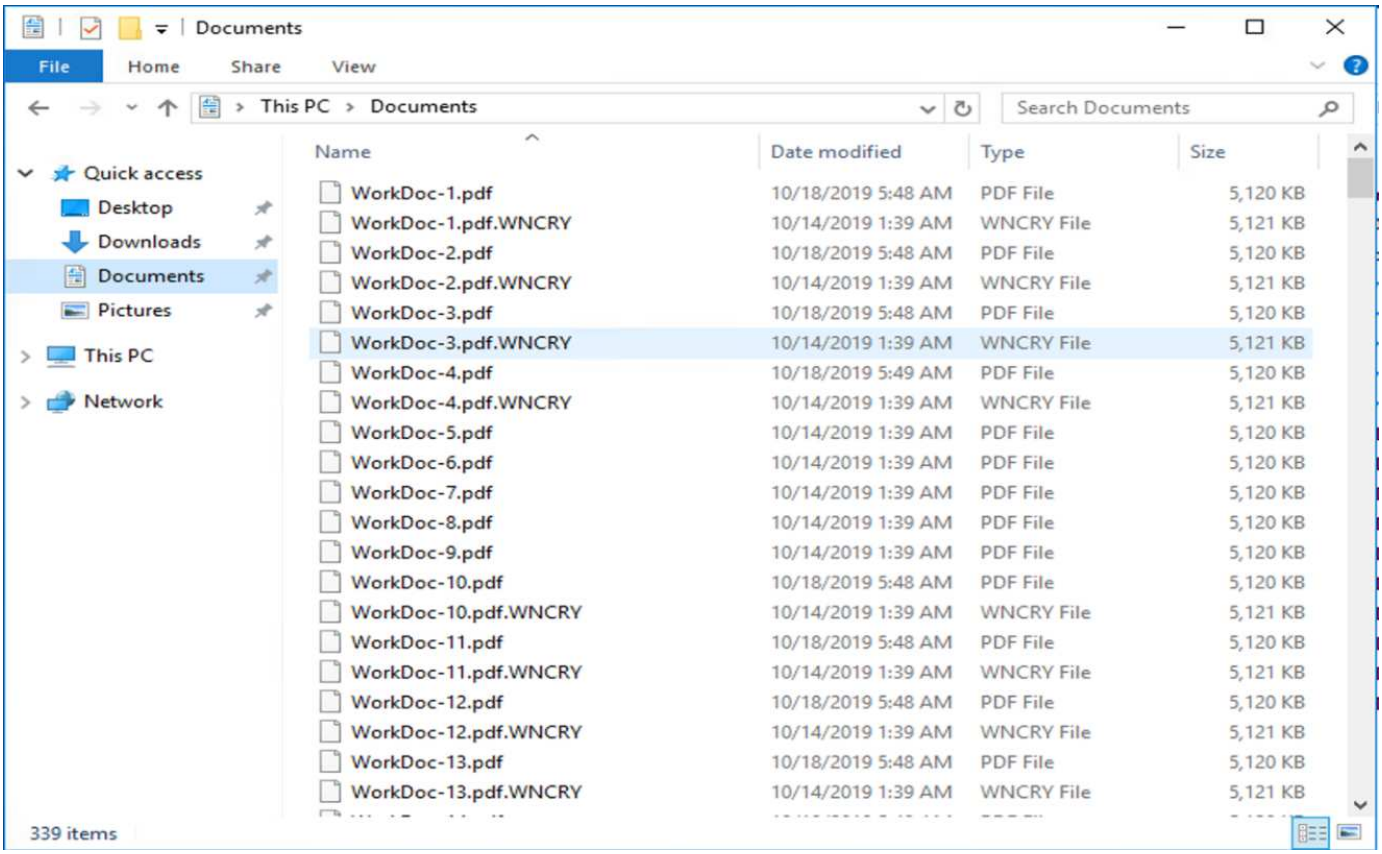
2. Il binario è stato eseguito.



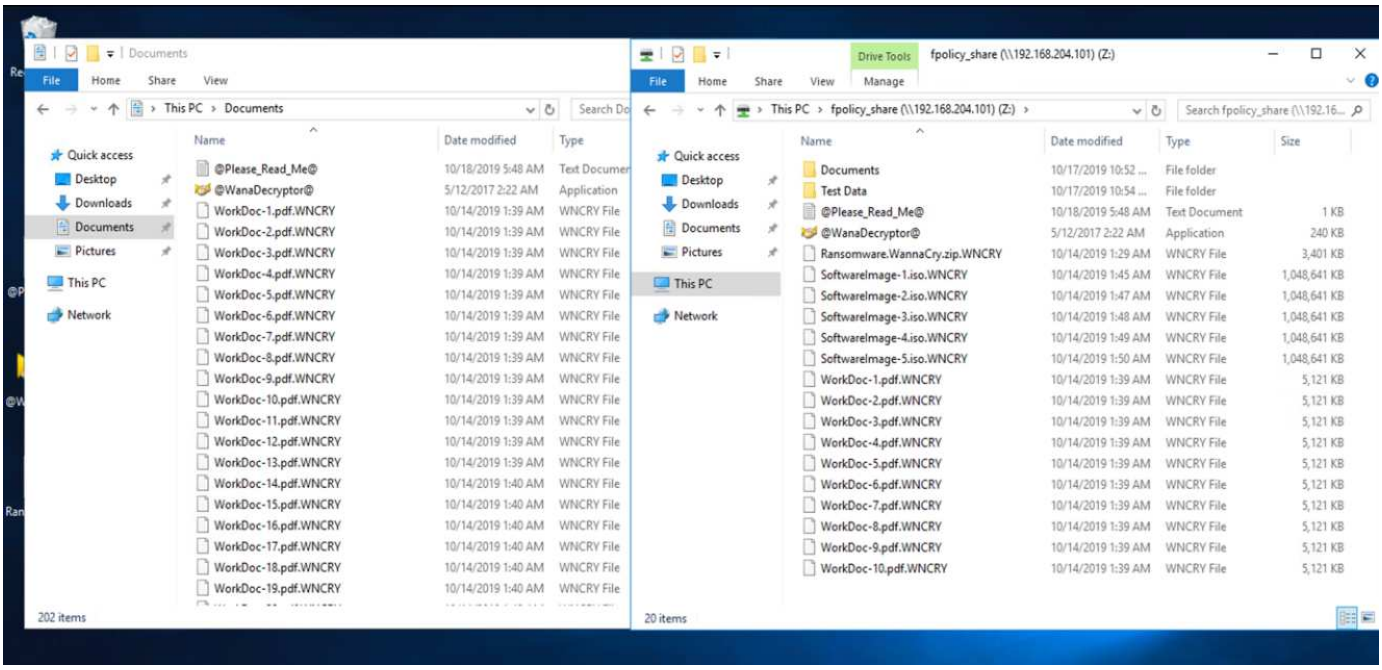
Caso 1: WannaCry crittografa il file system all'interno della VM e della condivisione CIFS mappata

Il file system locale e la condivisione CIFS mappata sono stati crittografati dal malware WannaCry.

Il malware inizia a crittografare i file con estensioni WNCRY.



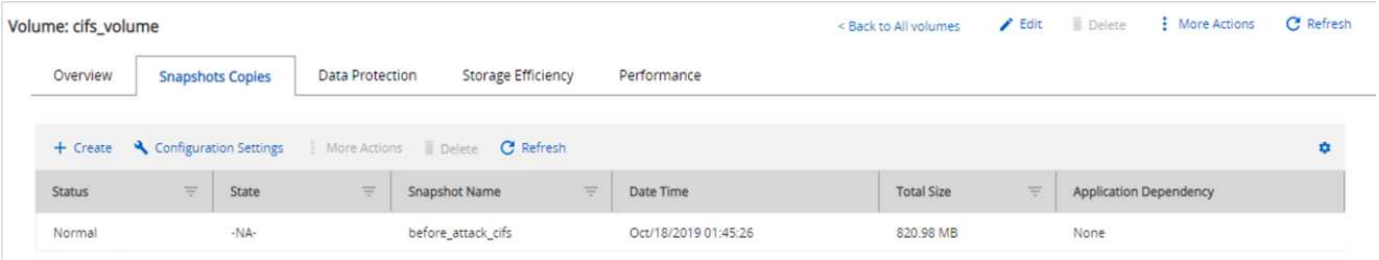
Il malware crittografa tutti i file nella VM locale e nella condivisione mappata.



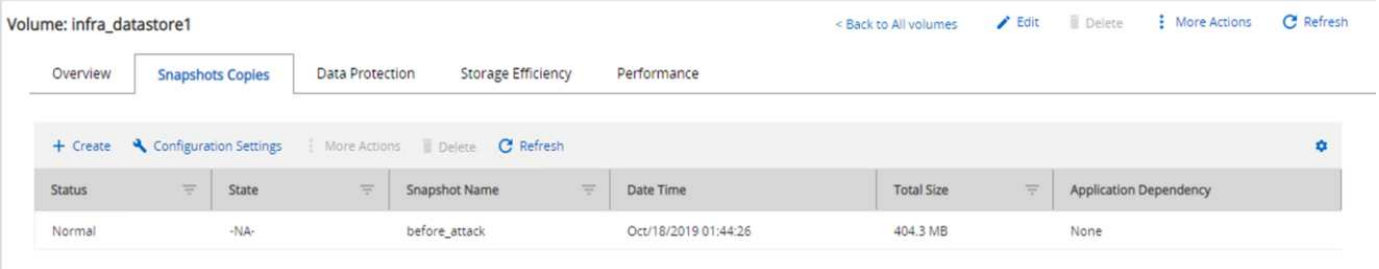
Rilevamento

Dal momento in cui il malware ha iniziato a crittografare i file, ha generato un aumento esponenziale delle dimensioni delle copie Snapshot e una diminuzione esponenziale della percentuale di efficienza dello storage.

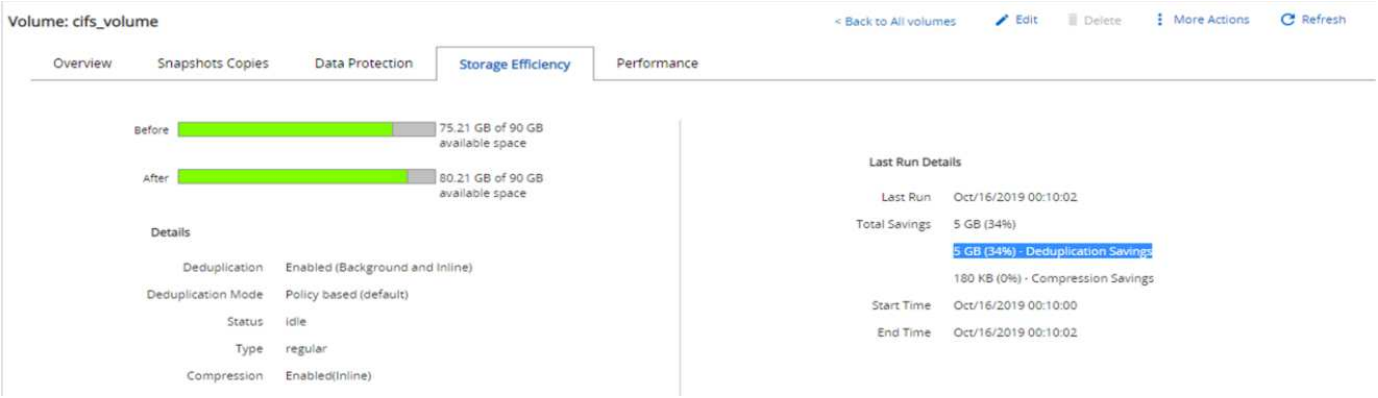
Durante l'attacco, è stato rilevato un notevole aumento delle dimensioni di Snapshot fino a 820,98 MB per il volume che ospita la condivisione CIFS.



È stato rilevato un aumento delle dimensioni della copia Snapshot fino a 404,3 MB per il volume che ospita la macchina virtuale.



L'efficienza dello storage per il volume che ospita la condivisione CIFS è scesa al 34%.



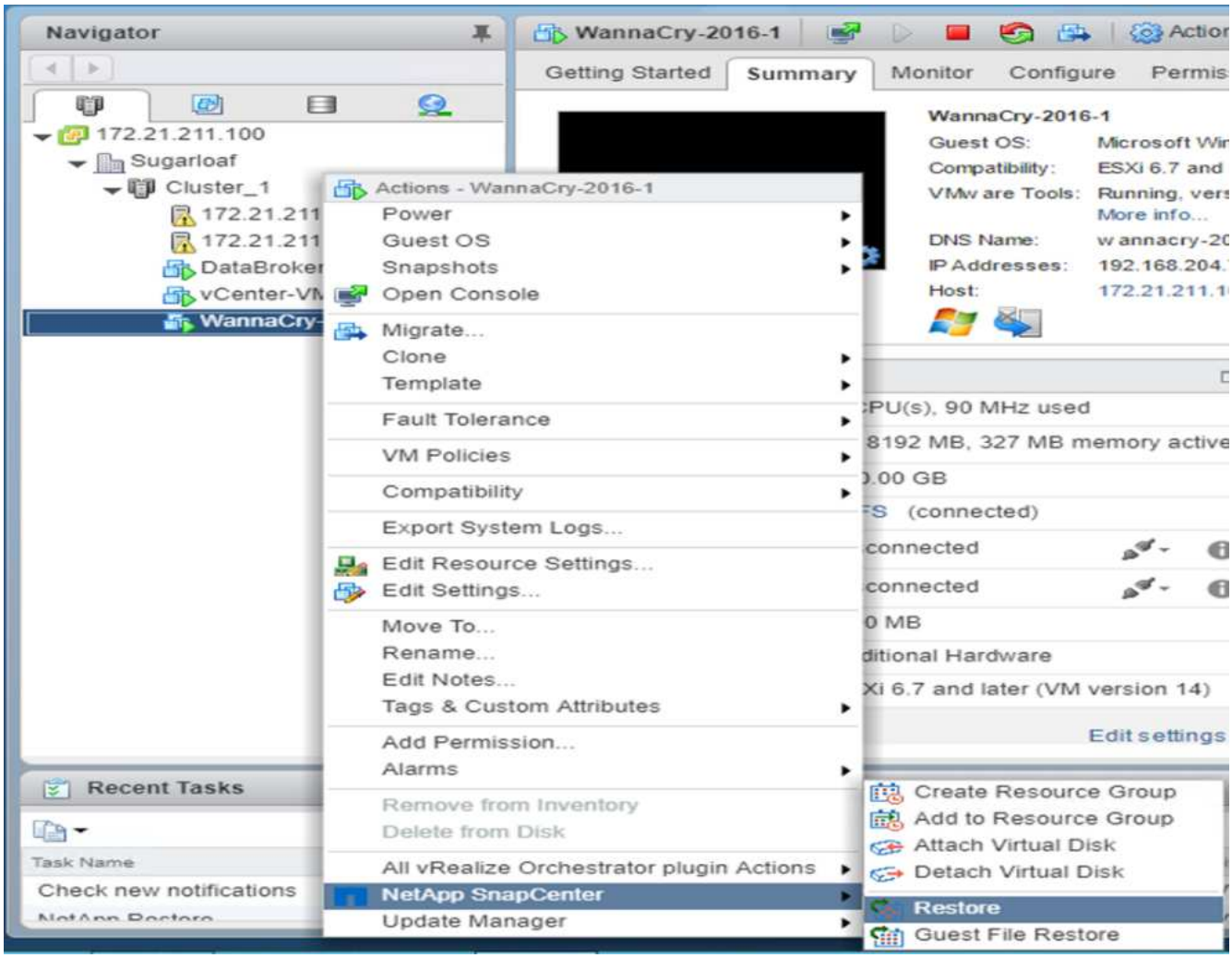
Risoluzione dei problemi

Ripristinare la VM e la condivisione CIFS mappata utilizzando una copia Snapshot pulita creata prima dell'attacco.

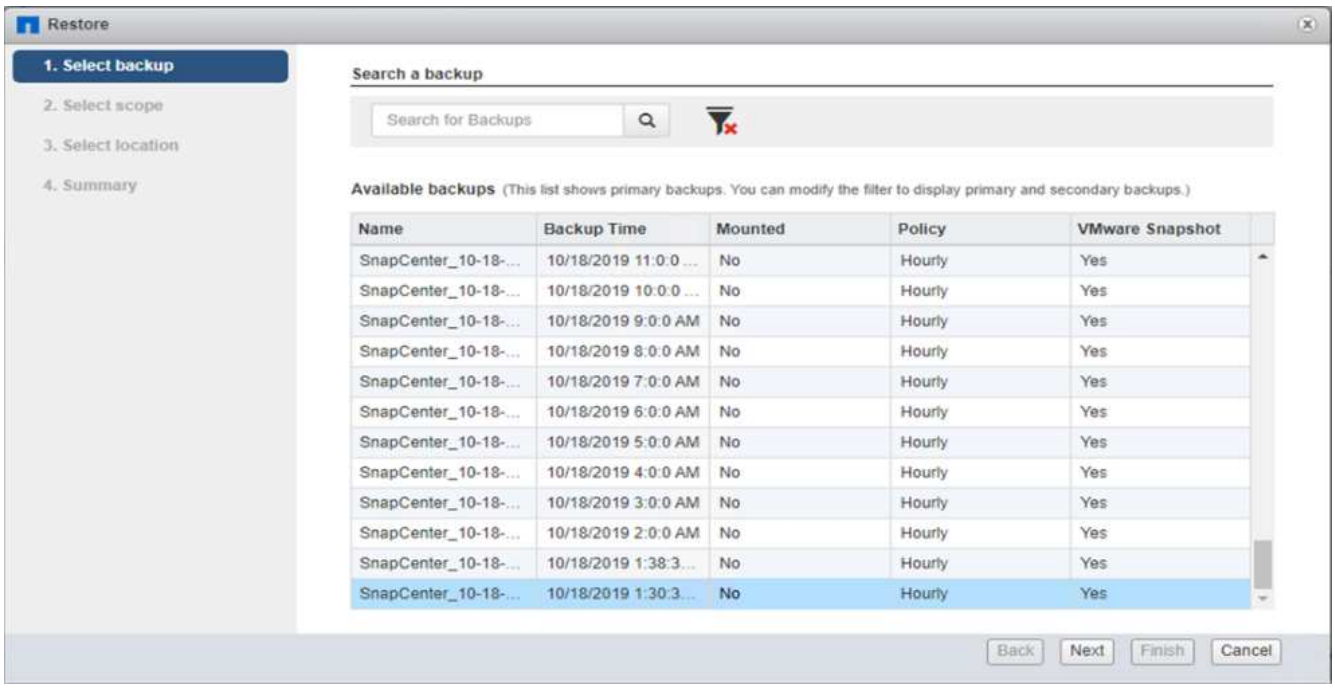
Ripristinare la macchina virtuale

Per ripristinare la macchina virtuale, attenersi alla seguente procedura:

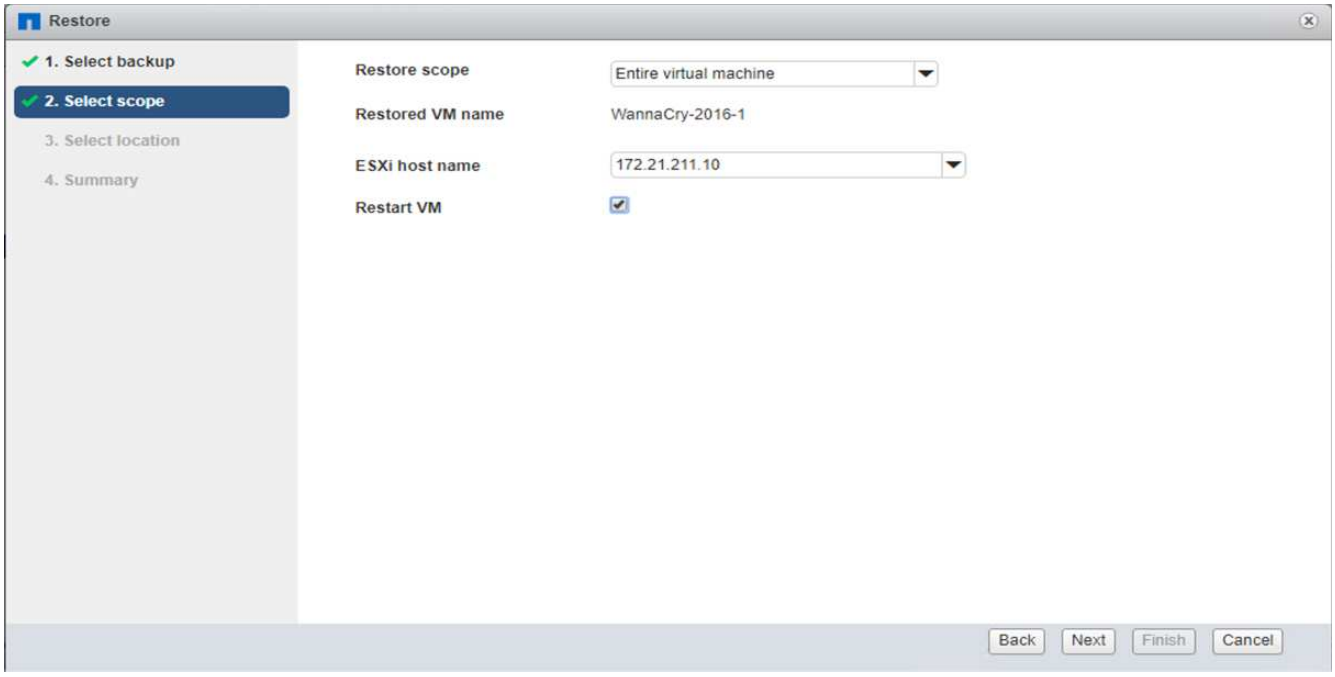
1. Utilizzare la copia Snapshot creata con SnapCenter per ripristinare la macchina virtuale.



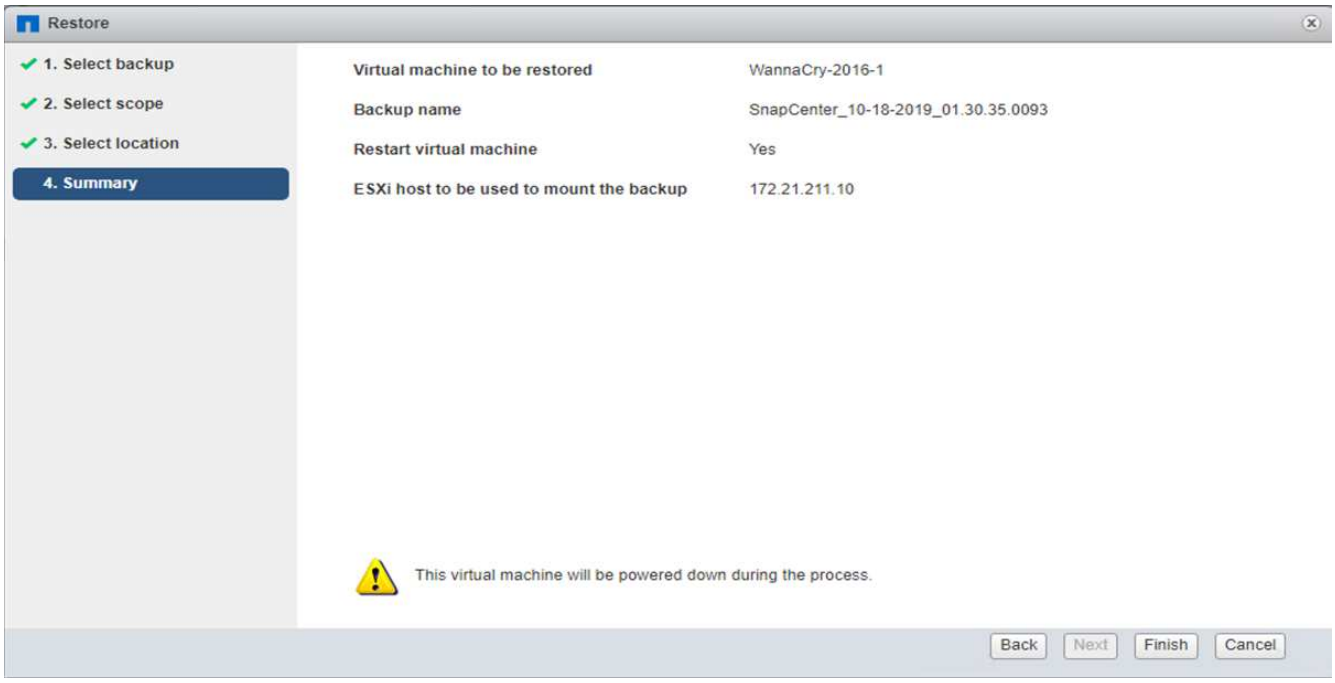
2. Selezionare la copia Snapshot coerente VMware desiderata per il ripristino.



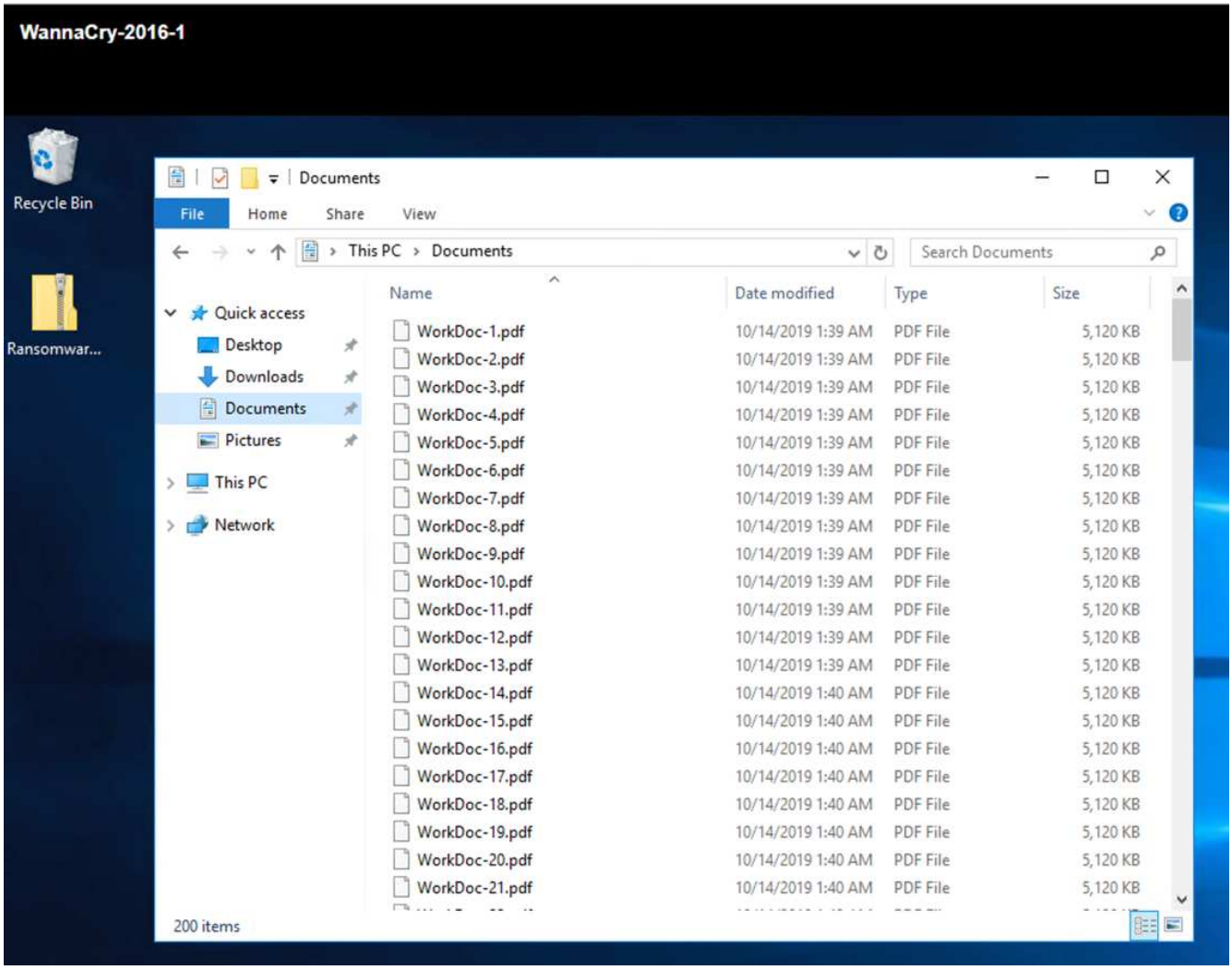
3. L'intera macchina virtuale viene ripristinata e riavviata.



4. Fare clic su Finish (fine) per avviare il processo di ripristino.



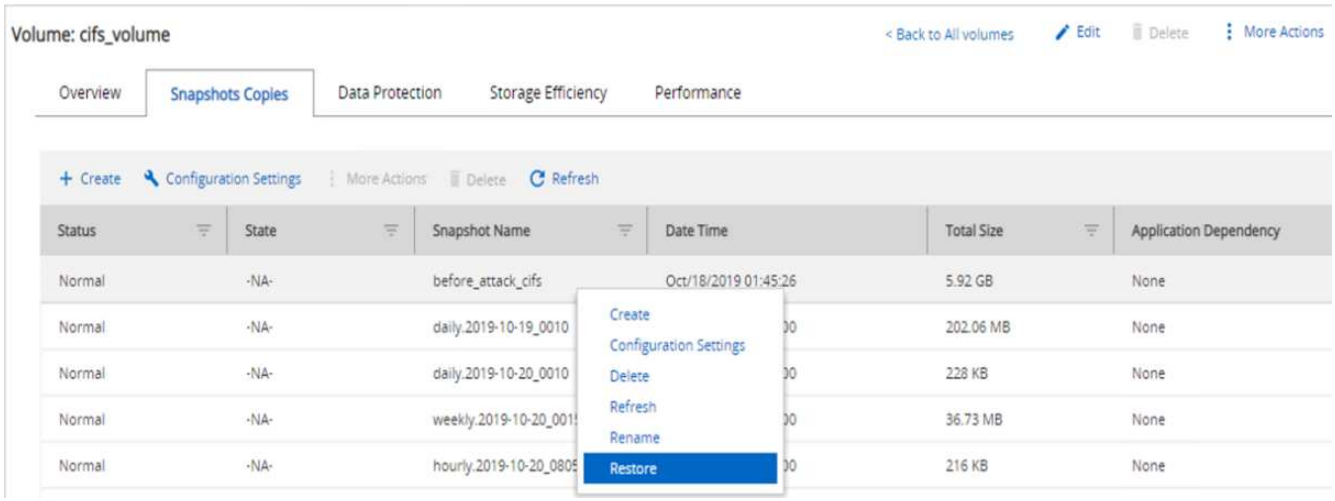
5. La macchina virtuale e i relativi file vengono ripristinati.



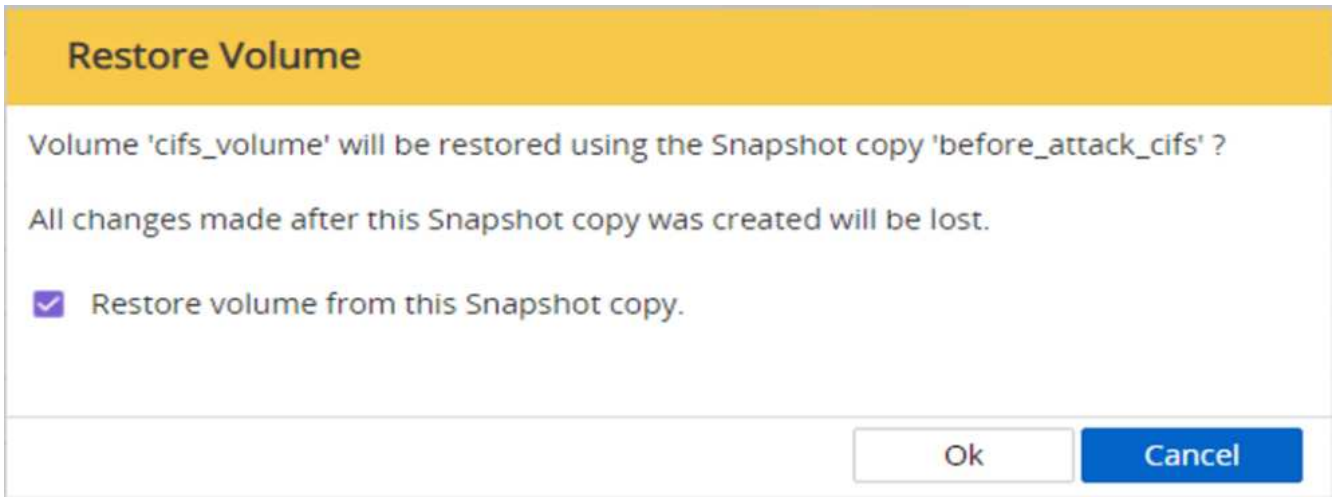
Ripristina condivisione CIFS

Per ripristinare la condivisione CIFS, attenersi alla seguente procedura:

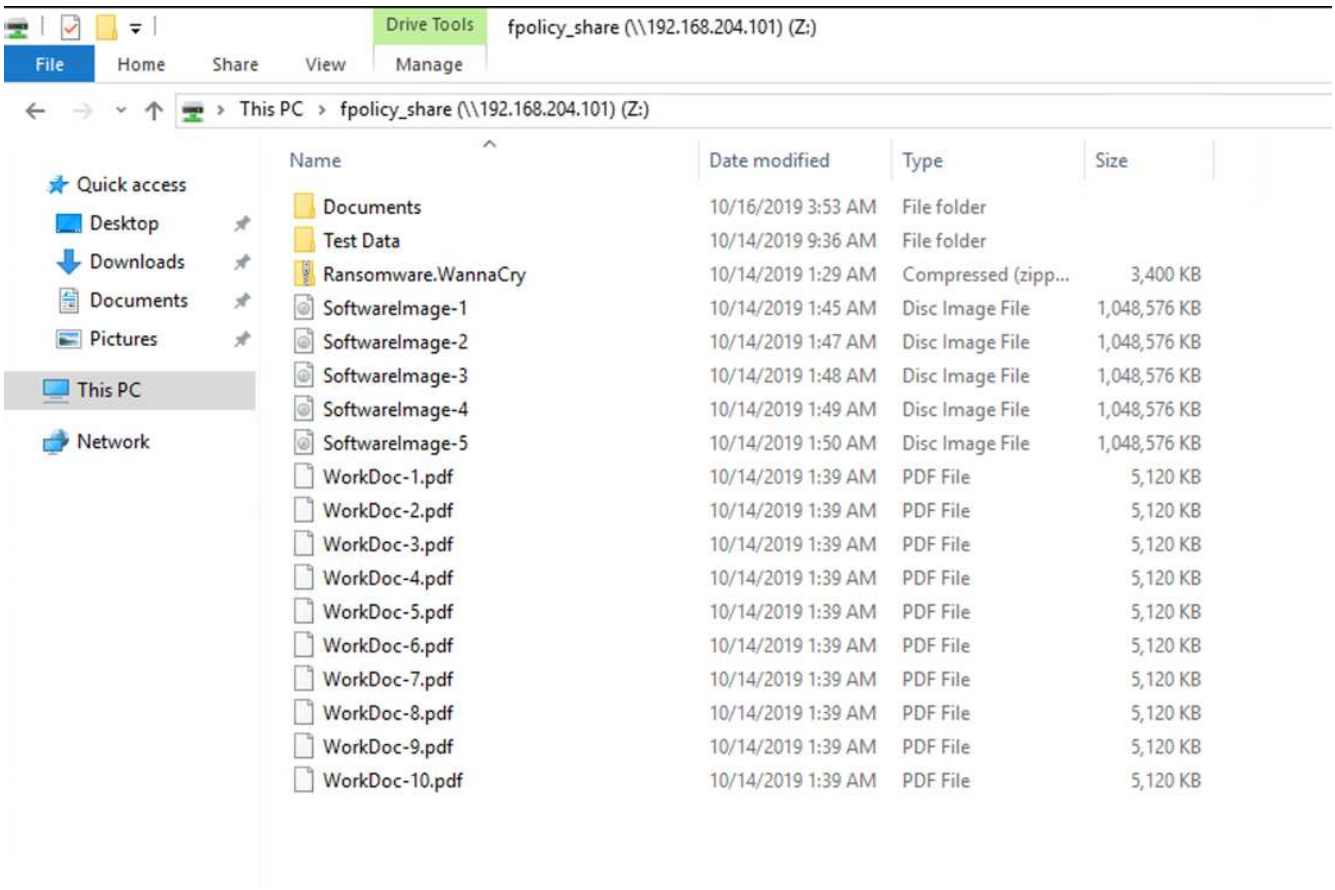
1. Utilizzare la copia Snapshot del volume preso prima dell'attacco per ripristinare la condivisione.



2. Fare clic su OK per avviare l'operazione di ripristino.



3. Visualizzare la condivisione CIFS dopo il ripristino.



Caso 2: WannaCry crittografa il file system all'interno della macchina virtuale e tenta di crittografare la condivisione CIFS mappata protetta tramite FPolicy

Prevenzione

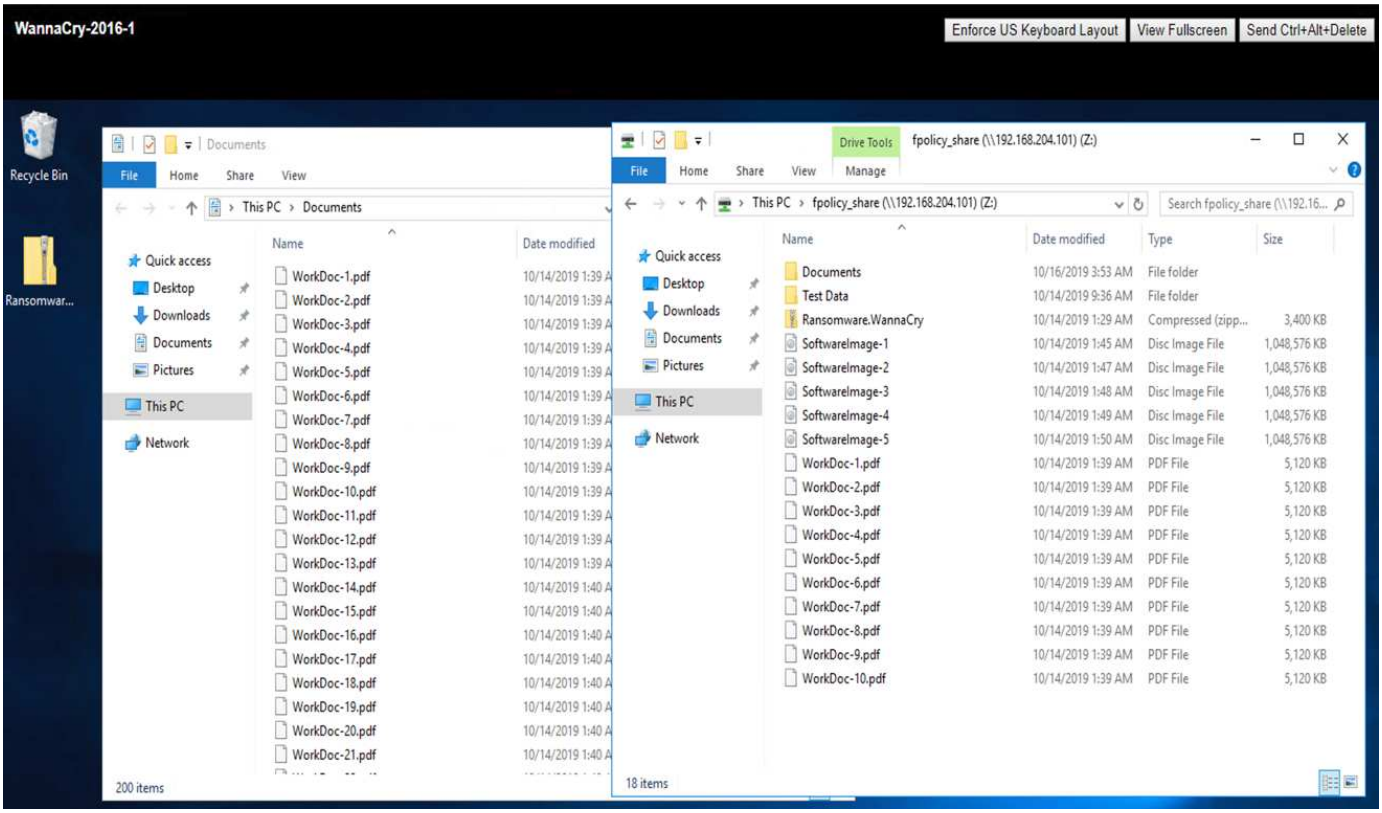
Configura FPolicy

Per configurare FPolicy sulla condivisione CIFS, eseguire i seguenti comandi sul cluster ONTAP:

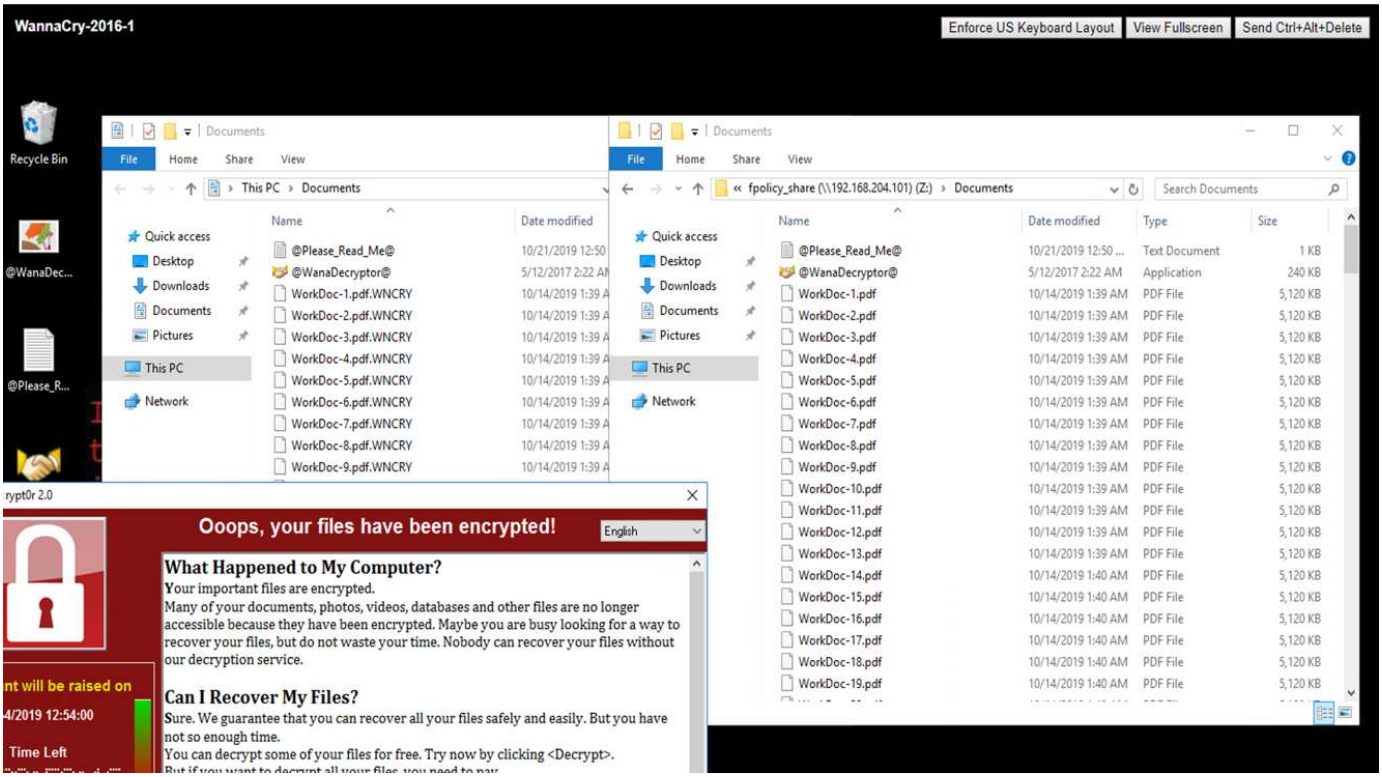
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -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 questo criterio, ai file con estensioni WNCRY, Locky e ad4c non è consentito eseguire le operazioni di creazione, ridenominazione, scrittura o apertura dei file.

Visualizzare lo stato dei file prima dell'attacco: Sono non crittografati e in un sistema pulito.



I file sulla macchina virtuale sono crittografati. Il malware WannaCry tenta di crittografare i file nella condivisione CIFS, ma FPolicy impedisce che influiscano sui file.



Continua le operazioni di business senza pagare il riscatto

Le funzionalità di NetApp descritte in questo documento consentono di ripristinare i dati entro pochi minuti dopo un attacco e prevenire gli attacchi, in modo da poter continuare le operazioni di business senza ostacoli.

È possibile impostare un programma di copia Snapshot per soddisfare l'obiettivo RPO (Recovery Point Objective) desiderato. Le operazioni di ripristino basate su copia Snapshot sono molto rapide, pertanto è possibile raggiungere un obiettivo RTO (Recovery Time Objective) molto basso.

Soprattutto, non è necessario pagare alcun riscatto a seguito di un attacco e si può tornare rapidamente alle operazioni regolari.

Conclusione

Ransomware è un prodotto di crimine organizzato e gli autori degli attacchi non operano con l'etica. Possono astenersi dal fornire la chiave per la decifratura anche dopo aver ricevuto il riscatto. La vittima non solo perde i propri dati, ma anche una notevole quantità di denaro e si trova ad affrontare le conseguenze associate alla perdita dei dati di produzione.

Secondo a. "Articolo di Forbes", solo il 19% delle vittime del ransomware ottiene i propri dati dopo aver pagato il riscatto. Pertanto, gli autori consigliano di non pagare un riscatto in caso di attacco, in quanto ciò rafforza la fiducia dell'utente malintenzionato nel proprio modello di business.

Le operazioni di backup e ripristino dei dati svolgono una parte importante del ripristino ransomware. Pertanto, devono essere inclusi come parte integrante della pianificazione aziendale. L'implementazione di queste operazioni deve essere preventivata in modo da non compromettere le funzionalità di recovery in caso di

attacco.

La chiave è scegliere il partner tecnologico corretto in questo percorso e FlexPod fornisce la maggior parte delle funzionalità necessarie in modo nativo senza costi aggiuntivi in un sistema FAS all-flash.

Ringraziamenti

L'autore desidera ringraziare le seguenti persone per il loro supporto nella creazione di questo documento:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Ulteriori informazioni

Per ulteriori informazioni sulle informazioni descritte in questo documento, consultare i seguenti documenti e/o siti Web:

- Software NetApp Snapshot

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

- Gestione del backup di SnapCenter

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

- Conformità dei dati SnapLock

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

- Documentazione sui prodotti 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 Stealthwatch

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