FlexPod, The Solution to Ransomware

FlexPod

NetApp
March 25, 2024

Table of Contents

FlexPod, The Solution to Ransomware

TR-4802: FlexPod, The Solution to Ransomware

Arvind Ramakrishnan, NetApp

In partnership with:

To understand ransomware, it is necessary to first understand a few key points about cryptography. Cryptographical methods enable the encryption of data with a shared secret key (symmetric key encryption) or a pair of keys (asymmetric key encryption). One of these keys is a widely available public key and the other is an undisclosed private key.

Ransomware is a type of malware that is based on cryptovirology, which is the use of cryptography to build malicious software. This malware can make use of both symmetric and asymmetric key encryption to lock a victim's data and demand a ransom to provide the key to decrypt the victim's data.

How does ransomware work?

The following steps describe how ransomware uses cryptography to encrypt the victim's data without any scope for decryption or recovery by the victim:

1. The attacker generates a key pair as in asymmetric key encryption. The public key that is generated is placed within the malware, and the malware is then released.
2. After the malware has entered the victim's computer or system, it generates a random symmetric key by using a pseudorandom number generator (PRNG) or any other viable random number- generating algorithm.
3. The malware uses this symmetric key to encrypt the victim's data. It eventually encrypts the symmetric key by using the attacker's public key that was embedded in the malware. The output of this step is an asymmetric ciphertext of the encrypted symmetric key and the symmetric ciphertext of the victim's data.
4. The malware zeroizes (erases) the victim's data and the symmetric key that was used to encrypt the data, thus leaving no scope for recovery.
5. The victim is now shown the asymmetric ciphertext of the symmetric key and a ransom value that must be paid in order to obtain the symmetric key that was used to encrypt the data.
6. The victim pays the ransom and shares the asymmetric ciphertext with the attacker. The attacker decrypts the ciphertext with his or her private key, which results in the symmetric key.
7. The attacker shares this symmetric key with the victim, which can be used to decrypt all the data and thus recover from the attack.

Challenges

Individuals and organizations face the following challenges when they are attacked by ransomware:

- The most important challenge is that it takes an immediate toll on the productivity of the organization or the individual. It takes time to return to a state of normalcy, because all the important files must be regained,

and the systems must be secured.

- It could lead to a data breach that contains sensitive and confidential information that belongs to clients or customers and leads to a crisis situation that an organization would clearly want to avoid.
- There is a very good chance of data getting into the wrong hands or being erased completely, which leads to a point of no return that could be disastrous for organizations and individuals.
- After paying the ransom, there is no guarantee that the attacker will provide the key to restore the data.
- There is no assurance that the attacker will refrain from broadcasting the sensitive data in spite of paying the ransom.
- In large enterprises, identifying the loophole that led to a ransomware attack is a tedious task, and securing all the systems involves a lot of effort.

Who is at risk?

Anyone can be attacked by ransomware, including individuals and large organizations. Organizations that do not implement well- defined security measures and practices are even more vulnerable to such attacks. The effect of the attack on a large organization can be several times larger than what an individual might endure.

Ransomware accounts for approximately 28% of all malware attacks. In other words, more than one in four malware incidents is a ransomware attack. Ransomware can spread automatically and indiscriminately through the internet, and, when there is a security lapse, it can enter into the victim’s systems and continue to spread to other connected systems. Attackers tend to target people or organizations that perform a lot of file sharing, have a lot of sensitive and critical data, or maintain inadequate protection against attacks.

Attackers tend to focus on the following potential targets:

- Universities and student communities
- Government offices and agencies
- Hospitals
- Banks

This is not an exhaustive list of targets. You cannot consider yourself safe from attacks if you fall outside of one of these categories.

How does ransomware enter a system or spread?

There are several ways in which ransomware can enter a system or spread to other systems. In today’s world, almost all systems are connected to one another other through the internet, LANs, WANs, and so on. The amount of data that is being generated and exchanged between these systems is only increasing.

Some of the most common ways by which ransomware can spread include methods that we use on a daily basis to share or access data:

- Email
- P2P networks
- File downloads
- Social networking
- Mobile devices
- Connecting to insecure public networks

- Accessing web URLs

Consequences of data loss

The consequences or effects of data loss can reach more widely than organizations might anticipate. The effects can vary depending on the duration of downtime or the time period during which an organization doesn't have access to its data. The longer the attack endures, the bigger the effect on the organization's revenue, brand, and reputation. An organization can also face legal issues and a steep decline in productivity.

As these issues continue to persist over time, they begin to magnify and might end up changing an organization's culture, depending on how it responds to the attack. In today's world, information spreads at a rapid rate and negative news about an organization could cause permanent damage to its reputation. An organization could face huge penalties for data loss, which could eventually lead to the closure of a business.

Financial effects

According to a recent McAfee report, the global costs incurred due to cybercrime are roughly $600 billion, which is approximately 0.8% of global GDP. When this amount is compared against the growing worldwide internet economy of $4.2 trillion, it equates to a 14% tax on growth.

Ransomware takes a significant share of this financial cost. In 2018, the costs incurred due to ransomware attacks were approximately $8 billion—an amount predicted to reach $11.5 billion in 2019.

What is the solution?

Recovering from a ransomware attack with minimal downtime is only possible by implementing a proactive disaster recovery plan. Having the ability to recover from an attack is good, but preventing an attack altogether is ideal.

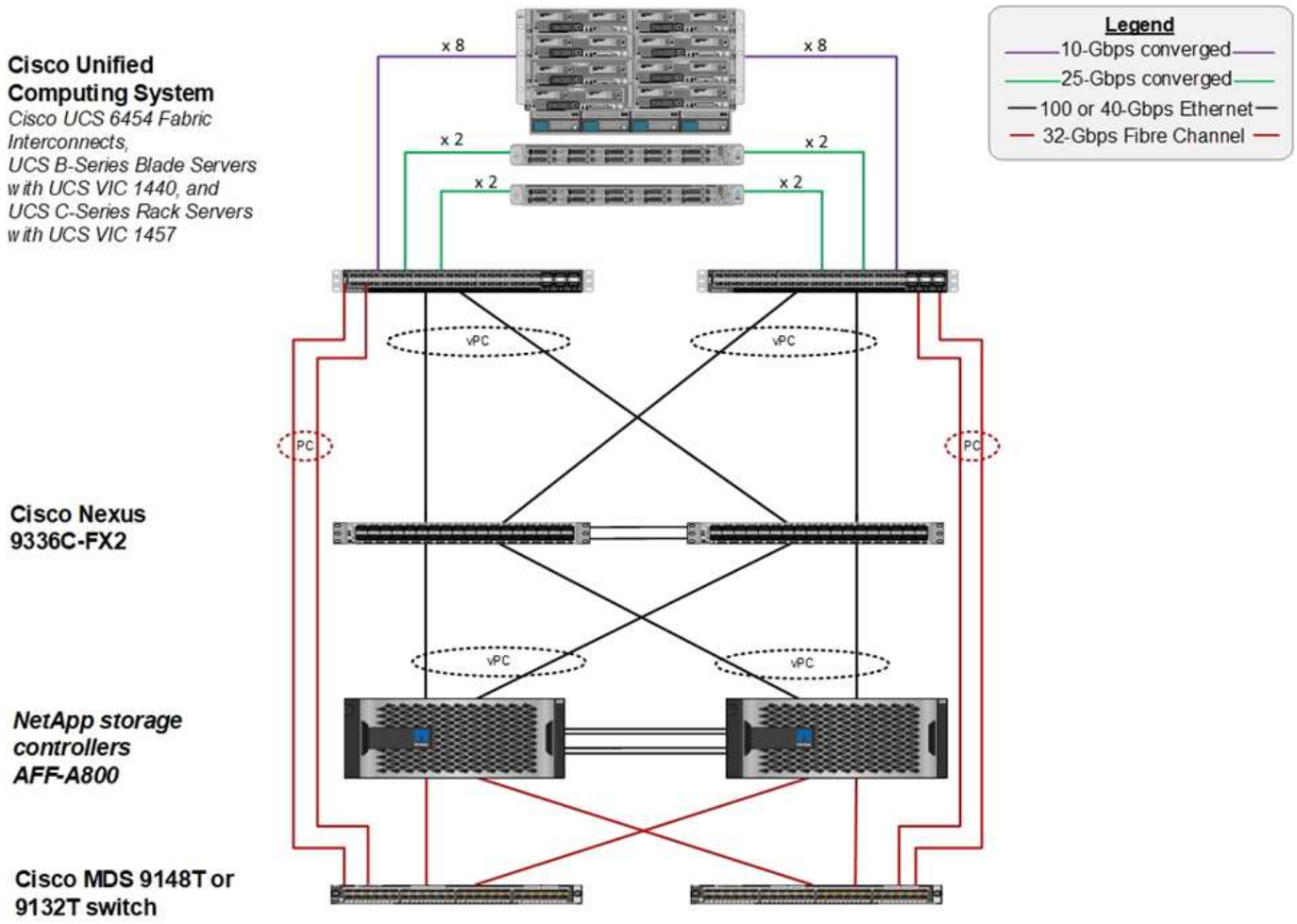
Although there are several fronts that you must review and fix to prevent an attack, the core component that allows you to prevent or recover from an attack is the data center.

The data center design and the features it provides to secure the network, compute, and storage end-points play a critical role in building a secure environment for day-to-day operations. This document shows how the features of a FlexPod hybrid cloud infrastructure can help in quick data recovery in the event of an attack and can also help to prevent attacks altogether.

FlexPod Overview

FlexPod is a predesigned, integrated, and validated architecture that combines Cisco Unified Computing System (Cisco UCS) servers, the Cisco Nexus family of switches, Cisco MDS fabric switches, and NetApp storage arrays into a single, flexible architecture. FlexPod solutions are designed for high availability with no single points of failure, while maintaining cost-effectiveness and design flexibility to support a wide variety of workloads. A FlexPod design can support different hypervisors and bare metal servers and can also be sized and optimized based on customer workload requirements.

The figure below illustrates the FlexPod architecture and clearly highlights the high availability across all the layers of the stack. The infrastructure components of storage, network, and compute are configured in such a way that the operations can instantaneously fail over to the surviving partner in case one of the components fail.



A major advantage for a FlexPod system is that it is predesigned, integrated, and validated for several workloads. Detailed design and deployment guides are published for every solution validation. These documents include the best practices that you must employ for workloads to run seamlessly on FlexPod. These solutions are built with the best- in-class compute, network, and storage products and a host of features that focus on security and hardening of the entire infrastructure.

IBM's X-Force Threat Intelligence Index states, "Human error responsible for two-thirds of compromised records including historic 424% jump in misconfigured cloud infrastructure."

With a FlexPod system, you can avoid misconfiguring your infrastructure by using automation through Ansible playbooks that perform an end-to-end setup of the infrastructure according to the best practices described in Cisco Validated Designs (CVDs) and NetApp Verified Architectures (NVAs).

Ransomware protection measures

This section discusses the key features of NetApp ONTAP data management software and the tools for Cisco UCS and Cisco Nexus that you can use to effectively protect and recover from ransomware attacks.

Storage: NetApp ONTAP

ONTAP software provides many features useful for data protection, most of which are free of charge to customers who have an ONTAP system. You can use the following features at all times to safeguard data from

attacks:

- **NetApp Snapshot technology.** A Snapshot copy is a read-only image of a volume that captures the state of a file system at a point in time. These copies help protect data with no effect on system performance and, at the same time, do not occupy a lot of storage space. NetApp recommends that you create a schedule for the creation of Snapshot copies. You should also maintain a long retention time because some malware can go dormant and then reactivate weeks or months after an infection. In the event of an attack, the volume can be rolled back using a Snapshot copy that was taken before the infection.
- **NetApp SnapRestore technology.** SnapRestore data recovery software is extremely useful to recover from data corruption or to revert only the file contents. SnapRestore does not revert the attributes of a volume; it is much faster than what an administrator can achieve by copying files from the Snapshot copy to the active file system. The speed at which data can be recovered is helpful when many files must be recovered as quickly as possible. In the event of an attack, this highly efficient recovery process helps to get business back online quickly.
- **NetApp SnapCenter technology.** SnapCenter software uses NetApp storage-based backup and replication functions to provide application- consistent data protection. This software integrates with enterprise applications and provides application- specific and database- specific workflows to meet the needs of application, database, and virtual infrastructure administrators. SnapCenter provides an easy-to-use enterprise platform to securely coordinate and manage data protection across applications, databases, and file systems. Its ability to provide application- consistent data protection is critical during data recovery because it makes it easy to restore applications to a consistent state more quickly.
- **NetApp SnapLock technology.** SnapLock provides a special purpose volume in which files can be stored and committed to a nonerasable, nonrewritable state. The user's production data residing in a FlexVol volume can be mirrored or vaulted to a SnapLock volume through NetApp SnapMirror or SnapVault technology, respectively. The files in the SnapLock volume, the volume itself, and its hosting aggregate cannot be deleted until the end of the retention period.
- **NetApp FPolicy technology.** Use FPolicy software to prevent attacks by disallowing operations on files with specific extensions. An FPolicy event can be triggered for specific file operations. The event is tied to a policy, which calls out the engine it needs to use. You might configure a policy with a set of file extensions that could potentially contain ransomware. When a file with a disallowed extension tries to perform an unauthorized operation, FPolicy prevents that operation from executing.

Network: Cisco Nexus

Cisco NX OS software supports the NetFlow feature that enables enhanced detection of network anomalies and security. NetFlow captures the metadata of every conversation on the network, the parties involved in the communication, the protocol being used, and the duration of the transaction. After the information is aggregated and analyzed, it can provide insight into normal behavior.

The collected data also allows identification of questionable patterns of activity, such as malware spreading across the network, which might otherwise go unnoticed.

NetFlow uses flows to provide statistics for network monitoring. A flow is a unidirectional stream of packets that arrives on a source interface (or VLAN) and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow. You can export the data that NetFlow gathers for your flows by using a flow exporter to a remote NetFlow collector, such as Cisco Stealthwatch. Stealthwatch uses this information for continuous monitoring of the network and provides real-time threat detection and incident response forensics if a ransomware outbreak occurs.

Compute: Cisco UCS

Cisco UCS is the compute endpoint in a FlexPod architecture. You can use several Cisco products that can

help to secure this layer of the stack at the operating system level.

You can implement the following key products in the compute or application layer:

- **Cisco Advanced Malware Protection (AMP) for Endpoints.** Supported on Microsoft Windows and Linux operating systems, this solution integrates prevention, detection, and response capabilities. This security software prevents breaches, blocks malware at the point of entry, and continuously monitors and analyzes file and process activity to rapidly detect, contain, and remediate threats that can evade front-line defenses.

  The Malicious Activity Protection (MAP) component of AMP continually monitors all endpoint activity and provides run-time detection and blocking of abnormal behavior of a running program on the endpoint. For example, when endpoint behavior indicates ransomware, the offending processes are terminated, preventing endpoint encryption and stopping the attack.

- **Cisco Advanced Malware Protection for Email Security.** Emails have become the prime vehicle to spread malware and to carry out cyber-attacks. On average, approximately 100 billion emails are exchanged in a single day, which provides attackers with an excellent penetration vector into user's systems. Therefore, it is absolutely essential to defend against this line of attack.

  AMP analyzes emails for threats such as zero-day exploits and stealthy malware hidden in malicious attachments. It also uses industry-leading URL intelligence to combat malicious links. It gives users advanced protection against spear phishing, ransomware, and other sophisticated attacks.

- **Next-Generation Intrusion Prevention System (NGIPS).** Cisco Firepower NGIPS can be deployed as a physical appliance in the datacenter or as a virtual appliance on VMware (NGIPSv for VMware). This highly effective intrusion prevention system provides reliable performance and a low total cost of ownership. Threat protection can be expanded with optional subscription licenses to provide AMP, application visibility and control, and URL filtering capabilities. Virtualized NGIPS inspects traffic between virtual machines (VMs) and make it easier to deploy and manage NGIPS solutions at sites with limited resources, increasing protection for both physical and virtual assets.

Protect and recover data on FlexPod

This section describes how an end user's data can be recovered in the event of an attack and how attacks can be prevented by using a FlexPod system.

Testbed overview

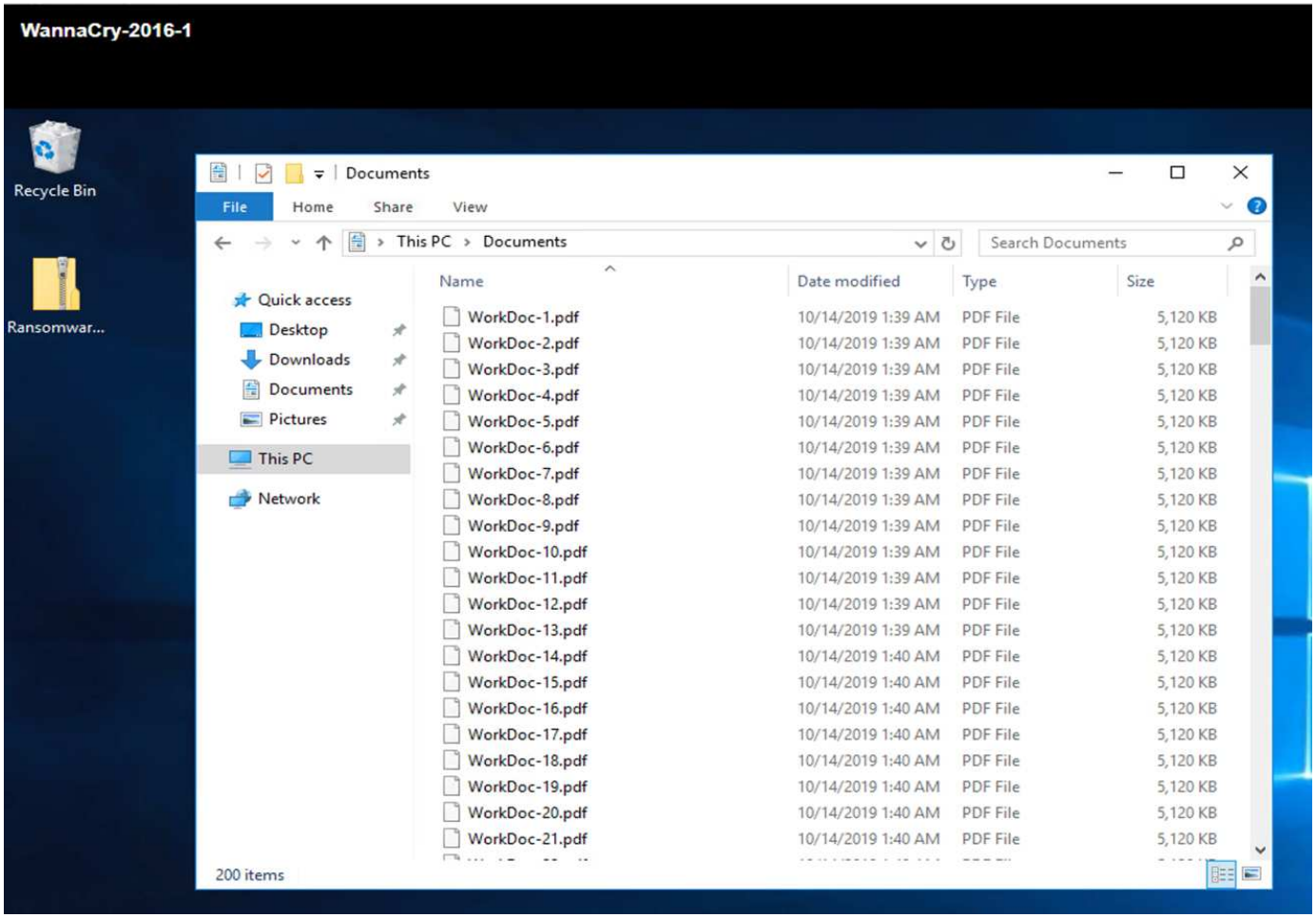
To showcase FlexPod detection, remediation, and prevention, a testbed was built based on the guidelines that are specified in the latest platform CVD available at the time this document was authored: FlexPod Datacenter with VMware vSphere 6.7 U1, Cisco UCS 4th Generation, and NetApp AFF A-Series CVD.

A Windows 2016 VM, which provided a CIFS share from NetApp ONTAP software, was deployed in the VMware vSphere infrastructure. Then NetApp FPolicy was configured on the CIFS share to prevent the execution of files with certain extension types. NetApp SnapCenter software was also deployed to manage the Snapshot copies of the VMs in the infrastructure to provide application- consistent Snapshot copies.

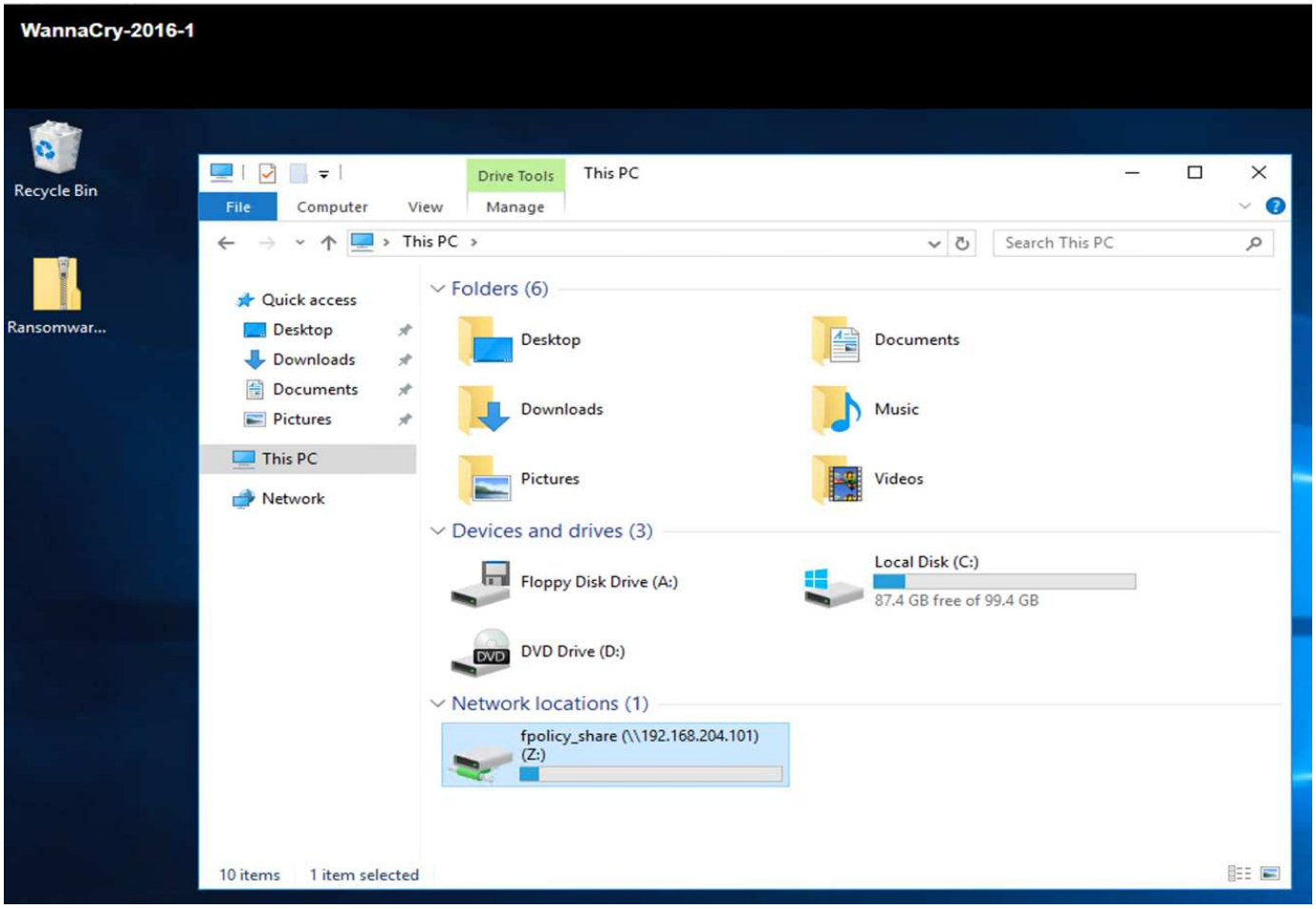
State of VM and its files prior to an attack

This section provides shows the state of the files prior to an attack on the VM and the CIFS share that was mapped to it.

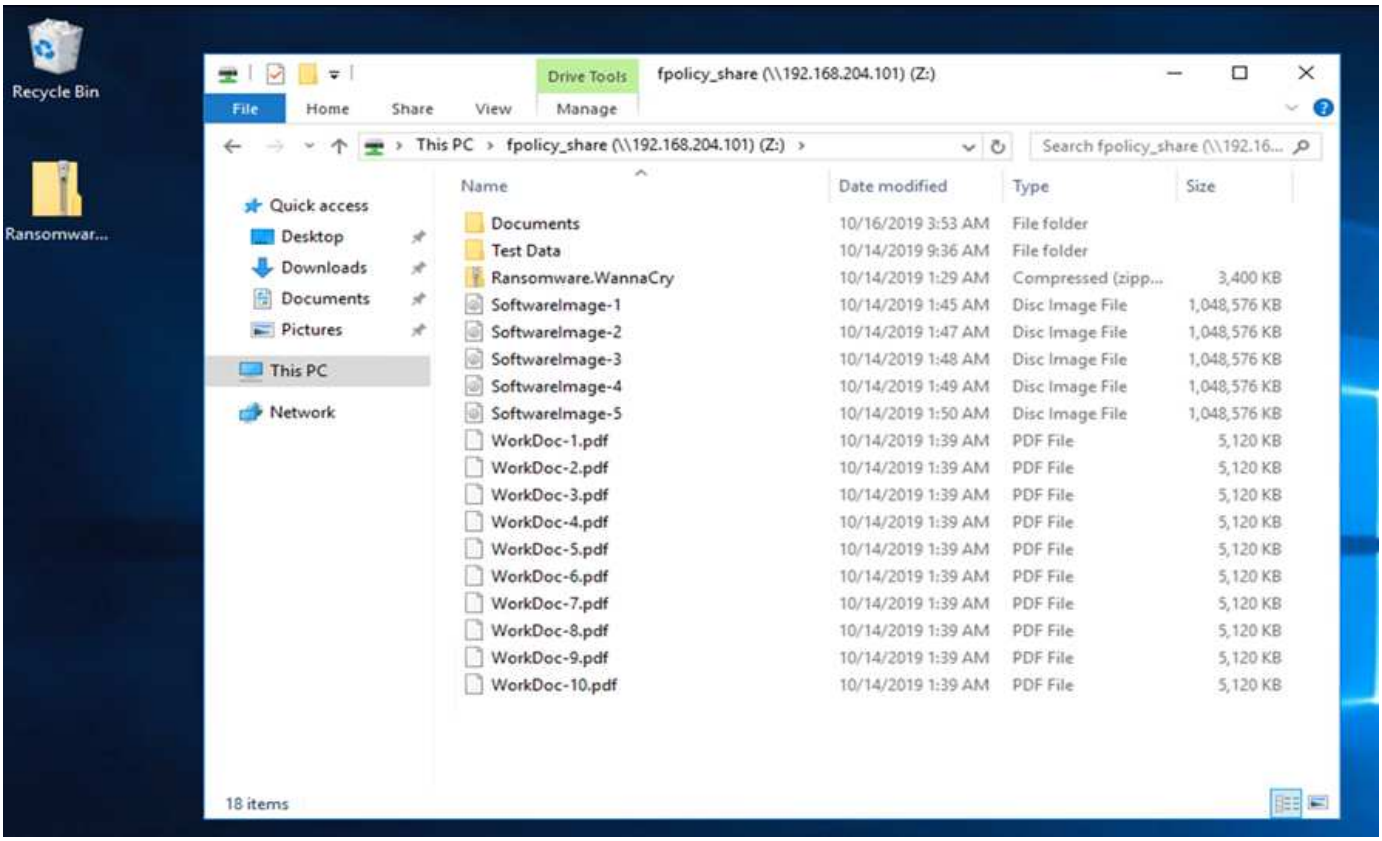
The Documents folder of the VM had a set of PDF files that have not yet been encrypted by the WannaCry malware.



The following screenshot shows the CIFS share that was mapped to the VM.



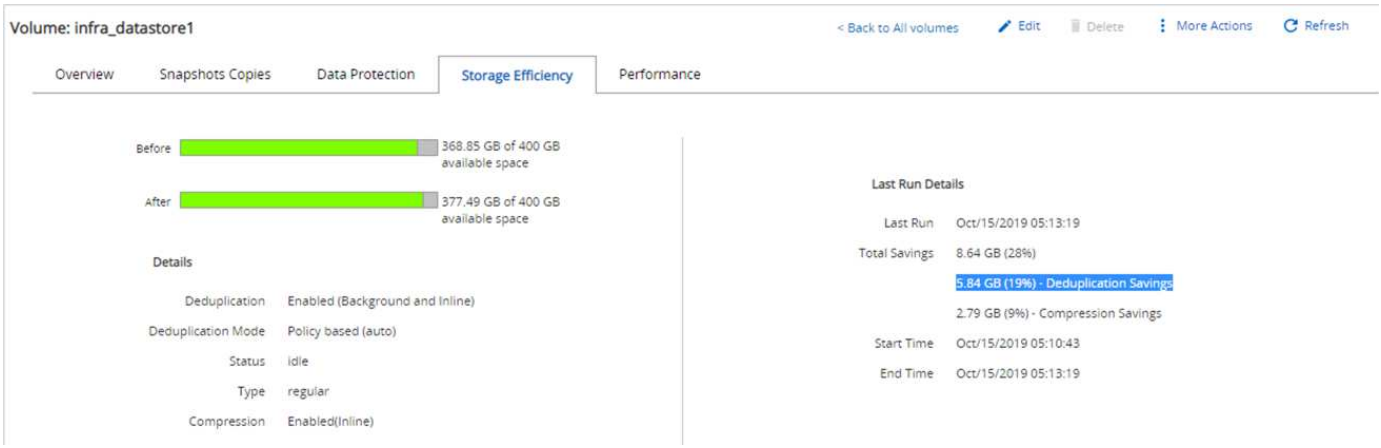
The following screenshot shows the files on the CIFS share `fpolicy_share` that have not yet been encrypted by the WannaCry malware.



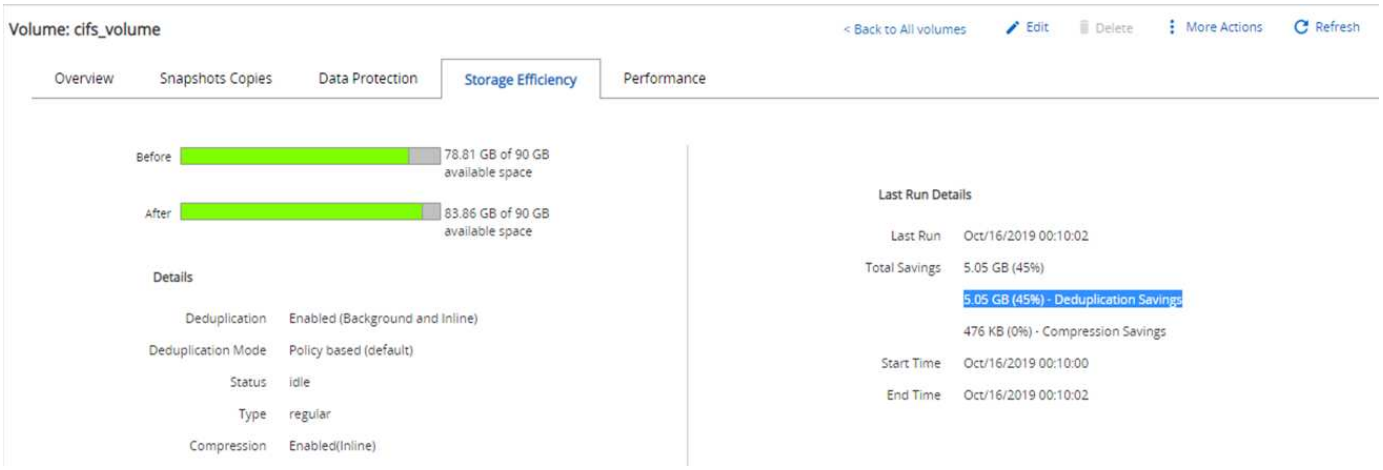
Deduplication and Snapshot information before an attack

The storage efficiency details and size of the Snapshot copy prior to an attack are indicated and used as a reference during the detection phase.

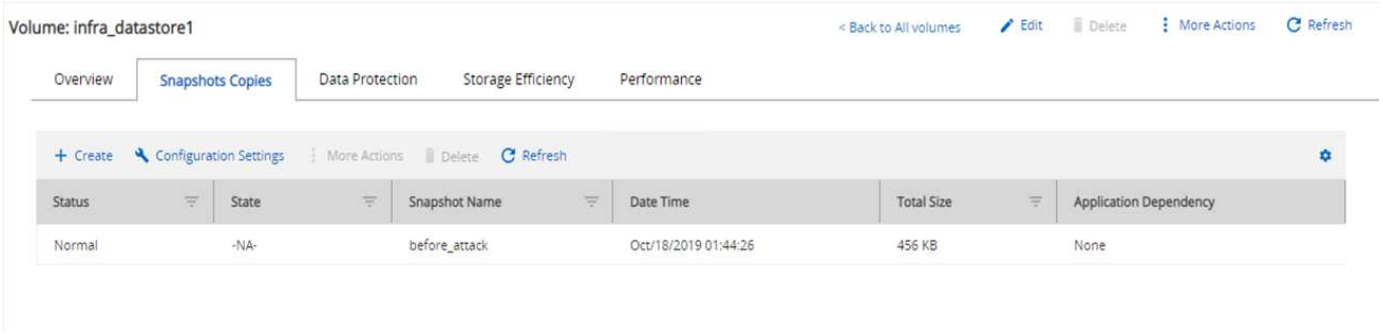
Storage savings of 19% were achieved with deduplication on the volume hosting the VM.



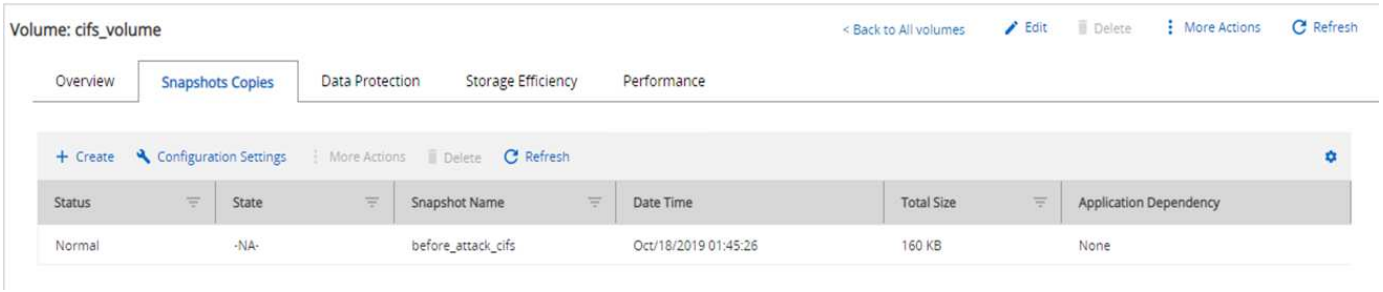
Storage savings of 45% were achieved with deduplication on the CIFS share `fpolicy_share`.



A Snapshot copy size of 456KB was observed for the volume hosting the VM.



A Snapshot copy size of 160KB was observed for the CIFS share `fpolicy_share`.



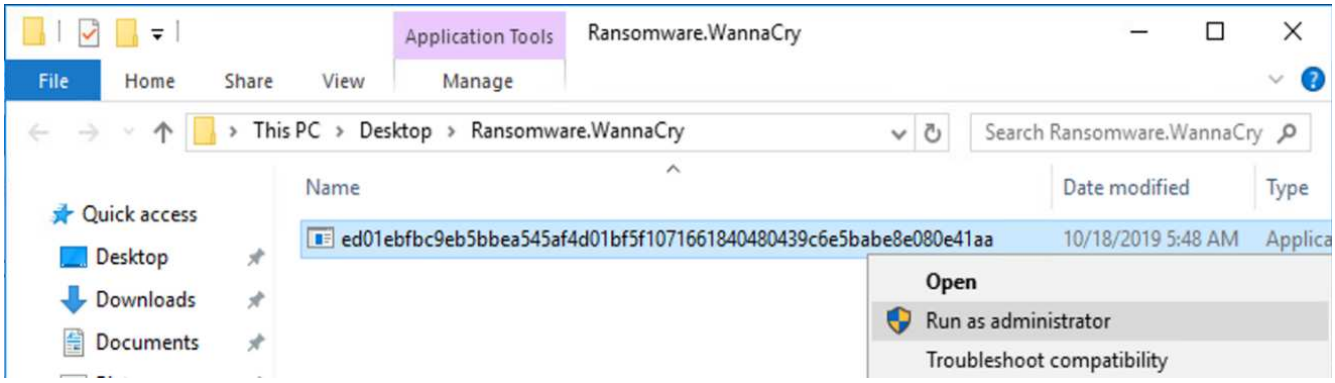
WannaCry infection on VM and CIFS share

In this section, we show how the WannaCry malware was introduced into the FlexPod environment and the subsequent changes to the system that were observed.

The following steps demonstrate how the WannaCry malware binary was introduced into the VM:

1. The secured malware was extracted.

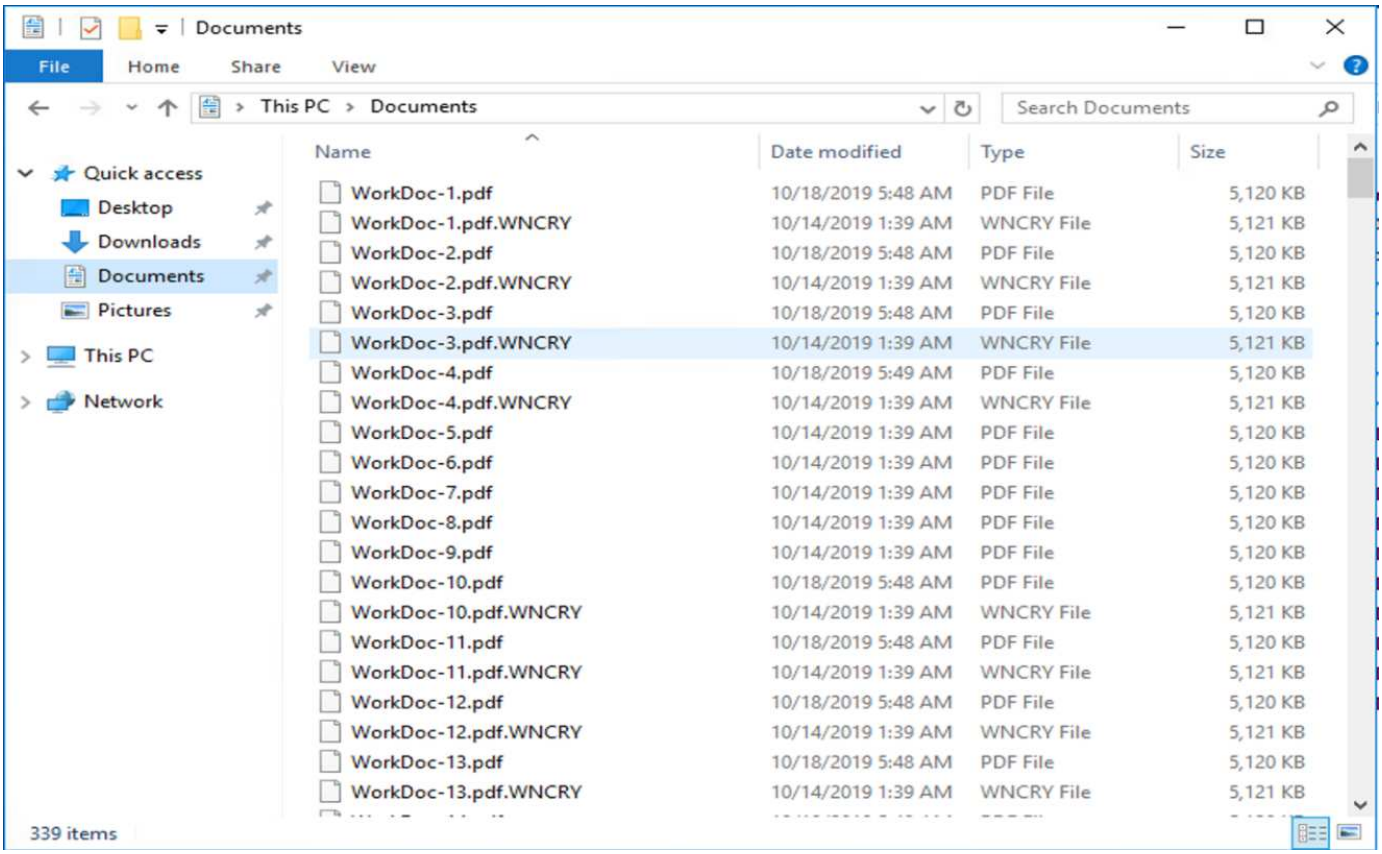
2. The binary was executed.



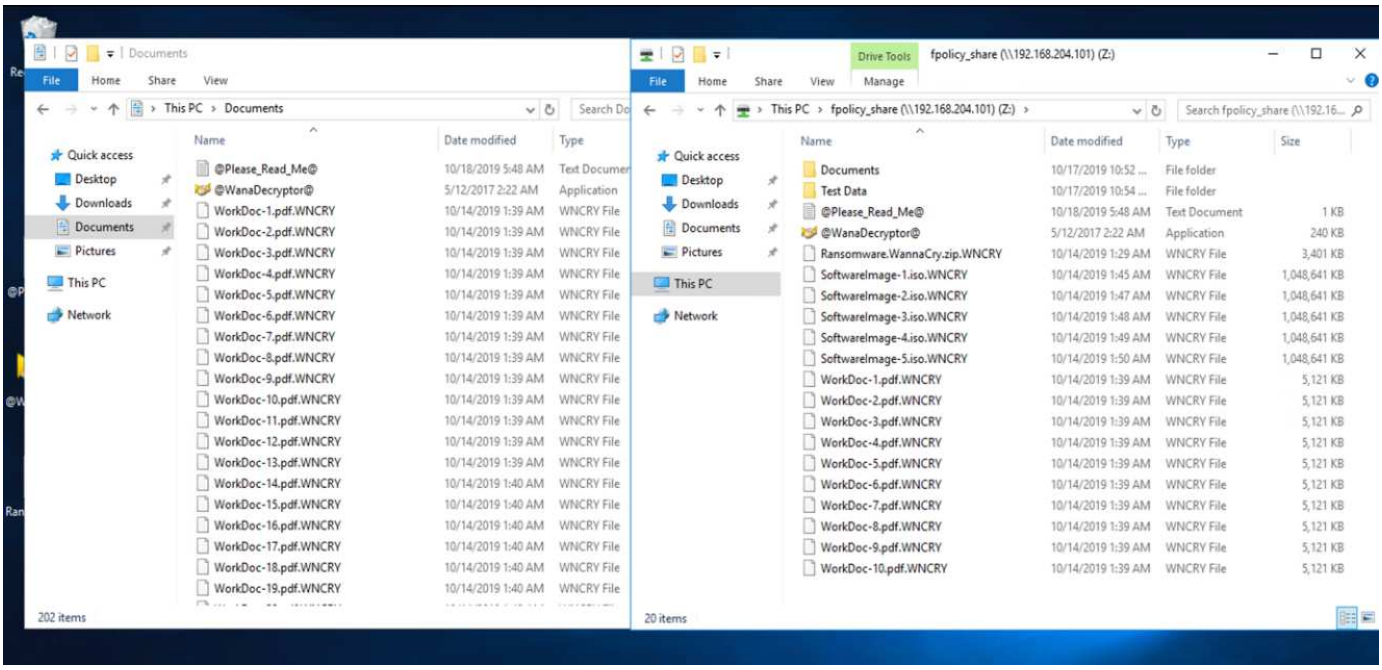
Case 1: WannaCry encrypts the file system within the VM and mapped CIFS share

The local file system and the mapped CIFS share were encrypted by the WannaCry malware.

Malware starts to encrypt files with WNCRY extensions.



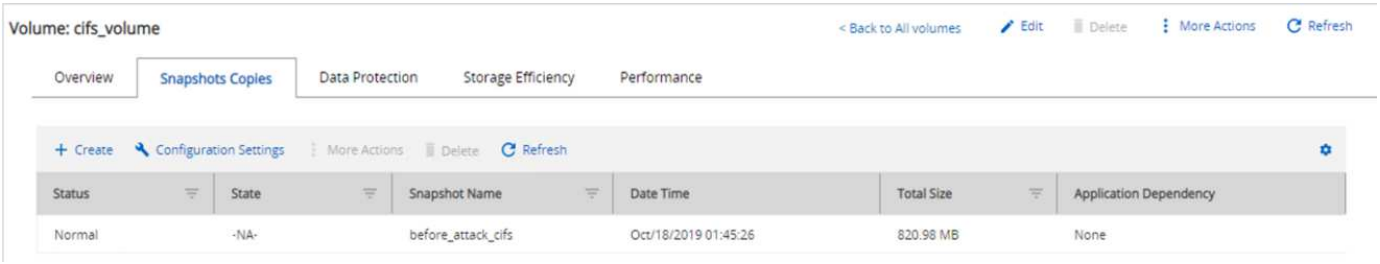
The malware encrypts all the files in the local VM and the mapped share.



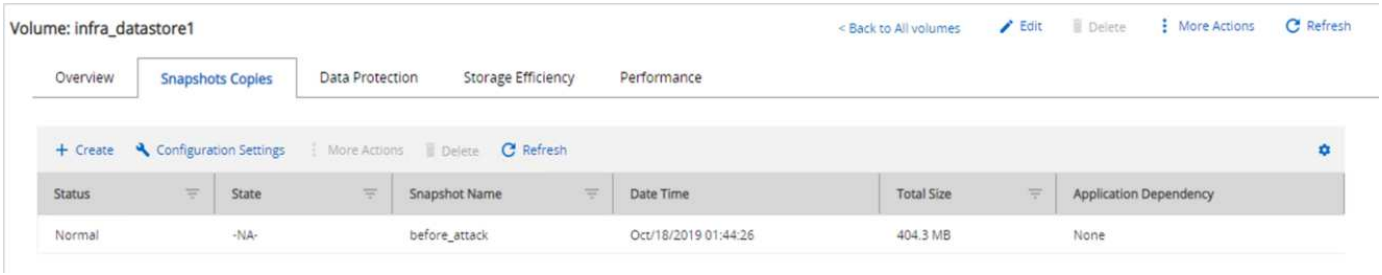
Detection

From the moment the malware started to encrypt the files, it triggered an exponential increase in the size of the Snapshot copies and an exponential decrease in the storage efficiency percentage.

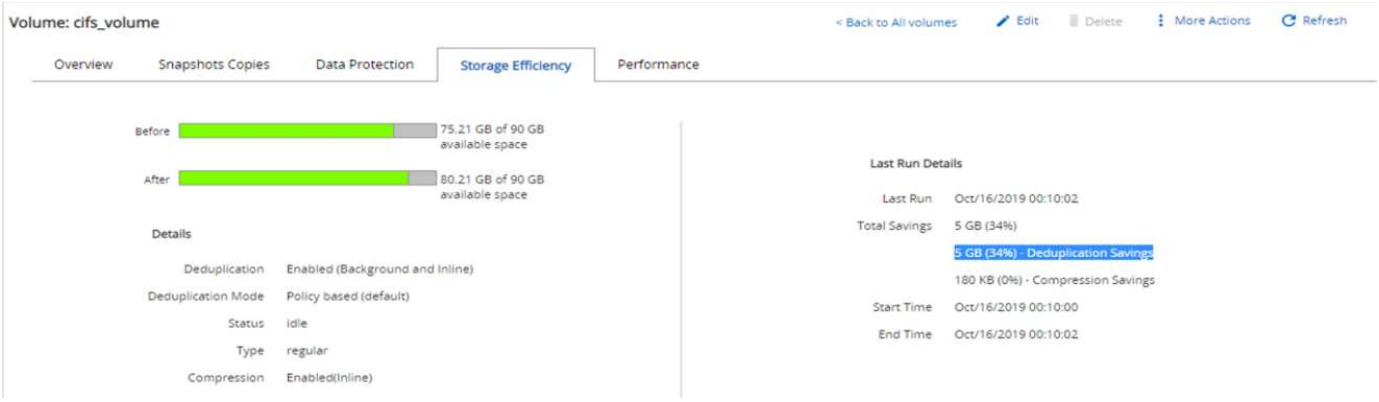
We detected a dramatic increase in the Snapshot size to 820.98MB for the volume hosting the CIFS share during the attack.



We detected an increase in the Snapshot copy size to 404.3MB for the volume hosting the VM.



The storage efficiency for the volume hosting the CIFS share decreased to 34%.



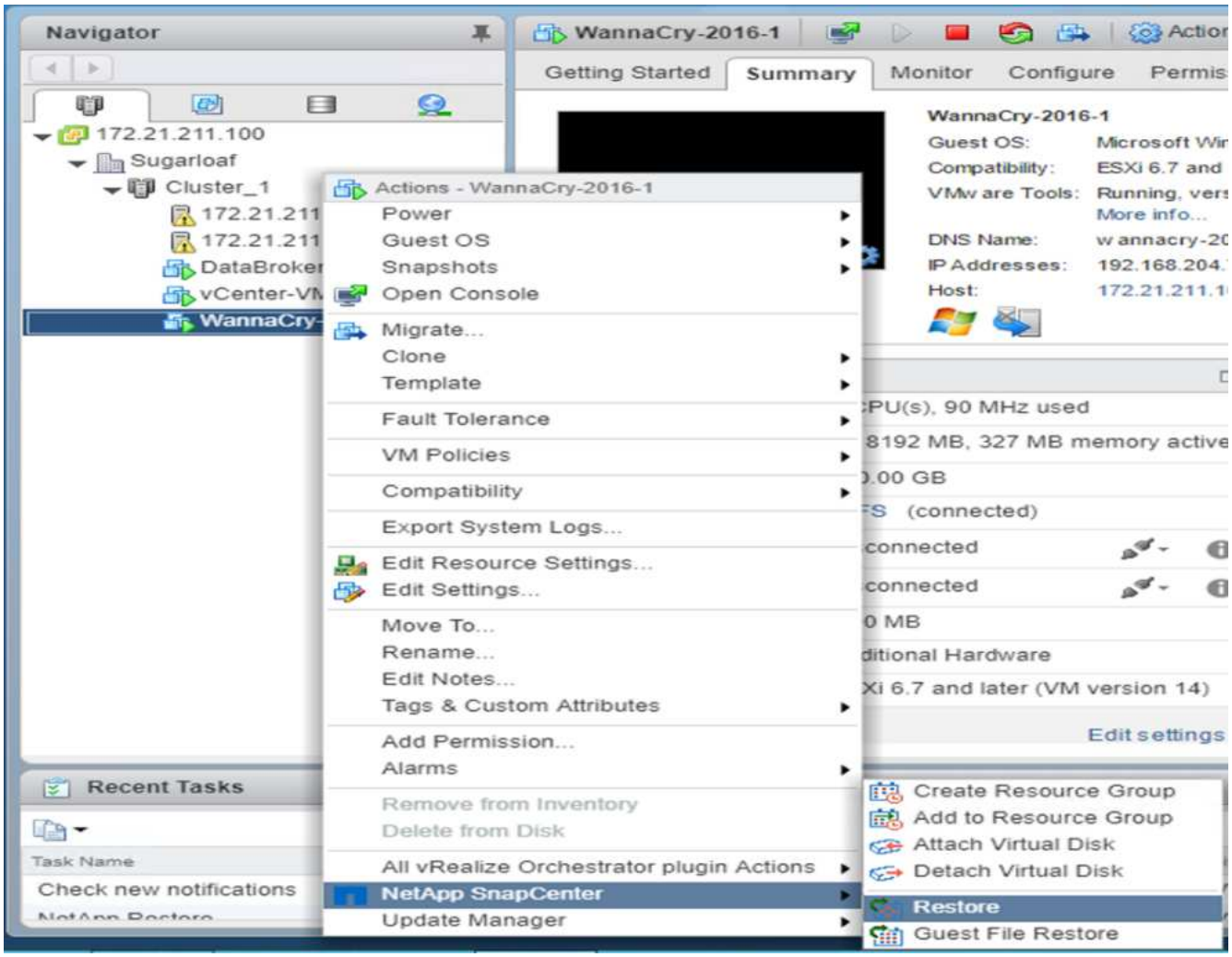
Remediation

Restore the VM and mapped CIFS share by using a clean Snapshot copy create prior to the attack.

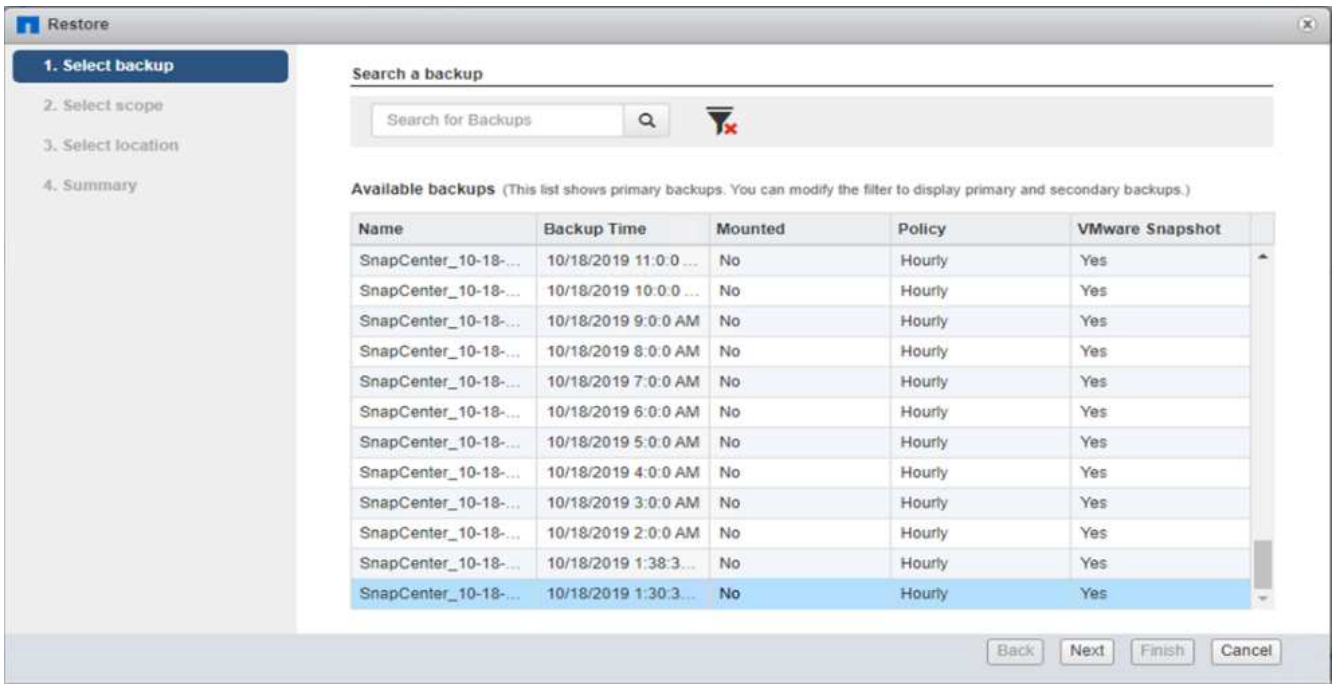
Restore VM

To restore the VM, complete the following steps:

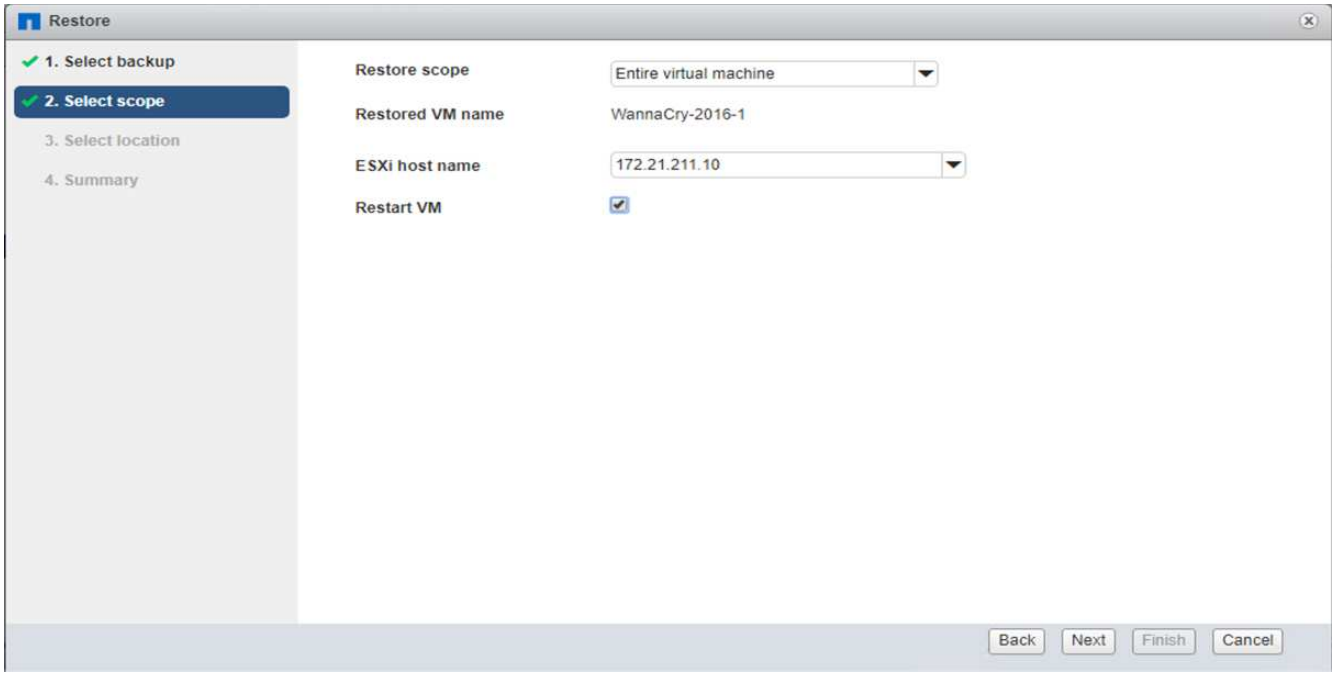
1. Use the Snapshot copy you created with SnapCenter to restore the VM.



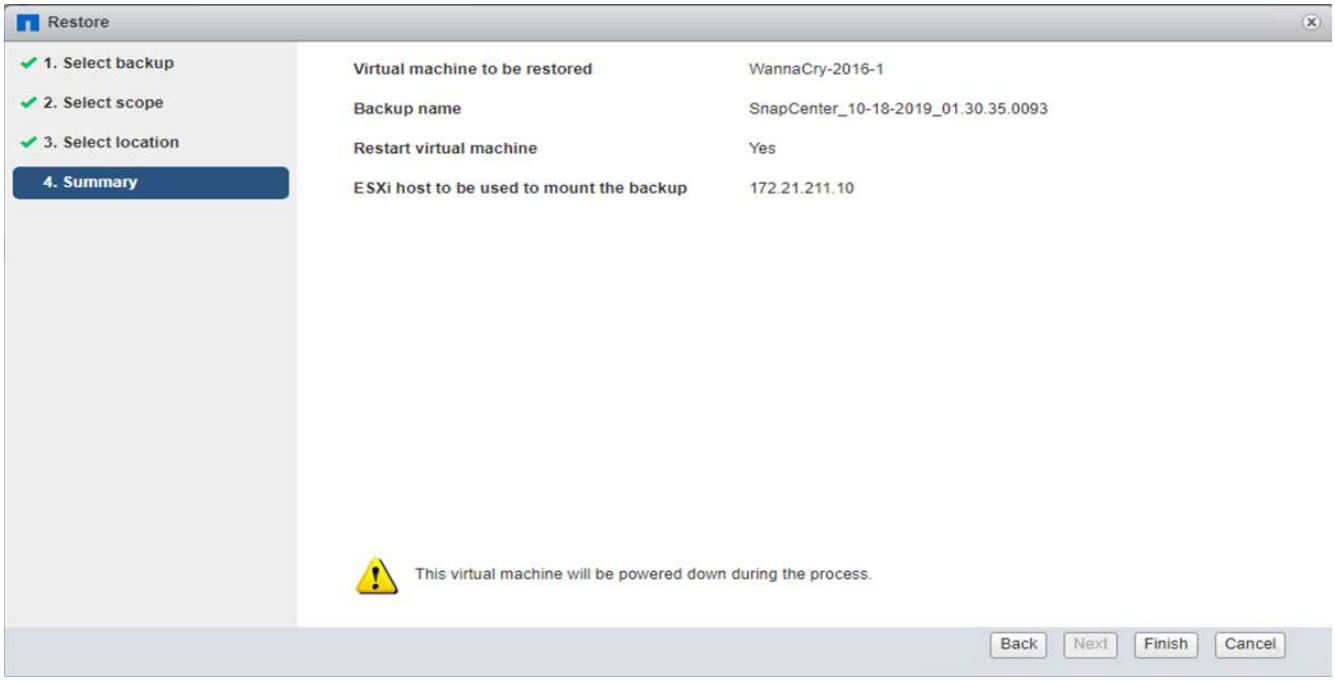
2. Select the desired VMware- consistent Snapshot copy for restore.



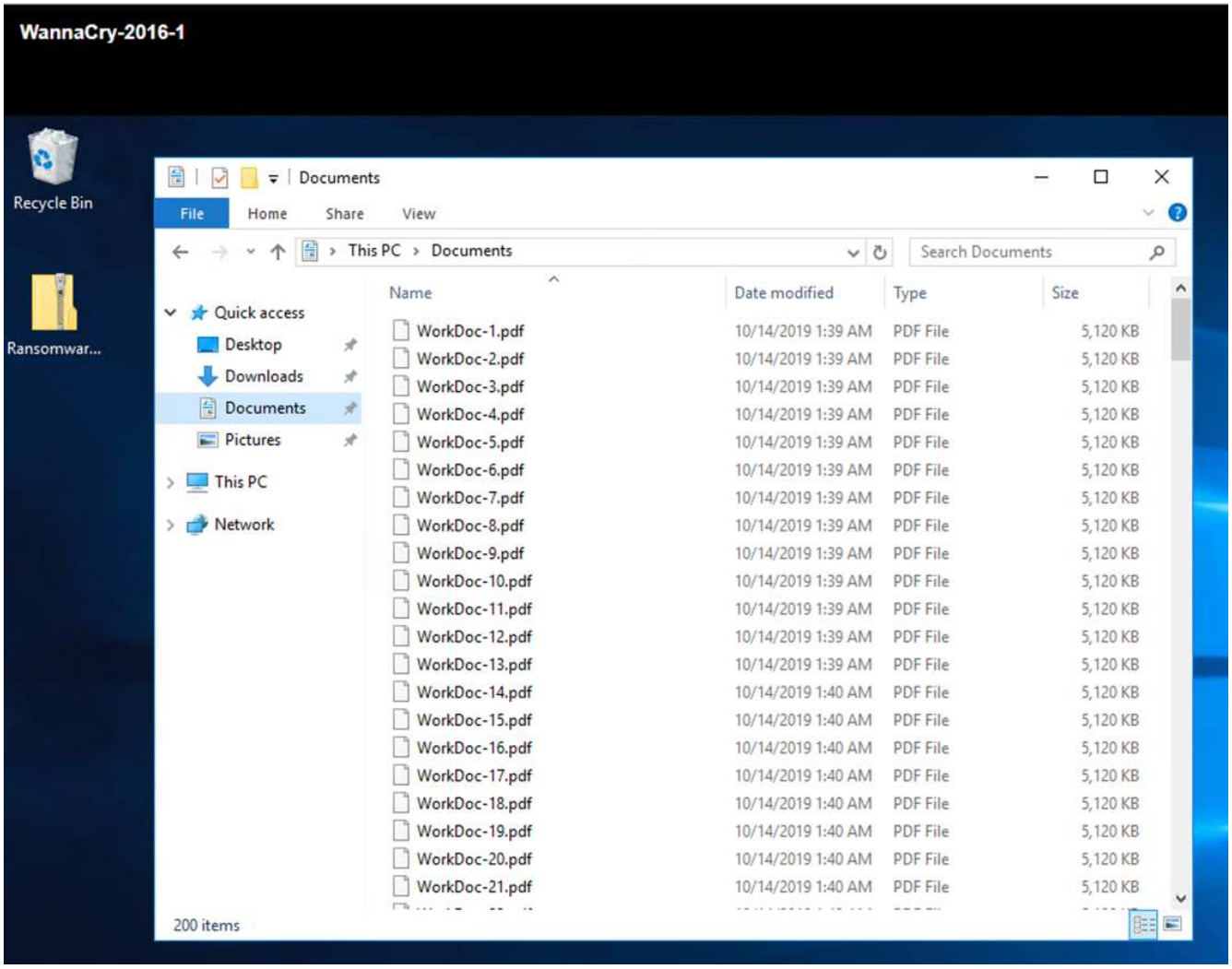
3. The entire VM is restored and restarted.



4. Click Finish to start the restore process.



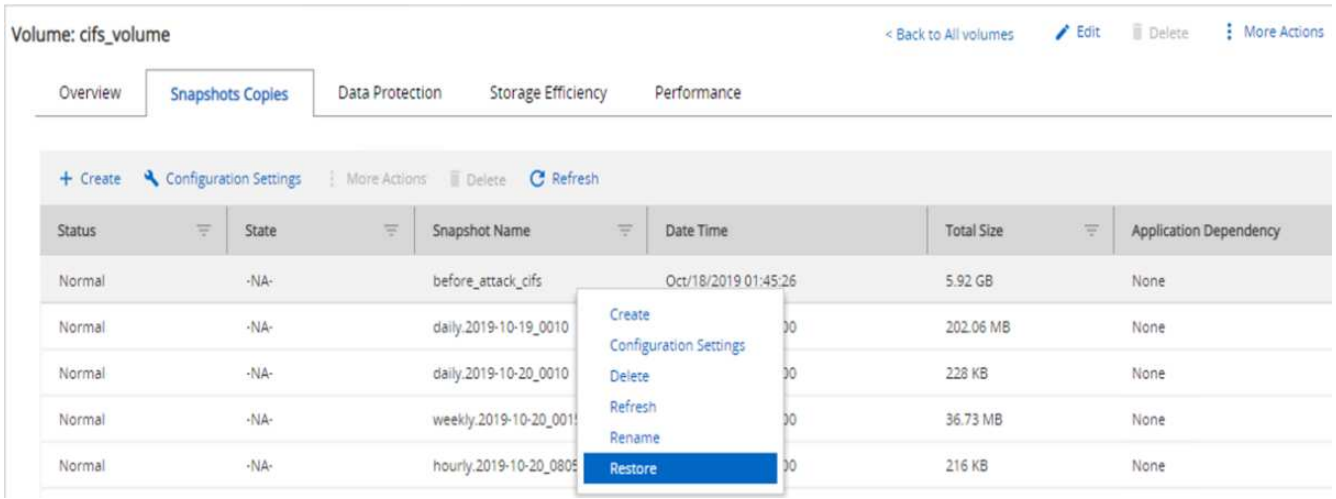
5. The VM and its files are restored.



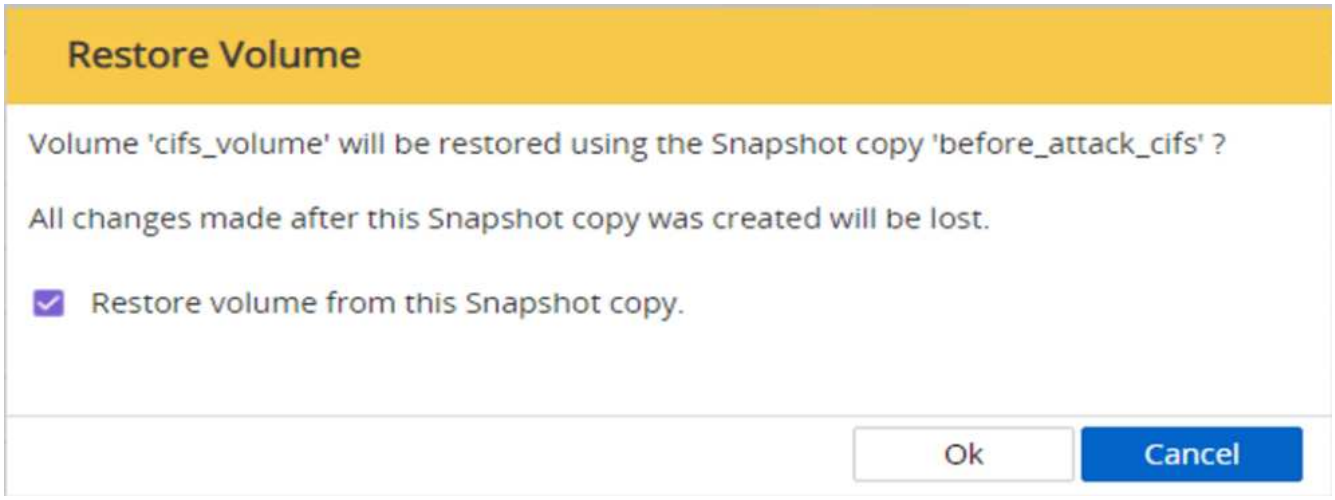
Restore CIFS Share

To restore the CIFS share, complete the following steps:

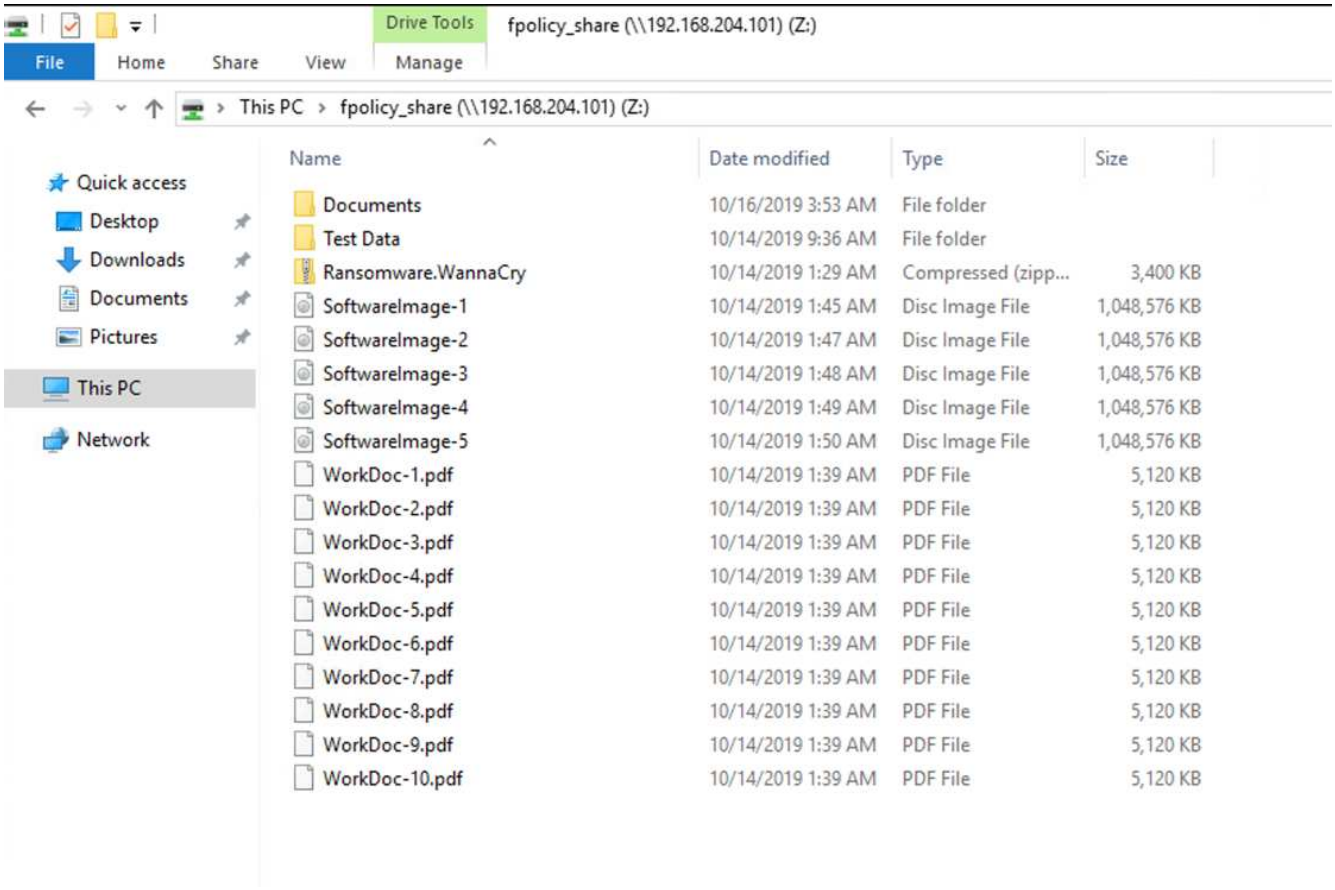
1. Use the Snapshot copy of the volume taken prior to the attack to restore the share.



2. Click OK to initiate the restore operation.



3. View the CIFS share after the restore.



Case 2: WannaCry encrypts file system within the VM and tries to encrypt the mapped CIFS share that is protected through FPolicy

Prevention

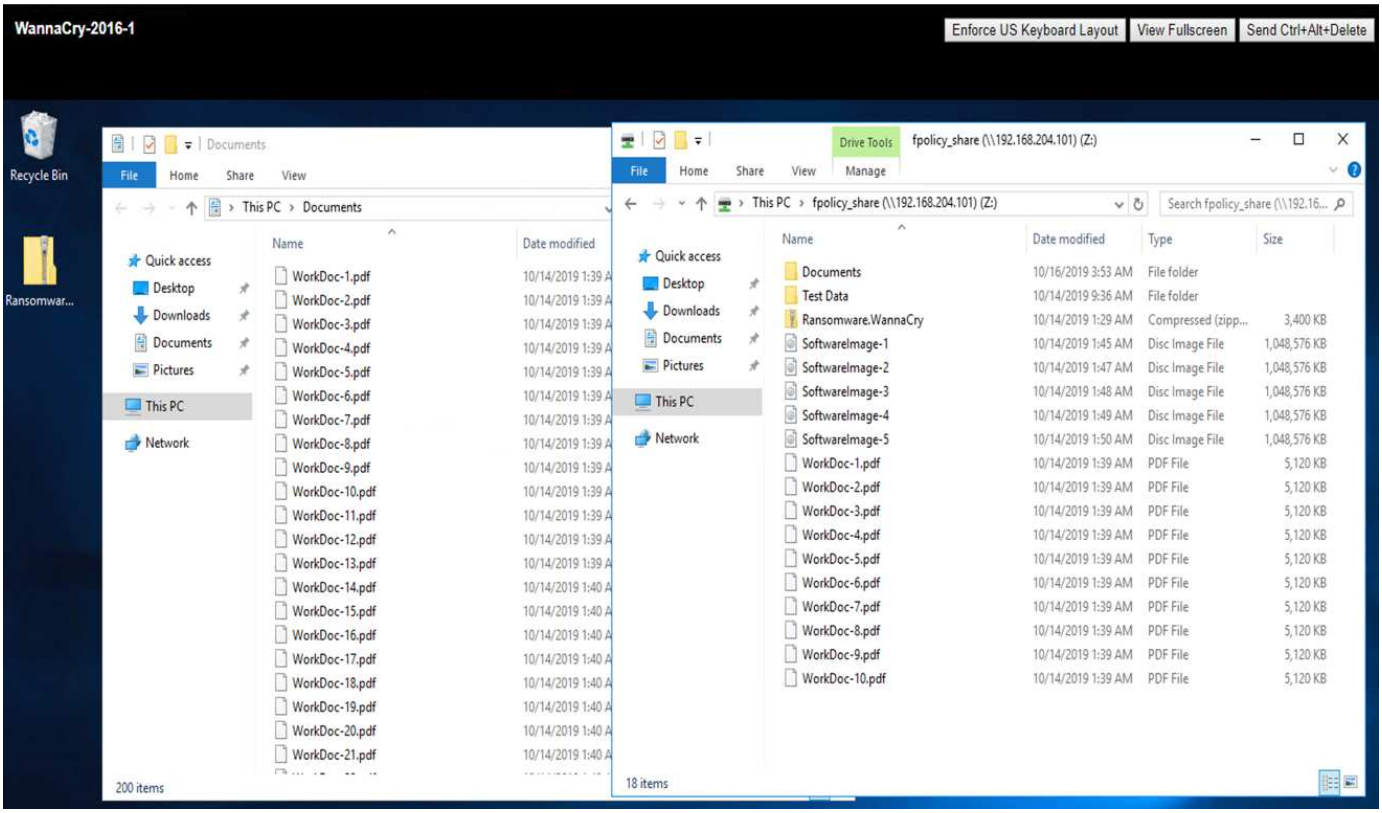
Configure FPolicy

To configure FPolicy on the CIFS share, run the following commands on the ONTAP cluster:

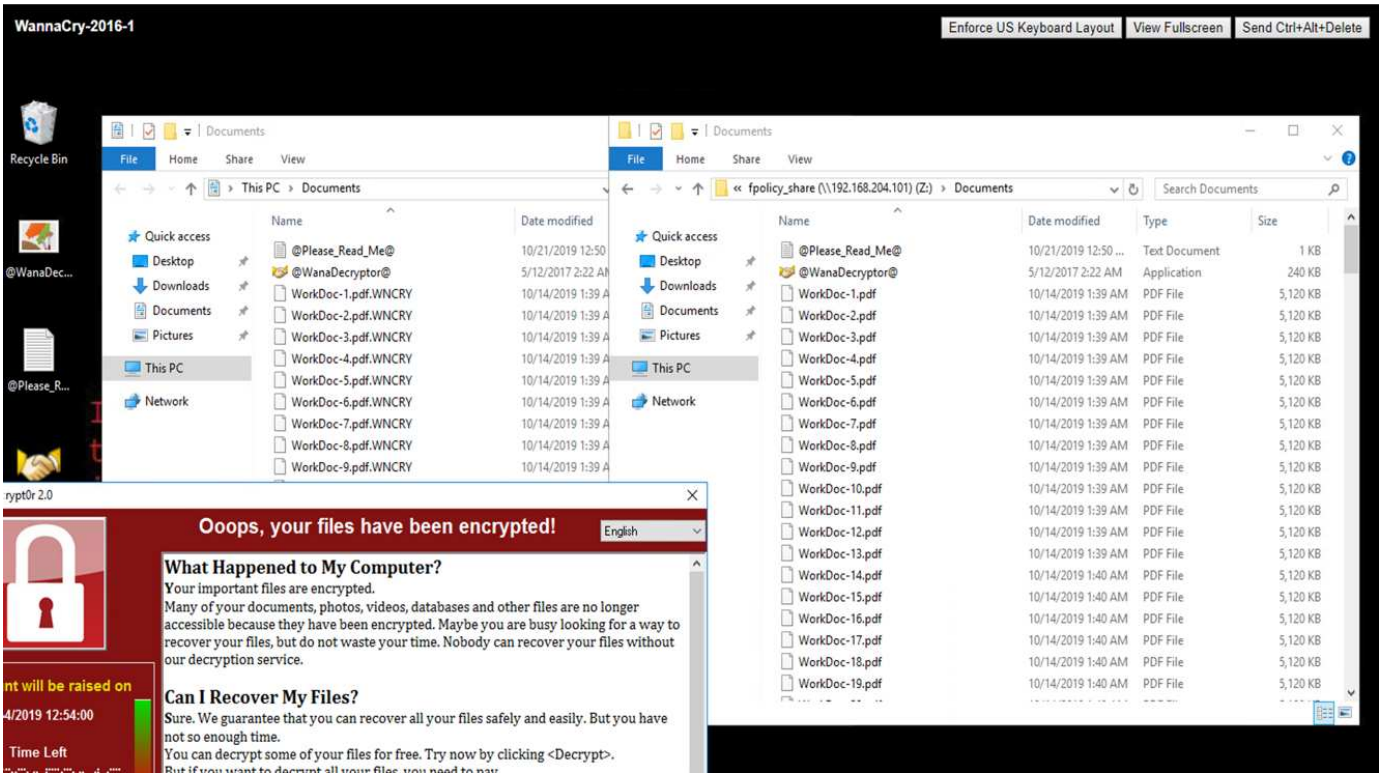
```
vserver fpolicy policy event create -vserver infra_svm -event-name
Ransomware_event -protocol cifs -file-operations create,rename,write,open
vserver fpolicy policy create -vserver infra_svm -policy-name
Ransomware_policy -events Ransomware_event -engine native
vserver fpolicy policy scope create -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
```

With this policy, files with extensions WNCRY, Locky, and ad4c are not allowed to perform the file operations create, rename, write, or open.

View the status of files prior to attack—they are unencrypted and in a clean system.



The files on the VM are encrypted. The WannaCry malware tries to encrypt the files in the CIFS share, but FPolicy prevents it from affecting the files.



Continue business operations without paying ransom

The NetApp capabilities described in this document help you restore data within minutes after an attack and prevent attacks in the first place so that you can continue business operations unhindered.

A Snapshot copy schedule can be set to meet the desired recovery point objective (RPO). Snapshot copy-based restore operations are very quick; therefore, a very low recovery time objective (RTO) can be achieved.

Above all, you do not have to pay any ransom as a result of an attack, and you can quickly get back to regular operations.

Conclusion

Ransomware is a product of organized crime, and the attackers do not operate with ethics. They can refrain from providing the key for decryption even after receiving the ransom. The victim not only loses their data but also a substantial amount of money and will face consequences associated with the loss of production data.

According to a Forbes article, only 19% of ransomware victims get their data back after paying the ransom. Therefore, the authors recommend not paying a ransom in the event of an attack because doing so reinforces the attacker's faith in their business model.

Data backup and restore operations play an important part of ransomware recovery. Therefore, they must be included as an integral part of business planning. The implementation of these operations should be budgeted for so that there is no compromise on recovery capabilities in the event of an attack.

The key is to select the correct technology partner in this journey, and FlexPod provides most of the needed

capabilities natively with no additional cost in an all-flash FAS system.

Acknowledgements

The author would like to thank the following people for their support in the creation of this document:

- Jorge Gomez Navarrete, NetApp
- Ganesh Kamath, NetApp

Additional information

To learn more about the information that is described in this document, review the following documents and/or websites:

- NetApp Snapshot software

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

- SnapCenter Backup Management

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

- SnapLock Data Compliance

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

- NetApp Product Documentation

  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

Copyright information

Trademark information