Technical white paper

Protecting data from ransomware with HPE StoreOnce Catalyst

Ransomware cannot affect what it cannot see

Contents

Executive summary

Ransomware has been on the rise. Although it has existed since 1989, criminal organizations started developing and distributing ransomware as an attack vector since 2013. Over the years, these attacks have been perfected to target a very vulnerable set of systems and protocols. Any company that has been impacted by malware should seriously consider the possibility that ransomware is also hidden within their environments.

In 2020, the threat landscape evolved to use COVID-19 for successfully depositing ransomware in networks. Changes in preventive and detective controls to accommodate flexible working practices as well as constraints on IT security teams during lockdowns have contributed to the vulnerability of the workplace.

When it comes to ransomware, the primary weakness in any storage system is within the user authentication process. This white paper covers common authentication methods and how they are compromised. Impacts to the data stored within various types of storage are summarized, including file-sharing technology, along with object and block devices as related to the issue of ransomware. This paper also provides technical detail on how ransomware impacts the traditional storage mechanisms employed by most businesses, as well as how Hewlett Packard Enterprise (HPE) StoreOnce Catalyst can help protect your enterprise data from ransomware and other forms of malware.

Audience

This paper is intended for information assurance and data protection technologists who are executive staff or IT operations staff responsible for the protection of enterprise data. It is assumed that subjects such as networking, storage area networks, data shares, encryption, malware, and backup are understood, as are the protocols they use. For those not already familiar with ransomware and the associated risks, refer to the HPE technical white paper Ransomware: Ensuring Protection from a Growing Threat.

Background

The use of ransomware attacks is more prevalent today simply because it is a relatively low-touch attack method for criminals, and it works. Criminal groups are pivoting to COVID-19-themed lures in order to exploit end users' concerns over the pandemic and the safety of their loved ones. Remote working significantly increases the risk of a successful ransomware attack due to a combination of weaker controls on home IT and a higher likelihood of users clicking on COVID-19-themed ransomware lure emails. Ransomware has real consequences for victims who, if affected, will find themselves requiring data recovery, paying the ransom due to a lack of preparedness (or lack of secure backups), or accepting the loss of their data altogether. Some sources estimate the revenue generated from ransomware attacks in 2020 alone at $20 billion.[1] The cost for victims is obviously much greater than the ransom itself. There are significant costs associated with downtime, loss of productivity, and a potentially permanent loss of customers when they are not served appropriately. Furthermore, making significant changes to the enterprise infrastructure and processes to prevent future compromises can be costly considering the time, resources, and money required.

Traditionally, organizations are leveraging a variety of methods to retain and make redundant copies of data. For example, snapshots and replication of network attached storage (NAS), Network File System (NFS) data shares, and Common Internet File System (CIFS) data shares are used to connect, map, and provide data services, all of which are susceptible to ransomware encryption malware.

Online and nearline file-based storage commonly leverages the cross-platform Server Message Block (SMB) protocol to map network drives and read/write remote files in Windows environments (Samba for Linux®/UNIX®). The longevity and backward compatibility of SMB make it widely adopted for general-purpose file storage; although it functions very well for this purpose, it also carries inherent risk in the case of ransomware and should not be relied upon as a mission-critical data repository. SMB can be utilized as a cost-effective and efficient means

[1] PurpleSec: 2021 Ransomware Statistics, Data, & Trends

of temporarily storing data for small businesses or work groups in an enterprise, but eventually all critical data needs to be stored securely.

The primary weakness in securing SMB is in the authentication process. Commonly NT LAN Manager (NTLM) is used in smaller shops and work groups, and Kerberos is used in larger enterprises where a separate authentication server is deployed for this purpose. SMB authentication is the process of confirming a valid user and system combination (system logon credentials) for which rigorous policies should be in place. Different machines on a network then exchange authentication information using NTLM or Kerberos in a challenge-and-response process as needed.

SMB can be made vulnerable in either authentication scenario using pass-the-hash attacks. Authentication using a hash of the user's system password or a Kerberos ticket during the SMB connect exchange with the server is stored in the memory of every system accessed until powered down (assuming volatile memory) in Single Sign-On (SSO) environments. Attackers can grab this hash by playing man in the middle through packet captures or after compromising either the client or server where the hash resides in memory from a memory dump. After the NTLM hash is captured, it is easily used by an attacker. NTLMv1 should not be used at all per Microsoft because it uses an MD4 hash with 56-bit encryption chunks that almost any computer can easily crack. NTLMv2 is better because it has MD5 encryption that should prevent cracking the hash, but this still does not protect a connection from the man-in-the-middle approach where a hostile server intercepts and forwards the uncracked but still valid credentials during the authentication process. This is why strict data classification and authentication policies are so vital for helping to protect an organization and minimize the number of users with access to critical data.

The same is true for object and block storage devices that do not incorporate immutable data technologies. Applications and block devices that use immutable data storage technologies might prevent ransomware from affecting some portion of your data, but there are too many variations to detail here. The integration of immutable block technologies with other common enterprise systems and software should be completely investigated before relying on them as a preventative measure against ransomware. Block devices with or without immutable technologies are susceptible to the same authentication issues described here for SMB and Samba. The immutable technology might be able to provide access to unaffected original block data even when the majority of revised data is affected; however, how much and how efficiently data can be recovered can present a challenge especially for large enterprises.

After a storage system integrated with Active Directory has been compromised, it is wide open to an attack that is difficult to identify because legitimate processes and credentials are used to take advantage of the compromised systems. Usually the only way to recognize this means of attack is when things start to go wrong. Obviously, this is far too late.

HPE StoreOnce catalyst features and benefits

The HPE StoreOnce purpose-built backup appliance and HPE StoreOnce Catalyst bring a wealth of benefits to an organization in the way of space-efficient backup, deduplication, data lifecycle management, and information assurance. However, the single most important feature of HPE StoreOnce Catalyst is its ability to completely isolate data from being tampered with unintentionally.

Data is isolated and protected

HPE StoreOnce is a purpose-built backup appliance (or virtual machine) that includes HPE StoreOnce Catalyst stores to effectively isolate critical data where attackers cannot have impact on it without resorting to direct physical interactions that ultimately would result in the destruction of some or all of the hardware itself. Even when physical destruction is achieved at a single location, whether from malware or a natural disaster, the more advanced implementation of HPE StoreOnce Catalyst stores (distributed implementation) would effectively protect mission-critical data by effectively isolating it from traditional lines of communication and command sets leveraged by ransomware attackers. HPE has hidden the Catalyst store from attackers in plain sight but behind an

application programming interface (API) that both enhances and simplifies the process of backing up and deduplicating data while making it practically impossible for ransomware to attack it directly.

HPE StoreOnce Catalyst stores do not prevent the rest of the enterprise from being compromised by malware, but they will protect the mission-critical data stored from being either targeted or affected. Ransomware cannot encrypt what it cannot see, and because the Catalyst store does not use standard operating system command instructions for its operations, malware cannot become active while inside. HPE StoreOnce Catalyst efficiently backs up and restores data using a tamperproof method. HPE StoreOnce Catalyst, initially designed for use as a disk-based solution and now extended to the cloud, is capable of leveraging deduplication, compression, encryption, and data isolation for backup and archiving processes. HPE StoreOnce Catalyst prevents ransomware from accessing data on the HPE StoreOnce appliance ensuring data integrity.

Command and data sessions

The Catalyst architecture is accessed through an API command set that is directly integrated into a backup application media agent, which includes the HPE StoreOnce Catalyst client library. This library is effectively an API that uses a proprietary set of commands to send and retrieve data from the Catalyst store using command and data sessions, as shown in Figure 1.

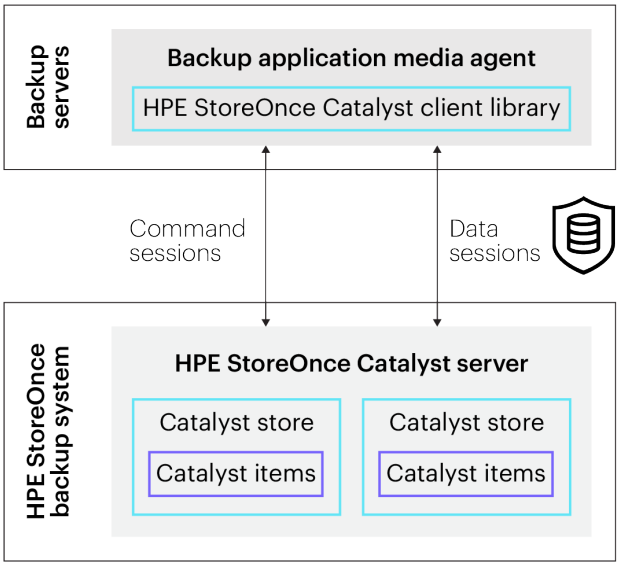

Figure 1. Command and data session communication

These command and data sessions are comparable to the SMB (or Samba) connections in a traditional datastore using NAS and similar technologies. The key difference with the HPE StoreOnce Catalyst store is that it does not rely on the same authentication methodology or most importantly the same set of instructions stemming from the operating system that these other technologies do. HPE StoreOnce Catalyst can be considered a kind of demilitarized zone where malware is concerned.

It is this separation from the operating system instruction set that isolates and protects the HPE StoreOnce Catalyst store and its items from a ransomware attack. The systems that the Catalyst media agent reside upon are still vulnerable to attack without further hardening, and the malware itself could be potentially sent across the network to the Catalyst store; however, the Catalyst store itself is completely protected from being encrypted by the malware due to the separation of it from any usable command sets (targeted operating systems such as Windows and Linux). All communication to and from the HPE StoreOnce Catalyst store is sent through the Catalyst client library (API) and its associated command and data sessions that create the pipes between systems using HPE technology specific to this task.

The command and data sessions run over standard TCP/IP Ethernet or Fibre Channel connections depending on the HPE StoreOnce model. These sessions use remote procedure call (RPC) through the API, which causes

subroutines to run in different memory address spaces on each system associated with the solution. The memory segregation further isolates the process by adding additional protective layers between the data and the malware before it gets to the Catalyst store, taking the layered security methodology all the way to the end point. This is also conducive to cross-platform data movements where instruction sets are likely not the same (for example, Windows to Linux).

Interprocess communication

The item of importance where ransomware is concerned is that all communication between the backup server and the HPE StoreOnce Catalyst store is handled using interprocess communication (IPC), which is a mechanism within the context of RPC used to enable communication between a client and a server regardless of where the parts are physically located (remotely, same system, and so on). This communication is not dependent on the local operating system command set to perform its duties. This secures the data, not the device, and enables data mobility in a way that brings the data closer to the systems where compute happens, increasing efficiency and potentially decreasing costs while eliminating risk. How HPE implements deduplication on HPE StoreOnce appliances is not directly relevant to the security aspect of the Catalyst solution aside from employing encryption algorithms to reduce the data set size, but additional information can be found in other documentation referenced in the Resources section of this white paper.

Backup methodologies

Data isolation effectively protects the data, but efficient data management requires the use of one or more technologies depending on the services and efficiency requirements of an organization. One consideration should be the implementation of solid backup methodologies as indicated by the United States Computer Emergency Readiness Team (US-CERT) in its report Data Backup Options. The 3-2-1-1 rule refers to the practice of creating at least three copies of data (one primary copy and two backups). Two copies are stored on at least two different types of media (for example, disk and tape) with at least one copy stored off-site and one copy offline.

Backup applications

Several software vendors have integrated HPE StoreOnce Catalyst technology into their data protection applications, providing advanced backup, data management, and automation capabilities. Using the 3-2-1-1 backup methodology as recommended by US-CERT is still very applicable as a process control even when HPE StoreOnce Catalyst isolates the data. The 3-2-1-1 method helps to ensure data is protected from a variety of potential problems, including human error and natural disasters. One unique and very useful third-party capability is Veeam Mount Server, which enables the ability to immediately mount backed up virtual machine files for instant VM recovery and unparalleled RTO efficiency when combined with HPE StoreOnce Catalyst. VMs recovered in this fashion are mounted Read-Only by default, further protecting the environment should any malicious software remain within the backup data.

Immunize backup repositories against viruses

The best backup solution is useless if ransomware can access your backup repositories. Figure 2 illustrates how HPE StoreOnce Catalyst provides protection for backup repositories. Backup applications integrated with HPE StoreOnce Catalyst stores primarily enhance the ability to manage the lifecycle of backup data through policies and scheduling.

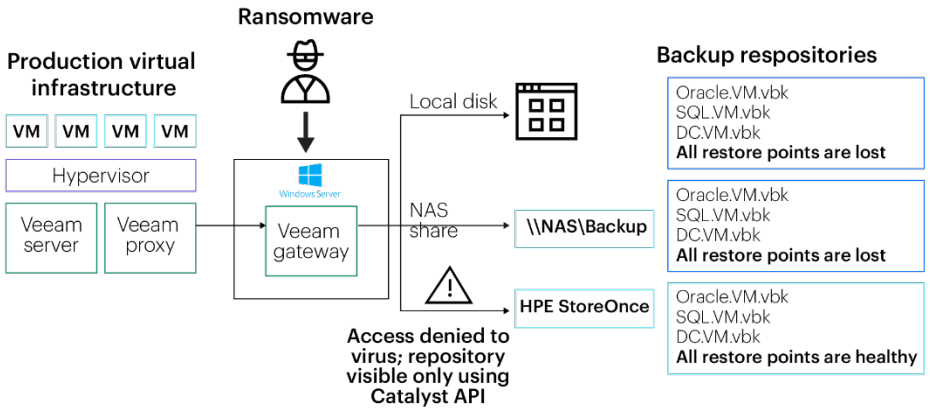

Figure 2. HPE StoreOnce Catalyst protects data because the repository is only visible through the Catalyst API

HPE StoreOnce catalyst array integration with HPE Recovery Manager Central and backup applications

HPE Recovery Manager Central

HPE Recovery Manager Central (RMC) is tailored to many enterprise software applications to enable the ability to create snapshots, replicate volumes, and back up storage while providing stringent recovery point objective (RPO) and recovery time objective (RTO) service-level agreements (SLAs) in conjunction with HPE Primera and HPE Nimble Storage[2] arrays. All-flash enabled applications running on HPE 3PAR StoreServ or HPE Primera arrays can take advantage of crash consistent backups and snapshots to ensure that the right data is available for recovery at the right time. The HPE StoreOnce Catalyst store serves as an ideal final destination for any information on the array that is considered mission-critical enough to protect from ransomware. When used in conjunction with HPE RMC, the HPE StoreOnce Catalyst store is fully integrated for a seamless and efficient data protection experience. Additional information about these products can be found in the Resources section or through speaking with an HPE presales professional.

Backup applications

Many backup software products such as Commvault CommServe and Veeam Backup & Replication are integrated with HPE StoreOnce Catalyst leading to faster backups and recovery. A greater number of backup images can be stored on disk, providing more recovery points and faster restores from backups. HPE StoreOnce variable-length deduplication provides a fine-grained deduplication capability that increases the overall storage efficiency of backups and reduces costs. HPE StoreOnce allows you to deduplicate across the backup jobs, further improving deduplication efficiency. Commvault CommServe and Veeam Backup & Replication software integration includes reliable security and ransomware protection that fends off increasing risks of cyberthreats now and into the future, delivering unprecedented resiliency for companies of any size. HPE StoreOnce Catalyst effectively isolates critical data so attackers cannot access it without resorting to direct physical interactions. Even in instances a single location is physically compromised, HPE StoreOnce Catalyst stores continue to protect mission-critical data by effectively isolating the data from traditional lines of communication and command sets leveraged by ransomware attackers.

[2] HPE Nimble Storage RMC integration is planned.

Ransomware protection in the cloud with HPE cloud volumes backup

A modern data protection plan should extend to the cloud for scalability. The cloud offers flexible capacity and supreme agility without requiring additional capital investment. Cloud services scale up or down to meet unpredictable demands, and because data is managed off-site, your IT staff is freed up from additional data center tasks.

HPE Cloud Volumes Backup delivers a simple, efficient, and flexible way for users to backup data in the cloud. This enterprise backup service enables the customer to backup seamlessly to the cloud—directly from any storage using any backup ISV—without changing existing data protection workflows. Start backing up to the cloud in less than 5 minutes with automated backup policies in just a few clicks and recover with ease. HPE Cloud Volumes Backup is secure by design and safeguards against any threat with encrypted backups that are invisible to ransomware attacks. Using the proven HPE Catalyst API, it makes backup images invisible and inaccessible to ransomware, ensuring data integrity and enabling restores in the event of an attack. You can restore workloads on-premises or easily leverage public cloud for multiple use cases, such as test/dev, reporting, and analytics, helping you to transform your backup data into a business asset.

Conclusion

Data protection has slowly morphed into a never-ending series of disk-based replications and snapshots, which serve to recover specific files quickly. However, the move away from more redundant and secure methods such as tape and off-site archives has left a large security gap for cybercriminals to distribute ransomware. Many organizations can now unfortunately attest that simply backing up data by making copies is not sufficient. If an operating system can see your data, so can ransomware. In traditional backups, knowing what data has been affected and when plays a crucial role in determining which backup repositories can be used to recover post-attack. The 3-2-1-1 rule that data protection specialists have relied on must always be remembered: Preserve three copies of your data on at least two different media types with one stored offline, and one stored off-site at another physical location or in the cloud.

The best method for protecting enterprise data is a combination of well documented and communicated policies, effective implementation of critical security controls (particularly access controls), and HPE StoreOnce Catalyst, which is the critical data protection component in safeguarding data from ransomware in a backup or data archiving solution. HPE StoreOnce Catalyst deployed as the backup target for mission-critical data ensures the ability to recover data from either a specific RTO or a configuration RPO. Most importantly, it shields data from ransomware and other forms of malware that target specific operating systems. HPE StoreOnce Catalyst stores effectively isolate data and protect it from unintended manipulation and, in the case of ransomware specifically, encryption.

Some companies have tried to hide ransomware incidents, only to have the media report the data breaches later for customers, shareholders, and board members to see. You can find the right hardware and software solution by combining the fully integrated, industry-leading disk technology of HPE Primera and HPE Recovery Manager Central with the HPE StoreOnce Catalyst store technology. The procedures and policies of the US-CERT recommended backup methodology of 3-2-1 ensure true enterprise-level information assurance. Remember that ransomware cannot infect what it cannot see. Be sure your data is securely isolated from cybercriminals with HPE StoreOnce Catalyst stores, and shift from data protection to information assurance.

Call to action

Download the 60-day free trial of HPE StoreOnce VSA and try Catalyst stores in your own test and development environment. There are virtual machine versions for VMware ESXi™, Microsoft Hyper-V, and Kernel-based Virtual Machine (KVM).

Resources

HPE Recovery Manager Central

US-CERT Data Backup Options

HPE StoreOnce 3100, 3520, 3540, 5100, and 5500 User Guide

Veeam and HPE StoreOnce Catalyst

Veritas NetBackup and HPE StoreOnce Catalyst

Center for Internet Security Critical Security Controls

NIST Special Publication 1800-11A

Data Integrity—Recovering from Ransomware and Other Destructive Events

SANS Critical Security Controls poster

Managing HPE Nimble Storage snapshots, replication, and backup to HPE StoreOnce with Veeam

Learn more at

HPE.com//us/en/storage/StoreOnce.html

Visit HPE.com

Chat now

a00042003ENW, Rev. 3

HEWLETT PACKARD ENTERPRISE

hpe.com