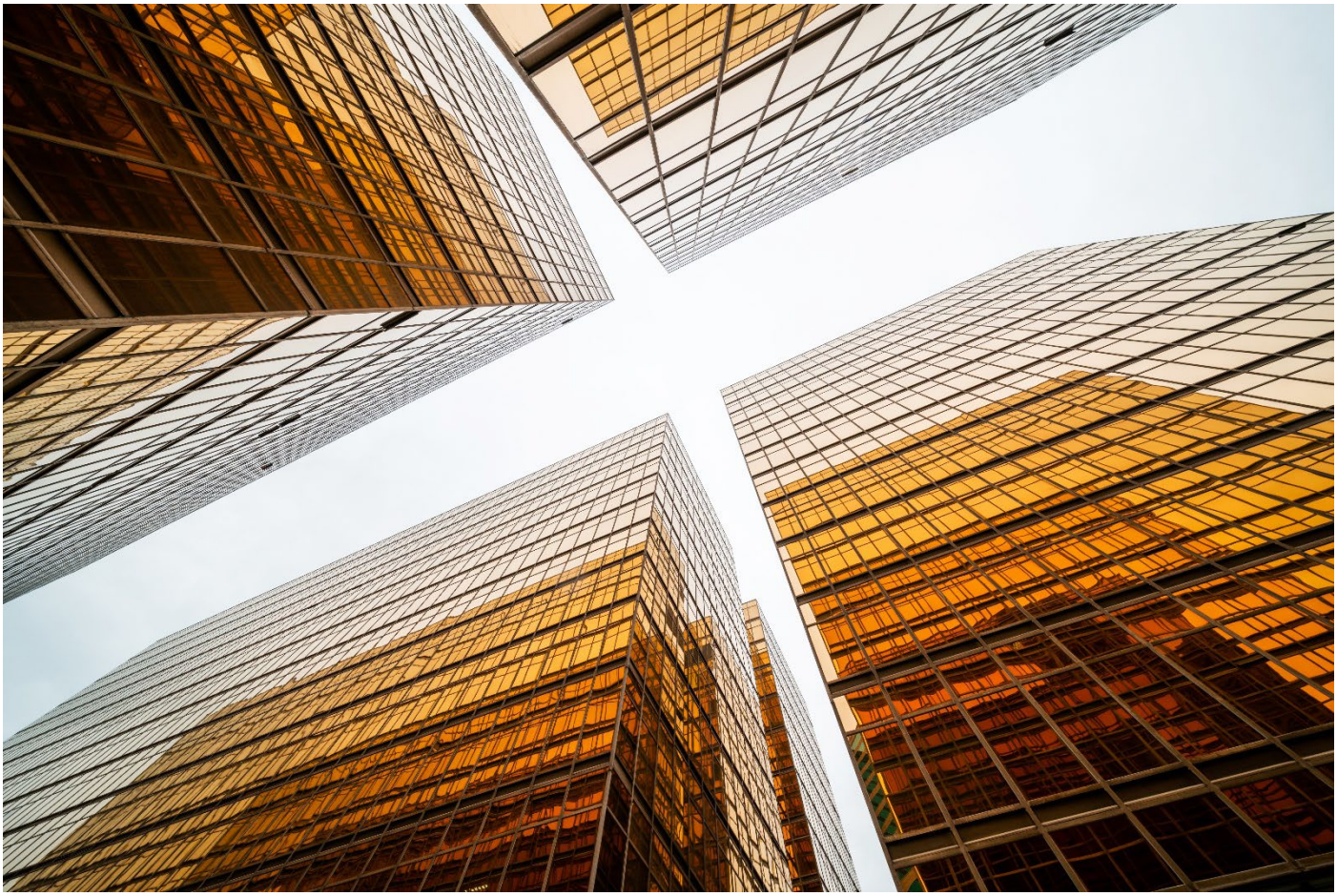
HPE GreenLake

Technical white paper

Ransomware: Ensuring protection from an increasingly complex threat

Building a multi-layered cybersecurity defense with data protection



Contents

Executive summary

Cybercriminals continue to evolve their toolsets and corruption methods in a quest to stay ahead of law enforcement and security experts. Companies ranging from small businesses to major corporations across all industries have suffered losses from sophisticated attacks that have stolen intellectual property and customer data. But one specialized form of cyberattack that is on the rise does not *steal* data—rather, it holds data hostage. This advancing threat is called *ransomware*.

Ransomware is designed to restrict users from accessing data on their own systems while perpetrators demand payment (a ransom) to remove the restriction. This kind of attack is accomplished by encrypting data over time and ultimately blocking user access to it.

When ransomware occurs, it hits with devastating results. Here are the top five ransomware statistics[1] (1 and 5 in particular—the number of days of downtime and the ransomware payout—are sobering):

1. The average downtime a company experiences after a ransomware attack is 22 days. (Statista, 2021)
2. Malicious emails are up 600 percent because of COVID-19. (ABC News, 2021)
3. A recent survey found 37 percent of respondents' organizations were affected by ransomware attacks in the last year. (Sophos, 2021)
4. Ransomware is the No. 1 malware threat. (Datto, 2020)
5. In 2021, the largest ransomware payout was made by an insurance company for $40 million, setting a world record. (Business Insider, 2021)

If a business becomes infected, paying a ransom to unlock data offers no guarantee of obtaining the key—or of unlocking all the data. It certainly does not remove the ransomware. In fact, consider the following example: If 10,000 hosts are infected, then in a perfect world, 10,000 unlabeled keys are returned. That means that it is up to the IT staff to manually match each key (which has no description) to its correct host. To envision the time commitment required for this task, just think of a hospital with a dozen sites or more.

Regardless of the specifics, the task of recovering from ransomware is time consuming. Implementing a solid data protection policy is the best line of defense that businesses can use to protect against and recover from infection.

An older method that has proven successful was the leveraging of data deduplication to provide insight into the health of an organization's ransomware posture. The ratio analysis on the stored backup data is no longer a viable method, however, because of the emergence of a new way of encrypting the data, namely *intermittent encryption*. With this method, the ransomware decryptor has to encrypt only 16 bytes of the file to accomplish its mission of denying the particular file that is being used by the business. Variants emerging since 2021 include LockFile and ALPHV (BlackCat), PLAY, Agenda, and Oyick, to name a few. Intermittent encryption enables the ransomware payload to increase its *dwell time*, the time it uses to reside in the network undetected before it mushrooms across all the infected systems horizontally to produce the ransomware bounty message.

This use of intermittent encryption is a relatively new development that renders ratio analysis on deduplicated data meaningless. The method still has value for variants that do not use intermittent encryption, but a business cannot guarantee which variant of malware[2] might infect it. Suffice it to say that intermittent encryption is currently effective and is likely to be used more frequently in years to come.

Two more relatively new types of ransomware deserve mention here:

- **Exfiltration** is the practice of explicitly leaking only the data that contains personal information online if the victim business does not pay the ransom. This increasingly used method is an insidious development that shows just how innovative cybercriminals have become. The number of exfiltration-only incidents is rising because this practice requires far less effort on the part of the cybercriminal community since they do not have to provide keys to decrypt the business.
- **Blackmail leakage**, the latest development, involves all of the data. Cybercriminal organizations today are undergoing some restructuring. In this context, there is a crypto developer, and there are also a number of their affiliates. The developer develops the payload, and the affiliates use that payload on the potential ransomware targets they acquire. The newest practice, conducted exclusively by the affiliates and to the exclusion of the developer, is to fully corrupt the data. Much like exfiltration, this blackmail leakage means no more concerns about distributing keys for the decryption/ransom. This new model maximizes the affiliates' revenue and effectively cuts out the crypto developer.

[1] 86 Ransomware Statistics, Data, Trends, and Facts

[2] Malware includes not only ransomware, but rootkits, trojans, and botnets, to name a few. For a full list, see The 5 Most Common Types of Malware.

This white paper describes how ransomware works today, examines several trends, and summarizes prevention methods. It also explores ways to protect data by using deduplication ratios if systems become compromised. The dedupe ratio method works only with ransomware variants that use complete encryption and not with the newer intermittent encryption, but it has value if an organization is currently set up for it.

Target audience

The intended audience for this white paper is Hewlett Packard Enterprise sales, HPE systems engineers, HPE partners, and customers who are interested in learning more about prevention of and protection against ransomware.

Background

The first widely known ransomware emerged in 1989. It was called the Aids Trojan (also known as the Aids Info Disk or PC Cyborg Trojan). This ransomware worked by hiding directories and encrypting file names on the local disk drive. It would then prompt the user for payment of a "license renewal" (ransom) to restore the infected host back to its original state. Encryption mechanisms for ransomware were rudimentary at first.

By 1996, however, much stronger public-key encryption was found in some variants. Ransomware continued to mature, leveraging increasingly complex encryption schemes. By 2008, some instances of 1024-bit RSA keys were reported. Today, 2048-bit or 4096-bit keys are not uncommon. (The higher the bit strength, the harder the encryption is to crack.) The latter two cipher strengths have not been cracked to date, so cracking the decrypt key is simply not an option with today's classical computing model.

Employees working from home during the COVID-19 pandemic are a typical target for cybercriminals. According to the McAfee Labs Covid-19 Threats Report, "As remote workers and IT engineers increasingly use Remote Desktop Protocol (RDP) to access internal resources, attackers are finding more weaknesses to exploit, including authentication or security controls and even resorting to buying RDP passwords in the underground markets. Exploiting these weaknesses can give an attacker administrative access and thus an easy path to install ransomware in the network."[3]

Impact of ransomware

As noted earlier, ransomware is used primarily to extort a crypto bounty from victims by infecting computers and their files, rendering them unusable until ransom is paid to have the data restored. The extortion amount often varies. Because the cybercriminal has access to all of your data, sometimes they know the exact amount for which your data protection insurance policy is written, and they demand that amount. It should be stressed that payment does not guarantee the recovery of encrypted files, nor does it guarantee that a reinfection will not occur. A pattern has been observed that after a business is infected, cybercriminals tend to target it again.

A recent *Cybercrime Magazine* report[4] describes ransomware's evolution:

> Ransomware has evolved and expanded dramatically in the interim — and despite authorities' recent success in apprehending several ransomware gangs, this particular breed of malware has proven to be a hydra — cut off one head and several appear in its place.
>
> All signs are that the coming decade will be even worse as ransomware gangs continue to refine and intensify their attacks, vastly outflanking businesses that are juggling the need for ransomware defenses with a broad range of security, data protection, privacy, and corporate risk priorities.
>
> Ransomware will cost its victims more around $265 billion (USD) annually by 2031, Cybersecurity Ventures predicts, with a new attack (on a consumer or business) every 2 seconds as ransomware perpetrators progressively refine their malware payloads and related extortion activities. The dollar figure is based on 30 percent year-over-year growth in damage costs over the next 10 years.

Given how lucrative the ransomware industry is for cybercrime, ransomware attackers have begun to shift focus from consumers to small, medium, and enterprise organizations and municipalities because of the marketability of the data they possess. Although all organizations remain targets, education, hospitals, municipalities, energy, healthcare, and start-ups are now in the crosshairs, given the critical nature of their data. The more critical the data, the bigger the financial ransom.

An older ransomware attack on one U.S. healthcare organization debilitated 10 hospitals in Maryland and Washington and impacted 30,000 staff, 6000 physicians, and countless patients. As noted earlier, some ransomware attacks only lock data from the user, but some variants are more dangerous when criminals intend to leak stolen data to the dark web if a ransom is not paid.

In October 2022, the Los Angeles Unified School District (LAUSD) underwent exfiltration, necessitating the creation of a help desk and follow-up guidance and counseling to deal with each person's exposed personal information. The ability of interested parties to easily find

[3] McAfee® Labs Covid-19 Threats Report. McAfee Labs, July 2020
[4] Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031

your company's intellectual property or your medical conditions and prescription drugs is disturbing because these are all intensely personal and private pieces of information.

How ransomware works

The operational cycle of ransomware has unique aspects when systems are infected. Attackers need a delivery mechanism to get their malicious code (the payload) onto a targeted system, which is similar to traditional malware. Not-so-similar to traditional malware, however, ransomware has *execution* and *demand* phases to hold the compromised system hostage and provide instructions for the ransom payment.

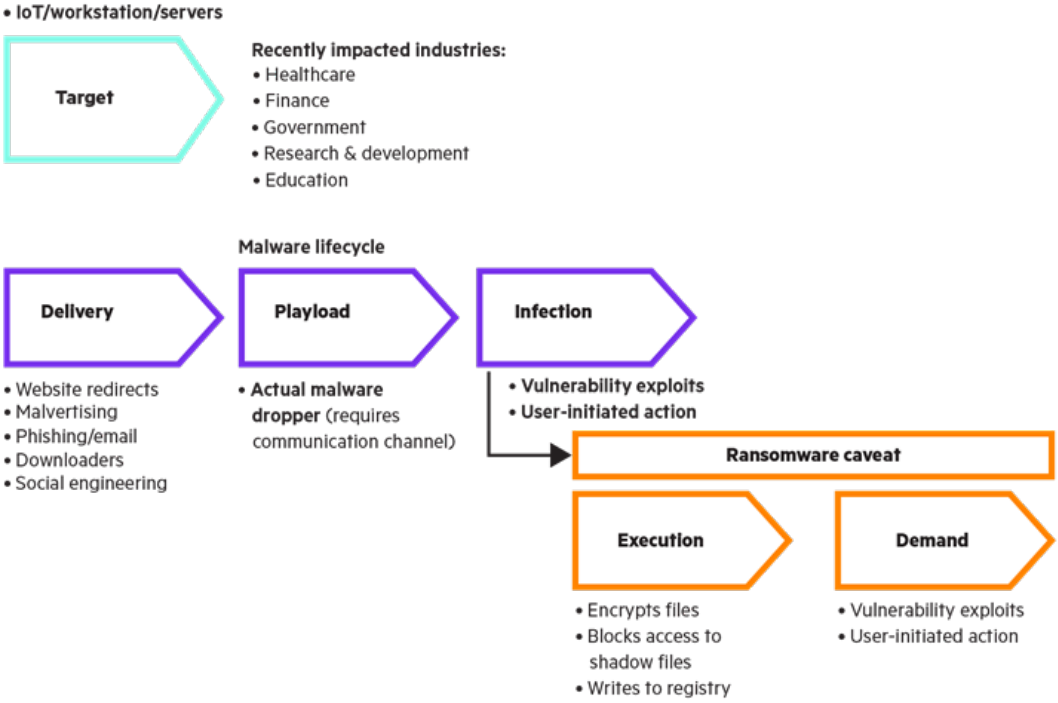


Figure 1. Malware and ransomware operational cycle

Figure 1 shows the operational cycle of malware and ransomware:

- **Target**—In the past, adversaries typically attacked consumers, but a shift toward businesses—from small businesses to enterprise corporations—is now mainstream. Smaller organizations are considered easy targets because they typically have fewer resources available to properly secure and monitor their environments. Medium-sized and enterprise businesses are becoming more desirable targets because their data centers hold large amounts of sensitive, critical, and more lucrative data.
- **Delivery**—Most ransomware is downloaded by users who unwittingly visit a malicious or compromised website through an email attachment or phishing link, or as a payload from another malware program. "Malvertising," or the use of online advertising to spread malware, is another means for delivery, one that is very difficult to prevent. The advertisement that triggers delivery is legitimate, but a malicious link is substituted for it after the ad begins to run. Some instances of ransomware delivery are orchestrated efforts that include exploiting specific vulnerabilities on the target host. After the target is compromised, various hacking techniques are used to establish a foothold and elevate privileges to ensure the eventual infection.
- **Payload**—The payload is either the malicious code itself or a *dropper*—a small file that is easily downloaded without raising suspicion and that automatically downloads subsequent ransomware executables. A dropper can be as simple as an intentionally corrupted Microsoft Word document or some other attachment in a phishing email. Whether ransomware code or a dropper serves as the payload, the end result is the same: Malware holds the host hostage and demands a ransom.
- **Infection**—After the payload is loaded onto the target system, it might start infecting immediately, or it might be activated by a communications path to a remote command-and-control server. This communications channel is used to exchange encryption keys, establish contact with the victim, and provide payment details for the ransom. In most cases, payment and command-and-control communications are handled through The Onion Router (Tor) network, as shown in Figure 2. Tor directs internet traffic through a free, worldwide volunteer network that effectively conceals the attacker's location and activity.

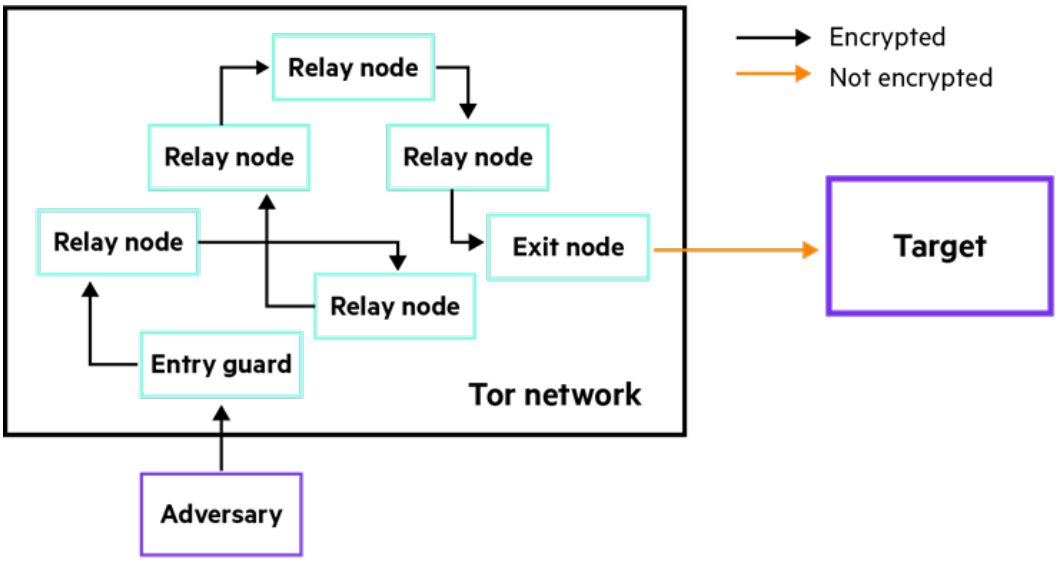


Figure 2. How a Tor network facilitates communications with the ransomware attacker, particularly the cryptocurrency payment

- **Execution**—After systems are infected, the ransomware program begins its execution. Although the execution differs for various ransomware strains, most malware types maintain a predefined, embedded list of file extensions to search for. These extensions might include all files generated by Microsoft Office applications, Adobe documents, .jpg files, .mp4 files, or any other file types. Some advanced variants identify a specific file to infect based on the number of times it was accessed. Ransomware programs search all system drives (including mapped network drives) and include any attached removable-storage media. New variants include Microsoft Exchange Server, Microsoft SQL Server, and even payloads designed to infect air-gapped systems. (The air-gapping form of protection, which was once considered nearly technically impervious, is beyond the scope of this paper. It is mentioned to show the march of delivery innovations in the cybercriminal community.)

  After the ransomware locates specific files to hold hostage, it creates temporary files, encrypts the original files into those temporary files, and then overwrites the original files with encrypted versions.

  To be successful, ransomware must remain undetected for a while. This latency period, called *dwell time*, typically ranges to 50+ days. Along with the encryption and the "ransom letter" aspects of malware, most ransomware uses Windows system files (`svchost.exe` and `explorer.exe`) to reduce the host's defenses. Some types even use `vssadmin.exe` to delete existing Windows shadow volume copies (backup files). More complex variants change registry settings to prevent warnings from non-SSL and non-HTTPS connections to disable Windows repair attempts upon startup. Linux® and Mac operating systems, although more difficult to penetrate because of their security defaults, or even their hardened security features, are now targets of opportunity as well.

  Other tactics include disabling anti-malware programs, using rootkits (malicious software designed to enable unauthorized access), and infecting Windows registries to load malware at boot-up, even in Safe Mode.

- **Demand**—After the encryption process is complete, ransomware generally displays some type of on-screen notice. In all cases, this notice indicates that files have been locked and that a "ransom fee" must be paid by a certain time to decrypt the files. One such CryptoLocker example demands 1 Bitcoin to restore the file system, as shown in Figure 4. Of course, the value of a Bitcoin or Monero, or any cryptocurrency varies day to day, but this type of payment has the benefit of being difficult to trace.

Figure 3. Ransomware notice example

Building a solid defense against ransomware

Although ransomware can be a powerful extortion tool for cybercriminals, building lines of defense to prevent and protect against it increases the likelihood of a successful recovery. Preparedness and leadership buy-in are critical to reducing the impact of ransomware.

Prevention

Conducting effective security awareness training, monitoring networks and systems, applying timely security patching, and employing a robust replication, snapshot, or backup and recovery program are some of the best ways to protect against and recover from a ransomware attack. Techniques to aid in preventing and removing ransomware include the following:

- **Awareness**—Because most ransomware enters a system through some type of social-engineering attack, user awareness is critical for prevention. As with all training and awareness programs, an ongoing effort to stay ahead of changing ransomware tactics is essential. A significant cultural change might be required to educate users on how to prevent exposure and protect themselves and the company. IT departments often provide a tutorial and follow-on quizzes to detect the multitude of methods now "in the wild." They might also sporadically send test messages to see how their user community handles them.
- **Antivirus software protection**—A crucial preventive step is installing antivirus software protection on all systems and keeping it up to date. An entire market has been created to cater to just this niche in the overall market.
- **Patching**—According to the Department of Homeland Security US-CERT, up to 85% of all targeted attacks can be prevented by applying a security patch. Maintaining current patch levels for all operating systems, software, antivirus, and other security programs can greatly reduce the chance of infection. The difficulty is in always responding immediately with patches in a world where all connectivity is maintained 24x7x365. Similarly, patch management has developed into its own industry as a result of malware exploiting unpatched systems.
- **File management**—In a shared environment, exchanging files is routine. Because the distribution of ransomware often depends on the file exchange process, it is imperative to implement a policy that enables documents to be transferred safely and securely. For example, using digital signatures for document exchange might decrease the likelihood of infection. Recent variants of malware have been curated to attack specific NAS systems such as Synology and QNAP.
- **Email security**—Technical controls related to email security go a long way toward reducing the potential for ransomware infection. Effective techniques include employing anti-spam and anti-phishing filters, blocking emails that contain hyperlinks, and quarantining images and attachments. Unfortunately, Exchange Server has been the target of a number of tailored malware variants.
- **Disabled services**—Ransomware and other malware leverage legitimate operating system processes and services in one form or another. Every system is different, so there is no "silver bullet" in relation to which services should be enabled or disabled. The IT department should determine which services are unnecessary before disabling them. Additional permissions can also be levied on risky services that are required for system operation.
- **Software restrictions**—Many ransomware variants copy, alter, and run critical system files (executables) in different locations for a variety of reasons. To stop this practice, policies can be created in the Group Policy Object (GPO) to prevent executables from running in

specific locations (such as ProgramData, AppData, and Temp). Recent variants have attacked logs and system events, so this list is opportunistic, depending on that component's security posture at the moment.

Data protection and deduplication

Prevention is an important approach to reducing the opportunity for a ransomware infection. Even with strong prevention measures, however, most infections are caused by innocent human actions that bypass prevention methods (poor passwords, failure to recognize advanced spoofing techniques, and so on). Therefore, proper data protection is a must-have in any IT environment.

Having a strong defense with a solid protection and recovery plan is key to a quick and effective recovery. Designing a protection strategy requires a robust and well-thought-out plan that incorporates best practices and leverages advanced techniques such as data deduplication.

Include the following precautions to protect your organization against ransomware:

- **Implement a plan**—Being caught off guard by ransomware is not a good position for any company, especially in light of recent exfiltration methods releasing private information. Even if it is possible to secure all of the host keys for decryption in a scenario in which you pay the ransom, it is time consuming to match all keys to their respective hosts and then test for full eradication of the malware afterward. It is better to have a plan that is never needed. If your organization's security policies do not include provisions for dealing with this type of attack, work with your leadership team to develop a protection and recovery plan. Understanding how ransomware works is the first step in determining which security controls are required to prevent and eradicate it. It is also a good idea to understand how Bitcoin and cryptocurrency wallets work. You do not want to start trying to understand cryptocurrency when time is limited. In the last two years, ransomware negotiators have begun offering their services, and they can be critical participants in negotiations.
- **Take steps to protect data**—Removing ransomware after it has done its damage is difficult. In most cases, removing an infection requires a complete system rebuild and recovery from a backup medium that is known to be reliable (data replication, snapshots, tape, disk, and so forth). A recent white paper, Ransomware Data Recovery Architectures, covers how to combine a data replication product from Zerto, an HPE company, to a snapshot-based data protection scheme that uses successive clean rooms to form a robust data protection solution. In this paper, the goal is simply to find—from replication, or snapshots, or tape where applicable—a noninfected copy of that host's data.

The primary technical control is to ensure that data and systems are replicated or backed up on a regular basis, although it is quite possible that the backups might contain ransomware. Recall that it is a horse race between the ransomware's dwell time (on average 54 days as of this writing) versus how quickly your muti-layered cybersecurity defense picks up evidence or becomes forensically aware of that malware. In this race, you are trying to beat the malware mushroom (the ransomware message) that surfaces on most or all systems after a typical 54 days.

- **Know your recovery time objective (RTO) and recovery point objective (RPO)**—Ensure that these measures align with backup and recovery policy service-level agreements (SLAs). Although ransomware does not encrypt all files, a complete restore will likely need to occur on a clean system; depending on the recovery source, this process might take a long time. For a typical 54-day dwell time, this might require going back 54 days to what the system looked like at that time to ensure that the root of the malware has been eradicated.
- **Develop a backup strategy**—Use the 3-2-1-1 data retention topology:
  - **Three** copies of data (the primary data and at least two copies)
  - **Two** different forms of media for its store, which can be replication, snapshot, disk, tape, cloud, or optical

    Isolating one medium from the other ensures that if one medium fails for any reason, there is a second source.
  - **One** off-site copy to the cloud

    Keep this copy away from the from the on-premises site to mitigate damage in the event of geographically local hazards or infections within the network.
  - **One** off-site copy to tape

    A tape removed from the tape library unit cannot be affected by a malware attack.
- **Use a purpose-built backup appliance (PBBA) as part of a 3-2-1-1 backup strategy**—PBBAs, or backup systems, are disk-based storage systems used in conjunction with backup applications for storing generations of backups from multiple sources simultaneously. Deduplication and compression are primary features of these devices with the goal of decreasing the overall backup storage footprint by reducing duplicate data.
- **Use full backups with versioning**—This approach ensures that media that are known to be reliable are available from a point in time before the infection (set at 54 days in this paper). Ransomware can remain hidden for weeks if not months before the demand is made (the dwell time). Having full backups beyond 30 days improves the likelihood of recovery. Some variants feature a very low dwell time of

seven days, but cybercriminals realize that going further back in the past is inherently more difficult, so the average dwell time continues to stay longer rather than shorter. Cybercriminals who elect for seven days dwell time simply see the advantage of getting their ransom money more quickly, but they are not currently in the majority.

- **Know your backup environment**—When backing up servers, be sure to include workstations, PCs, and laptops, because those are the most common end points infected. Tier 1 enterprise resource planning systems (ERP) and customer relationship managers (CRM) are usually mission-critical and are thus targets of opportunity.
- **Check related connections**—Ensure that backups are not connected to the computers and networks they are backing up. The Ransomware Data Recovery Architectures white paper covers this segregation of control and data planes very effectively.
- **Implement write protection/immutability**—Write-protect backups after they are stored offline and off-site. To counter the dramatic rise in malware, the use of immutable media in HPE snapshots, StoreOnce deduplication devices, and the cloud is on the rise. For example, Compliance Mode, or C-Mode, for HPE StoreOnce features dual authorization, requiring two separate users to delete data. C-Mode, or quorum authorization, is a feature you are likely to see more of in the future. The Amazon S3 object lock (most of which are API calls and therefore easy to use after they are set up) and many other types of immutability now exist to maintain geo (GDPR), industry (SEC 17a-3), or privacy (HIPPA) compliance while providing an immutable copy of data from that time period. Zerto data replication also supports these API calls, augmenting your multi-layered cybersecurity strategy.
- **Test (audit) backups regularly**—This step validates the data's integrity and the ability to restore it. Most backup products, and now public or private clouds, have begun addressing the need to provide a sandbox to test the integrity of replicated data, snapshots, and backup and recovery data. Cohesity recently debuted Fort Knox, which provides a cloud-based sandbox for its data integrity, whereas Zerto has had the ability to sequester data on a test network for a number of years now. After the data is in the sandbox, all of the business anti-malware tests can be conducted on that data from that point in time.
- **Combine snapshots and backups**—Snapshots are not backups. Mature ransomware attempts to disable system restore features and delete all Volume Shadow Copy (VSC) files on Windows systems. Snapshots on HPE Alletra, HPE Primera, or HPE SimpliVity arrays are another bulwark of protection against malware. Although malware variants have not been tailored to attack these systems as of this writing, the efficacy of a snapshot depends on whether its data is infected or not. Instead of using snapshots or backups, use both in conjunction: snapshots for quick recoveries and backups for long-term disaster recovery.

Deduplication as a means of detecting ransomware

Data deduplication is a method of shrinking storage needs by reducing redundant data so that over time only one unique instance of the data is retained on disk. Data deduplication works by examining the data stream either on a backup server (source-side) or as it arrives at the storage appliance, checking for blocks of identical data, and removing redundant copies. If duplicate data is found, a pointer is established to the original set of data as opposed to storing the duplicate blocks. The more data is reduced, the better the deduplication ratio. For example, it is not uncommon to see a 100:1 deduplication ratio when backing up hundreds of virtual machines simply because the bulk of the data is similar between all the virtual machines in a backup.

This is where deduplication can assist in recognizing potential ransomware encryption threats that do not use intermittent encryption. As data is backed up, deduplication provides an overall savings ratio. Any drastic drop to the overall ratio within a specific datastore might indicate a data breach or a security issue in which data is being modified. Encryption is designed to scramble file contents, transforming data into a unique and unreadable format. When a large amount of unique data is backed up and stored on a deduplication device, the overall ratio decreases. However, the use of intermittent encryption, which increases dwell time (to learn the system and find out where, for example, the ERP and CRM systems are or where the Exchange Server is located), is likely to render this method increasingly ineffective in the future. If you have such a method in place now, there is no reason not to maintain it for the near-term, but the malware industry is trending in such a way that this method will eventually become incomplete and misleading.

Data protection design considerations to defend against ransomware

It is a best practice to design a data protection environment using backup software that is tightly integrated and optimized with backup appliances. An all-inclusive protection solution provides enhanced backup and recovery performance, simplified management controls for data movement, retention across multiple media and locations, and resilient and secure network connections when transmitting backup data.

The following sections describe a few important software and hardware features to look for when properly architecting a ransomware data protection environment.

Backup application software

Consider backup applications that meet all needs of the data protection policy. Large-scale applications such as Veeam and Commvault can protect most systems and storage arrays within a data center.

For virtualized environments, Veeam Backup & Replication is a leading solution. Backup applications are rarely stand-alone products because most integrate directly with hardware for a unified end-to-end solution.

Backup application considerations include the following:

- PBBAs should be directly integrated by using backup software common interface plug-in modules leveraging HPE StoreOnce Catalyst to enable features such as optimized deduplication, intelligent data lifecycle catalog management, site-to-site replication, cloud archiving, and detailed reporting. Deploying a 3-2-1-1 data retention topology as a single backup policy enables users to effectively manage numerous revisions, efficiently move copies between on-site and off-site backup systems, and archive mature backups to tape or cloud. It also enables them to choose to apply immutability or not at each stop.
- Use source-side deduplication for backup and recovery because it provides a more optimized connection than NAS (Common Internet File System [CIFS] and NFS) or virtual tape library (VTL). Source-side deduplication provides the following benefits:
  - **Improved backup performance over networks.** Backup performance is improved because deduplication is applied at the source before the data is transferred to the backup appliance. This is important if backups are transmitted over slow links.
  - **The use of secure channels between a backup server (or client) and the target backup appliance.** Backup software vendors who provide source-side deduplication use exclusive application programming interfaces (APIs) that are generally not publicly available. This prevents ransomware authors from developing code to infect or lock down a backup appliance, thus making it technically more impervious to a ransomware infection.
- Create an on-demand sandbox to validate or test data if there is suspicion of data infection.
- Backup server recovery or server redundancy should be part of the data protection policy. Most likely, if an infection occurs within the data center, it will also infect the backup server. If the backup server is under ransom demand, a recovery cannot be performed without the creation of a new backup server installation, which is time consuming. In particular, the creation of a new VMware vSphere vCenter® is a critical task in recovering VMware virtualized environments (and preferably that vCenter is a restore—to preserve hundreds of settings on what could be thousands of VMs). Therefore, you should consider having a recovery plan or a redundant backup server on a separate network. A business impact assessment (BIA), whether formal (a business continuance consultancy product) or informal (a list of all the critical servers that comprise whatever makes the business run (infrastructure, IDP, Active Directory-equivalent, ERP, CRM, servers that control robots that build cars, and so forth) ensures that after the malware announces itself you have a printed list of mission-critical servers and their dependencies (that is, which ones should be recovered first).

Data replication, snapshots, backup and recovery, tape and archive

As a business evolves (for example, from medium-sized to enterprise and then global in scale), most of these systems will be a part of a larger scale-out grid architecture in which data is replicated between each node, providing a resilient, multisite data protection strategy as fed to backup and recovery systems to meet the 3-2-1-1 data retention topology described earlier.

Backup vendors offer competitive features for all of their products, and many products in this space are also strategically trying to form a fuller solution. Some vendors now offer data replication, and data replication vendors have embraced long-term retention along with various formats, premises, and types of media that support immutability. Describing the full scope of products that form a more complete strategy is beyond the scope of this paper, but the following points are part of a typical topology:

- Data replication should be commensurate with the SLAs for the application required in terms of RTO and RPO. A Wall Street-based financial application that might lose millions from a few seconds of data disruption is likely to have a sophisticated synchronous data connection at the storage level. On the other hand, Zerto software can protect as many virtual machines as required, enabling them to go back in time in 5-second increments for up to 30 days of full and continuous data protection. In addition, data replication components can be hardened to reduce the effectiveness of malware.
- Snapshots, although they are not backups, can be tiered in a clean room topology, enabling you to potentially go back through each in a layer of "clean rooms" to get at least one non-infected copy of data that does not have the ransomware's payload on board and ready to keep dwelling.
- Backup and recovery systems also play a critical part in the multi-layered cybersecurity recovery plan. Whereas data replication might be real-time as in the Wall Street example (synchronous communications), there is a place for other replication technologies that enable non-synchronous recoveries of replicated data—for example, every 5 seconds for a time span backward up to 30 days. Backup and recovery systems fulfill the next time span, getting a full backup of the data on an increasing choice of media (spinning disk, immutable, immutable to the cloud, and so forth) perhaps once or twice a day.

  Although it is slower than 5 seconds, backup has an essential place in the hierarchy because a full backup can go off-site to immutable media and then through tiering be automatically eligible for archiving. Backup also enables hardening, meaning that a system's configurations (ports, services, and processes) are locked down in accordance with the security specifications, making it very difficult for

an attacker to gain access and thus making that system highly resistant to malware infection. Some malware variants have been created to attack backup catalogs explicitly. Regarding PBBAs, these fit in backup because they use secure, private network emulation protocols when connecting to a supported backup server. Ransomware can infect mount points such as NAS or block (SAN), but unless otherwise engineered for that NAS (and yes, variants exist here) or SAN, it does not detect private channels because the connection point remains invisible outside the backup application.

- In the absence of a deduplication appliance, as discussed earlier, tape would be considered a court of last resort. The present cost of tape, as well as its price/performance ratios and resilience to malware make it a very appealing part of a multi-layered data protection plan. Any tape not in the tape library unit (TLU) is offline and not susceptible to what could be spreading malware. A tape cut 55 days ago and offline is called "a good copy." This tape, or span of tapes, might come down to being your only good, non-infected copy.
- Archiving can be described as the original piece of data—no copies apply in this case. The difference between archive and backup is that backup is engineered to back up copies of your data, whereas the archive contains the one-and-only original piece of data. An archive-locking feature should be implemented on archived data sets to prevent archive data from being overwritten. In the full lifecycle of data, the archive contains all of the original data. Although malware has not targeted archiving and its infrastructure explicitly, the archive system might be adversely impacted merely as collateral damage or simply by way of, for example, a Windows executable used in that archiving environment.
- If possible, all components should also be Federal Information Processing Standards (FIPS) certified.
- Look for appliances that can be managed by the backup application to easily move data to other media during its lifecycle. Source-side deduplication, replication, offload to tape (using the backup application as the control point), and cloud archiving can all be used to meet the 3-2-1-1 data retention policy.
- Reference backup vendor hardware compatibility lists (HCLs) and application support matrices to validate that hardware and software cleanly integrate into existing IT environments.

Conclusion

Ransomware is one of the most lucrative crimes devised by hackers in recent years. It is a type of malware that infects computer systems, restricting users from accessing the infected systems and data until a ransom is paid to the hackers in cryptocurrency. As this paper has explained, given the key strength that hackers are now using, there is no cracking the encryption.

In the absence of cracking the decryptor key, even a perfect scenario of a paid ransom is still time consuming. And sometimes not all the keys are included as well. This leaves only the establishing (and maintaining in each subsequent budget year) of a multi-layered data protection policy that embraces workload/endpoint detection and aggressive patch management as daily best practices. These best practices must then work in concert with a full spectrum of data protection gear, potentially leveraging replication, snapshots, and backup and recovery to best insulate your business from the ravages of malware—and in particular, ransomware.

The objective of detecting ransomware lurking on production or stored backup data is to protect the health of an organization's data, but without a defensive data protection strategy that uses most or all of the assets and best practices noted earlier, the effort cannot succeed. As evidence that the present state of the art is insufficient, note that even the Department of Homeland Security and Lockheed have been adversely impacted. This resolves to a "when, not if" condition. The trends towards exfiltration and blackmail of data with the newest trend of full data corruption make the present challenging both in the workplace and at home. So far, reputational risk has mostly been confined to businesses and workplaces, a soft cost that they have absorbed. Going forward, however, businesses must get used to the blackmail of exfiltrated data. The fact is that blackmail is likely to be a lucrative market, and thus one that cybercriminals will increasingly pursue in the name of increasing profits.

Resources

Ransomware Data Recovery Architectures

HPE StoreOnce Data Protection Backup Appliances

HPE StoreOnce + Veeam

Learn more at

HPE StoreOnce Data Protection Backup Appliances

a00041582ENW, Rev. 2

Hewlett Packard Enterprise