IDC TECHNOLOGY SPOTLIGHT

Sponsored by: LTO Program

Ransomware is a top concern for senior business leaders because of the severe consequences of a successful attack. Magnetic tape is a multi-tool technology that supports the five key best practices for protecting and recovering data from a ransomware attack.

Proactive Defense Strategies Provide the Best Chance to Defeat Ransomware

January 2022

Written by: Phil Goodwin, Research Vice President

Executive Summary

IDC surveys of worldwide enterprises have shown ransomware to be a top concern of both business leaders and technical leaders. Highlights from this research include the following:

- More than 90% of organizations surveyed indicated that they have been attacked by malware, and 87% of those organizations have been attacked successfully.
- One-third of organizations worldwide have experienced a ransomware attack or breach that blocked access to systems or data in the past 12 months.
- It is not uncommon for organizations to be attacked more than once by ransomware.
- Only 13% of organizations that reported a ransomware attack indicated they had not paid a ransom.

AT A GLANCE

WHAT'S IMPORTANT

The consequences of data-related ransomware include lost revenue, lost customers, financial losses, corporate embarrassment, and even shareholder and class-action lawsuits.

KEY TAKEAWAYS

Organizations should adopt five best practices and enabling technologies to give themselves the best chance of defending against ransomware and ensuring timely data recovery without paying the ransom.

Moreover, FBI data shows that ransomware attacks have more than doubled since the beginning of 2020, in part driven by the increase of work-from-home (WFH) workers who have opened new attack points for ransom perpetrators.

The consequences of a successful ransomware attack on data are severe. Some of the consequences have immediate impact on organizations, such as lost employee productivity, disrupted operations, "all hands on deck" disaster response, and ransom payments that can reach into the millions of dollars. Ransomware has long-term consequences as well, including lost revenue, permanent loss of customers, unrecoverable data, regulatory fines for data breaches, permanent loss of organizational reputation, and shareholder lawsuits for negligence. Ransomware attacks can also be embarrassing for an organization's leadership.

Organizational leaders must also be prepared to respond to evolving government directives. For example, a recent U.S. Executive Order directed U.S. federal agencies to harden their cybersecurity systems and included the creation of a Cyber Safety Review Board. While not affecting private enterprise directly, it is an indication that all organizations need to take their ransomware response more seriously and to consider deploying an internal group to assess corporate malware/ransomware readiness and response. Such a group should be chartered not only to prepare the organization but also to demonstrate a proactive approach to combat possible allegations of negligence from lawsuits.

As our previously mentioned research illustrates, it's a virtual certainty that organizations will be attacked — the issue is whether organizations are prepared to respond in such a way that minimizes impact and reduces the likelihood of paying a ransom. To give themselves the best chance against ransomware attacks on data, organizations need to adopt five key best practices:

- **Encryption.** Data should be encrypted at rest on primary storage and in flight when being sent over a network and when stored in a backup data set. Encryption is the best defense against data theft and exfiltration, whether from external or internal threats, because cybercriminals cannot utilize the data. Of course, organizations must pay careful attention to key management systems so that infiltrators cannot easily access the encryption keys.
- **Immutability.** Immutable copies prevent anyone from changing or deleting a data copy. Organizations should have backup copies in immutable formats to ensure data integrity when data needs to be recovered. These immutable copies can further be protected using encryption. IT teams should ensure that immutability cannot be circumvented using simple methods such as system clock resets or policy changes.
- **Air gap.** Air gap is a means of taking a data copy, usually a backup copy, offline so that it is physically disconnected from any network and therefore inaccessible to cybercriminals. An air gapped copy should be immutable and encrypted to stymie internal threats who may have physical access to the air gapped copy. It is important to note that to have a data copy in the cloud is not necessarily an air gap. Systems accessible over a network must ensure that the control path and the data path are separated by different access method and credentials.
- **3-2-1-1 backup strategy.** 3-2-1-1 is an update to the old 3-2-1 strategy. This means three copies of the data on two different types of media, with one copy on onsite and offline and one copy offsite and offline.
- **Backup scanning.** Malware may lie dormant in systems for many months prior to payload detonation. Therefore, it may not be detected and may be backed up with the rest of the data. Thus, scanning backup data sets for malware before data is restored is critical to avoiding reinfection.

Fortunately, solutions exist that will help organizations implement these best practices without adding complexity to the IT environment.

Benefits

Ransomware and malware are an ongoing arms race with cybercriminals. Attacking organizations is a full-time occupation in which the criminals' full effort is spent finding new ways to succeed. As IT organizations erect defenses against certain attacks, the criminals find ever more creative ways to circumvent them. In fact, IT organizations are inherently on defense, but they must take proactive measures to thwart attacks and to ensure recovery is a priority.

No technology or strategy can guarantee that a ransomware attack can be avoided. Thus, while intrusion detection and prevention tools are important, they simply are not enough. Unfortunately, cybercriminals have learned to attack backup data sets first, through either deletion or encryption. When backups are compromised, criminals significantly increase the chances of forcing the victim to pay the ransom.

The good news (if it can be called that) is that ransomers operate much like a business. That is, they seek to maximize profit with the least possible effort. Thus, they look for soft, profitable targets. Organizations that make themselves difficult targets have the best chance of forcing the cybercriminals to just move on.

Proactive defense strategies not only avoid the likelihood of a successful attack but also help avoid shareholder or other lawsuits based on allegations of negligence. Even if an attack is successful, organizations prepared to respond will suffer the least downtime or other potential consequences. These defenses factor in not only external threats but also internal threats from disgruntled or dishonest employees.

The best defense against data attacks is the assurance of recoverability through data survival. Though this is not a deterrence against attack, because the criminals are unaware of the data survival capabilities, data survival does allow organizations to immediately go into recovery mode without paying the ransom.

Key Trends

New ransomware attacks are constantly emerging, with device command and control being among the most recent methods. However, because data is essential to organizational survival, it is still the most common target for criminals. As noted previously, ransomers have learned to attack the backup first because removing the possibility of data restoration increases the chances that organizations will be forced to pay the ransom to get their data back.

Criminals use four main attack methods to compromise organizational data:

- **Encryption.** The hacker encrypts data files and then demands a ransom to provide the encryption key.
- **Corruption.** The hacker programmatically scrambles data and demands the organization pay a ransom to get the descrambling program.
- **Deletion.** Data deletion is most used against backup data sets; deletion is used to prevent organizations from restoring data without paying a ransom.
- **Theft (exfiltration).** Criminals (both internal and external attackers) steal data and then threaten to disclose sensitive information or sell it on the dark web unless a ransom is paid.

Of course, attackers may also use more than one attack method at the same time. Thus, organizations need a complete solution that addresses each possibility holistically.

To complicate data security further, work from home — or work from anywhere — has opened new attack opportunities for malware. In these attacks, hackers use the home systems of employees as the soft spot to attack because many users are not savvy about defensive technologies for home networks, firewalls, and intrusion detection.

These attacks do not target individual users (they're usually not very profitable); rather, they focus on stealing user credentials to access a corporate network. Most such attacks start with phishing scams to personal email accounts outside the purview of IT groups, which may flag the scam. To avoid these scams, organizations must focus on employee training, first teaching users to identify potential phishing scams and then having users diligently deploy firewalls, VPNs, and antimalware software on home systems.

LTO tape is an existing, proven technology that can enable the previously mentioned five best practices and help organizations address these threats.

Considering LTO Tape

LTO tape, also known as Ultrium, has become the de facto industry standard format for magnetic tape. The LTO Program is a group of tape drive manufacturers, tape library manufacturers, and tape media manufacturers that have combined efforts to ensure the progress of LTO tape technology. The LTO standard is now on its ninth generation, with specifications established through Generation 12. The LTO Program has a solid reputation for delivering announced technology on time.

LTO tape is now recognized as a multi-tool technology that can be an indispensable in the fight against ransomware, delivering reliability. The LTO Program can help companies establish best practices against ransomware attacks as noted previously with the following features and methods:

- **Encryption.** LTO tape drives have government-grade encryption built in. Because this encryption is at the hardware level, it can be implemented without performance penalty. Encrypted tapes will be useless to anyone without the encryption key.
- **Immutability.** LTO tape media contains a tab on the cartridge to make any tape into a write once, read many (WORM) immutable copy. Data may be read, but it cannot be changed or deleted by anyone who does not have physical access to the media.
- **Air gap.** The removal of tapes from a library eliminates the physical connectivity needed to access, modify, or delete the data on the cartridges. Physical access is needed to put the media into a device. Tape is arguably the easiest, lowest-cost. and most fail-safe means of establishing an air gap. Without physical access, criminals can't compromise the backup.
- **3-2-1-1.** Tape can serve as the second media type, the onsite/offline copy as well as the offsite/offline copy of data (the 2-1-1 part of the strategy). When combined with encryption and immutability, these copies are arguably the most certain chance an organization has to ensure data survival in the event of a malware attack.
- **Backup scanning.** Because there is no assurance that malware has not been backed up to tape (or any other backup system), LTO technology allows tapes to be scanned upon restore to detect and delete malware.

In addition to being a key tool to defeat ransomware, LTO tape has several other unique attributes that add value to the organization:

- **Long-term data retention.** LTO media is certified for up to 30 years for data retention integrity. Organizations that need to retain data for several years or several decades can use LTO as a reliable, long-term media with minimal administrative overhead.
- **Low total cost of ownership (TCO).** The cost to store data on tape media is extremely low because no power or cooling is required (although temperature extremes on stored tapes must be avoided). Magnetic tape is objectively the lowest-cost way to store data for long periods of time.
- **Rapid data restore.** Generation 9 LTO has a restore rate of up to 1,000MBps (assuming 2.5:1 data compression) per drive, more than 8x the throughput rate of a 1Gbps Ethernet link. Organizations can scale tape to match the ingest rate of target systems, making large-scale data operations practical where recall from the cloud simply is not practical.

When using tape, organizations typically implement the following backup strategy: Daily backups are retained for seven days, weekly backups are retained for a month, and monthly backups are retained for a year. This strategy

almost certainly ensures that data is available for restore at a point prior to the attack. Other technologies such as snapshot and clones — though useful and necessary — are often deleted on a much shorter-term basis to save disk space. This is especially important in cases where the attack takes place over an extended period of time and therefore the disk-based copies may not be available at the necessary point in time.

Challenges

Ransomware and malware are constantly evolving and will emerge in ways that no one can predict. Thus, no company or organization can be sure that today's solutions will meet tomorrow's threats. Specifically, tape does not address all types of ransomware (nor do other storage technologies) such as device command and control, which has been the method of attack in several recent high-profile ransomware attacks.

LTO tape is arguably the lowest-cost, simplest method of achieving ransomware recovery best practices.

Tape is primarily a responsive technology that helps restore lost data but must be combined with other technology such as intrusion detection and prevention. It can also help prevent data exfiltration from backup copies, but it does nothing to address attacks on primary storage, regardless of attack method. Moreover, organizations should not rely on tape alone for their ransomware protection. They must combine tape with other technologies, such as snapshots, mirrors, replication, and other data protection methods to address the range of data loss causes.

Conclusion

Ransomware and malware are threats that will not go away. Cybercrime is simply too profitable for criminals to abandon. Although no one is invulnerable to attack, organizations that take all reasonable steps to prevent attacks and establish assured recovery from ransomware are the most likely to avoid it in the first place or recover most quickly if attacked. Magnetic tape is an established, understood, and proven technology that can be an invaluable tool for defeating ransomware. LTO tape is unique in its ability to meet all five best practices for addressing ransomware and giving organizations the best chance of recovery and avoiding the consequences of an attack.

About the Analyst

Phil Goodwin, *Research Vice President*

Phil Goodwin is a Research Director within IDC's Enterprise Infrastructure Practice, covering research on data management. Mr. Goodwin provides detailed insight and analysis on evolving industry trends, vendor performance, and the impact of new technology adoption. He is responsible for producing and delivering timely, in-depth market research with a specific focus on cloud-based and on-premises data protection, business continuity and disaster recovery, and data availability. Mr. Goodwin takes a holistic view of these markets and covers risk analysis, service-level requirements, and cost/benefit calculations in his research.

MESSAGE FROM THE SPONSOR

About LTO Program

Linear Tape Open (LTO), also known as the LTO Ultrium format is a powerful, scalable, adaptable open tape format developed and continuously enhanced by technology providers Hewlett Packard Enterprise (HPE), IBM Corporation and Quantum Corporation (and their predecessors) to help address the growing demands of data protection in the midrange to enterprise-class server environments. This ultra-high-capacity generation of tape storage products is designed to deliver outstanding performance, capacity and reliability, combining the advantages of linear multichannel, bi-directional formats with enhancements in servo technology, data compression, track layout, and error correction.

Building on more than two decades of data protection and storage innovation, LTO-9, the latest generation of LTO tape technology, offers end users more energy-efficient storage capacity than previous generations. It delivers a powerful, scalable and adaptable open-tape storage format that can provide industries around the globe secured and protected data against storage cyber threats.

Since the first LTO products were brought to market, over 5.6 million drives, 351,732,245 cartridges and 370,870 Billion GB of media capacity have been shipped, making LTO Ultrium the most successful tape format in history.

For additional information on the LTO Program, visit www.lto.org

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com