Quantum

CASE STUDY

Fighting Ransomware with Multi-Tier Backup Strategy

Ransomware is one of the fastest-growing kinds of cybercrimes, affecting IT organizations around the world at a rapidly expanding pace—there were 56,000 attempted attacks in March 2016 alone, according to data reported by Symantec. More and more criminal organizations seem to be climbing on the ransomware bandwagon, sometimes combining it with denial-of-service (DoS) or other kinds of attacks, and the financial impact is enormous. The FBI estimates that official ransomware payments in 2016 reached $1 billion, and the total loss is even higher since many payouts are never reported.

FEATURED PRODUCTS

Scalar LTO Tape Libraries, Lattus Object Storage

Lattus provides a highly scalable archive repository using object storage technology to provide very high-capacity storage while protecting data by spreading it across many different disk spindles and, optionally, multiple locations.

Ransomware-style cyberattacks may be common and difficult to completely stop, but a best practice backup strategy that includes multiple copies of data on different kinds of media, including tape, can eliminate or minimize data loss.

SOLUTION OVERVIEW

- DXi® disk backup and replication appliances
- Scalar® LTO tape libraries
- StorNext® Pro Foundation archive system
- Lattus™ Object Storage private cloud

BEST PRACTICES

- Make sure all administrators, including those managing backups, can recognize a ransomware cyberattack and know how to shut down systems immediately when an attack is discovered.
- Do not stay logged in as an administrator any longer than strictly needed.
- Avoid browsing, opening documents, or other like activities while having administrator rights.
- Create a multi-tiered backup strategy that includes a tape layer to ensure that data can be rebuilt safely in the event of an attack.
- Backup best practice includes having three copies of data on two different media types, with one stored safely offline and off-site.
- Consider implementing a multiple-tier archive strategy, using tape or object storage, to provide a safe place to store copies of primary data and rebuild systems.
- Enforce policies that place all critical data on resources that are protected by the institution's disk and tape backup protocols.

Although the specifics differ, the majority of ransomware attacks use the same basic methodology: cybercriminals introduce malware into a computer system, which systematically encrypts stored files, and then demand payment in exchange for the decryption key. Ransom payments are not recommended by security experts because they encourage further attacks and the record for being able to retrieve data is not good. Many organizations have reported not being able to recover all their data even after paying the criminals. Nevertheless, organizations facing loss of data are often tempted to give in. A much better solution is creating a resilient data protection system that minimizes losses.

RANSOMWARE ATTACKS A MAJOR UNIVERSITY

An example of how IT organizations can minimize the effects of ransomware and save their institutions money is illustrated by the experience of a major U.S. West Coast university recently attacked by cybercriminals. The attack was carefully planned to target the specific institution. Trojan-horse malware was introduced into the computer networks by people in the university clicking on links in fraudulent emails and other bespoke tactics. The malware was installed a week before the full attack was carried out, and the intruders reached the backup administrator level. The uploaded malware software attacked files in NTFS, the default format that the Windows family of systems uses to store and retrieve files on hard drives. It was designed to spread between devices—ultimately infecting physical and virtual servers, laptops, and devices like thumb drives.

Although the university had up-to-date intrusion detection software installed, this was not an attack to steal data. As security experts remind us, there is no way for IT teams to permanently win the fight against malware—Trend Micro reports finding 50 new ransomware families in the first five months of 2016 alone. The university attack was timed to begin on Saturday night, starting with the backup servers to disrupt the system people rely on for protection, before spreading to other devices. Once on the live disk, the malware worked through files, encrypting them so they could no longer be read.

RAPID DISCOVERY A KEY TO MINIMIZING DAMAGE

The attack might have been discovered earlier, but there was a new backup administrator who was not fully aware of how to monitor backups to detect malware and shut down the system at the first signs of an infection. As a result, the malware encrypted files for a full eight hours before an administrator noticed that a server's data was unreadable and tracked down the head of IT, who diagnosed the problem and shut down all the systems. By that time, a full 20,000 files had been locked on 120 Windows servers, including all of the university's virtual machines (VMs).

The ransom demanded by the criminals was a huge amount—in six figures. But the university decided against making the payment because the IT team had a data protection methodology that would allow it to recover the data safely.

TAPE BACKUP LAYER CRITICAL COMPONENT FOR RECOVERY

The university had a well-defined backup and restore protocol that started with Quantum DXi disk backup systems as its first line of defense. However, since the files were stored in NTFS format and the backup servers themselves were the attackers' first target, the backup copies written to the disk target were compromised. Fortunately, the IT team also had multiple layers in the backup system—regularly replicating files to a second DXi deduplication appliance and writing backups to an LTO tape library, and then storing a copy of the data on tape in a secure, off-site location. Had the attack been discovered early enough, the replicated backup files could have been protected by shutting down the systems during the time gap between backup and replication. However, because of the delays in this case, the replicated copies were also compromised.

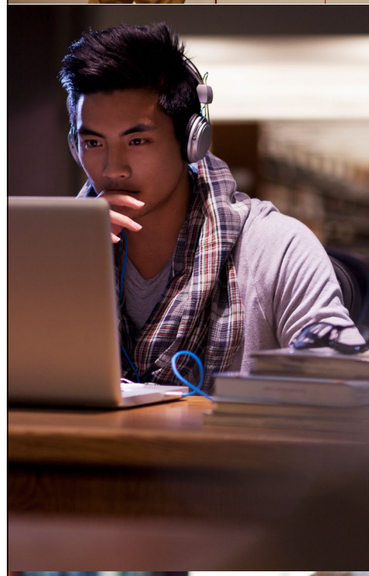
Although the backup copies on the disk target were encrypted by the malware, the tape layer was unaffected because the files were written to tape before the attack began. And even if contaminated copies of files had been written to tape, the malware would not have been able to spread to any other files.

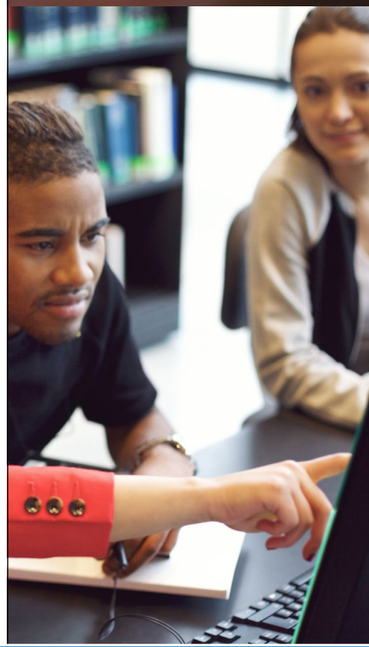
The IT team decided to reinstall the system from scratch because the servers had been compromised and a complete forensic discovery-and-recovery process would have been too time-consuming. The team scrubbed the original system and rebuilt everything, beginning with the most critical data to minimize delays—working files, servers, VMs, and backup systems—from the tape backup copies. The entire process took two weeks to complete.

ARCHIVE STRATEGY CAN PLAY A ROLE

The university might have been able to rebuild the systems directly onto the existing disks and servers, but it had another weapon—a Quantum StorNext archiving system that created duplicate copies of some of its primary data in an object-storage-based private cloud using Quantum's Lattus solution. The team discovered that the malware, which was designed to attack NTFS files, left several systems based on other protocols untouched—including Citrix XenApp and the StorNext archive layer stored in Lattus.

Lattus provides a highly scalable archive repository using object storage technology to provide very high-capacity storage while protecting data by spreading it across many





different disk spindles and, optionally, multiple locations. The team used the StorNext Lattus environment as a safe staging area to restore the systems before installing them on the now-clean original server infrastructure.

RECOVERY PLANS MINIMIZE LOSS

The copies on tape, along with duplicate copies on Lattus, provided the IT team with everything it needed to recover all the data that had been backed up using the multi-tier protocol and to rebuild the primary storage system. Full recovery, including systems tuning, took over a month. But the only data that had to be recreated was data stored outside that system, primarily data on laptops or thumb drives that were not part of the backup system. The loss amounted to about 600GB, a manageable level.

The bottom line? Ransomware-style cyberattacks may be common and difficult to completely stop, but a best practice backup strategy that includes multiple copies of data on different kinds of media, including tape, can eliminate or minimize data loss.

ABOUT THE UNIVERSITY

The university in this case study is one of the premier institutions of higher learning in the world, offering a complete curriculum of undergraduate and graduate programs across the arts and sciences to an engaged and diversified student body. It is also one of the nation's leading research institutions, generating globally significant discoveries in the natural sciences, social and behavioral sciences, engineering, information technology, and humanities.

Quantum

www.quantum.com

CS00408A-v01