HOW TO ENSURE YOUR BACKUPS PROTECT YOU FROM RANSOMWARE

by George Crump

Storage Switzerland, LLC

Ransomware is a multi-billion dollar business. In fact, CyberSecurity Ventures expects ransomware payments to exceed $11.5 billion in 2018. Ransomware is a big business, and it is motivating the malware developers to get increasingly more sophisticated in their attack methods. These developers know that infected organizations resort to their backups first when attempting to recover from the attack. As a result, they are targeting backup software configuration files and backup data as part of their attack. IT planners need to make sure that their backup solution is secured in addition to the organization's data.

RANSOMWARE RECOVERY CHALLENGES

Recovering from a ransomware attack is different from recovering from any other disaster. Ransomware does not destroy data and in many cases doesn’t impact all of the data within an organization. Ransomware files often sit idle for days or weeks before triggering, which means that multiple backup jobs may backup up the malware file. During the scramble to recover from the ransomware attack, the administrator may accidentally recover the infected file, which re-triggers itself and starts encrypting data all over again, leaving the organization in an endless attack loop.

Another unique aspect of a Ransomware attack is that the organization does have an alternative to recovery by paying the ransom. Paying the ransom has its own set of problems. Top of the list is that paying ransom doesn’t guarantee that organizations will get their data back. The executive team though may deem those problems worth the risk to get back into operation more quickly than going through the restore process. As a result, recovering from a ransomware disaster has built-in competition, and the restoration process has to be quick and painless enough not to tempt the organization to pay the ransom.

> “CyberSecurity Ventures expects ransomware payments to exceed $11.5 billion in 2018.

RANSOMWARE RECOVERY CHALLENGES

The biggest challenge facing organizations though is that the backup configuration files and the protected copy of data are targets of the attack. All forms of protection are targets including snapshots, backups, and replicated copies. Many data protection software solutions are vulnerable to attack. They often host the entire backup operation on Windows Servers (a prime target of ransomware). They also do little to limit access to the configuration files or the protected data set. The thought of the backup software itself being a target seems to have never occurred to its developers.

REQUIREMENTS FOR BACKUP RECOVERY SUCCESS

The backup application is a logical first stop when trying to recover from a ransomware attack, but the backup software has to meet five critical requirements. The first requirement, deep integration with primary storage, is critical to meet the recovery performance expectations. Backup solutions need to control primary storage snapshots instead of running them as a separate process.

With primary storage integration, the backup software can manage the snapshot schedule performing snapshots on an hourly basis, thus minimizing the amount of data loss if ransomware strikes. The backup software can then back up the snapshot instance. From a recovery standpoint, recovering from a snapshot if it is not infected is the fastest form of recovery.

The second requirement is for the backup software to understand the fastest source for recovery. Ransomware typically impacts entire volumes with millions of data files on them. If IT is performing frequent backups, the fastest form of recovery may be to restore the entire volume back to its former state. There are several ways to accomplish a rapid recovery of an entire volume.

As long as they are not infected, snapshots, again, are the obvious choice for rapid recovery. If the snapshot is infected, other options should be available including an image restoration or a “boot from backup" capability. If time allows, image restoration is generally preferred as it puts the data back on a production class storage system. The problem with “boot from backup” technology is the backup storage system is typically inadequate to stand-in for the production system. The advantage of “boot from backup” is that there is no data movement and users can access data sooner. As long as the backup storage system can deliver adequate performance, then this may be a preferred method.

REQUIREMENTS FOR BACKUP RECOVERY SUCCESS

Most "boot from backup" technology always assumes that the recovered system is a virtual machine, not a bare metal system. Most file servers and network attached storage (NAS) systems are bare metal systems, so the "boot from backup" technique has no value. In these situations, which may be very common, the ransomware recovery situation requires rapid bare metal recovery. It is essential that the bare metal recovery capabilities be able to recover to dissimilar hardware and that it can recover both system information and data as well.

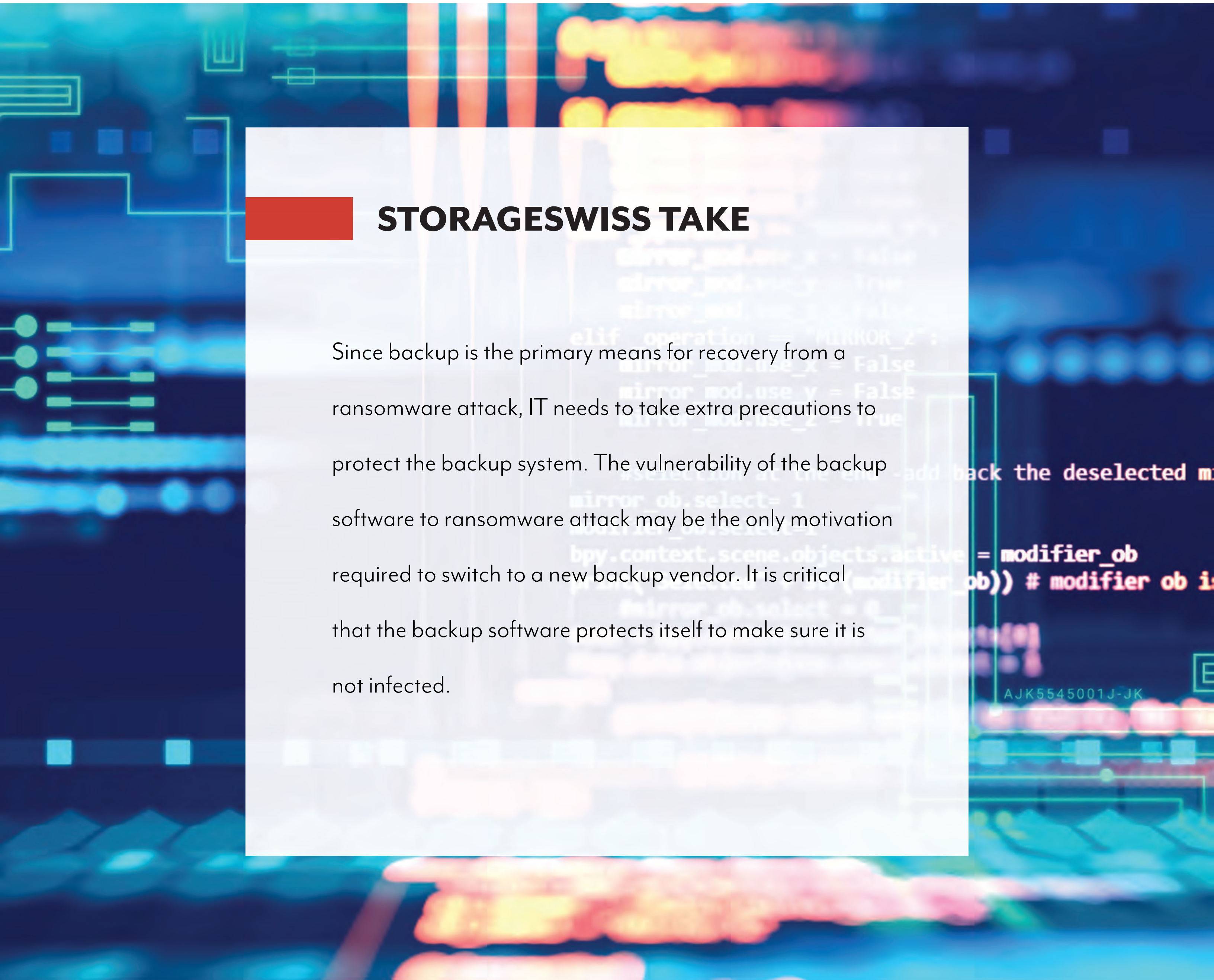
A final requirement, and potentially the most important, is to secure backup configuration files and the protected data itself. It is vital that the backup application only allow modification of its configuration files from within the application and not allow external modifications. The backup software should encrypt data in-flight and at-rest and only allow decryption of files from within the backup application. To protect the backed up copies the backup software should possess the ability to store copies of data on multiple targets, including snapshots, backup appliances, and various cloud locations.

WHAT TO DO IF RANSOMWARE STRIKES

- Identify the Attack: When ransomware strikes an organization, the first step is to identify the attack. Third party software applications and increasingly, operating systems can alert administrators of a high rate of change.
- Identify File Zero: The next step is to identify "file zero", the malware file itself. IT needs to remove this file from all storage systems (it may be in multiple places), it also needs to exclude the file from any recovery attempts.
- Identify Known Good Copies: The third step is to identify known good copies, data not infected by the malware. IT can do this by looking at changed files before recovering them. The backup application should have the ability to compare the current file system to data previously backed up. IT should carefully examine each file changed since the malware first attacked before restoring them. In most cases, an encrypted file is larger than its original. Also suspect are files that were inactive for a long period, and suddenly all changed at about the same time.

WHAT TO DO IF RANSOMWARE STRIKES

- Recover Rapidly: Look for the best source of recovery. The backup software should provide guidance and the fastest recovery point. If a recent snapshot copy is available or if the ransomware attack was an "all-at-once" type of attack, then it is an ideal restore point because no data needs to move across the network. Boot from backup is typically the second choice. Another method, if the backup software supports it, is an incremental recovery, which only recovers files changed between specific date ranges.
- Monitor for Reinfection: The final step is to monitor closely for reinfection. In most cases, if the malware file made it into the backup infrastructure, once restored, it automatically starts re-encrypting data immediately since all the trigger dates have passed.



STORAGESWISS TAKE

Since backup is the primary means for recovery from a ransomware attack, IT needs to take extra precautions to protect the backup system. The vulnerability of the backup software to ransomware attack may be the only motivation required to switch to a new backup vendor. It is critical that the backup software protects itself to make sure it is not infected.

ABOUT US

Storage Switzerland, LLC

Storage Switzerland is an analyst firm focused on the storage, virtualization and cloud marketplaces. Our goal is to educate IT Professionals on the various technologies and techniques available to help their applications scale further, perform better and be better protected. The results of this research can be found in the articles, videos, webinars, product analysis and case studies on our website storageswiss.com

MICRO® FOCUS

Micro Focus Data Protector includes a range of solutions that enable an adaptable, smart backup and recovery environment, which can evolve with your business. It enables you to take action in real time, based on insights into your backup data. With an agile, adaptable backup infrastructure, you can confidently deal with the infrastructure complexities and uptime challenges of your business, such as 24x7 operations, hybrid IT, continued growth of data, technology disruptions, and increasingly demanding recovery objectives. The suite facilitates a deep, 360-degree analysis of the backup environment and its processes via insights, allowing you to adapt and tune your environment to run at optimum levels.

George Crump is President and Founder of Storage Switzerland. With over 25 years of experience designing storage solutions for data centers across the US, he has seen the birth of such technologies as RAID, NAS and SAN. Prior to founding Storage Switzerland he was CTO at one the nation's largest storage integrators where he was in charge of technology testing, integration and product selection.