Protection Strategies Against Ransomware

This article provides some general advice against protecting your systems and backups against a class of threats commonly known as **Ransomware**.

> *Ransomware is a type of malware which restricts access to the computer system that it infects, and demands a ransom paid to the creator(s) of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive (cryptoviral extortion, a threat originally envisioned by Adam Young and Moti Yung), while some may simply lock the system and display messages intended to coax the user into paying.*

Source: Wikipedia (March 10th 2015)

The good news is that by having system backups you already have some protection against these (and any other) types of viruses. If a system is infected you can simply restore the system to a pre-infection state from one of your backups.

Unfortunately, these types of viruses can now spread throughout your network and potentially encrypt your backups. This type of attack was popularised in 2014 by a virus known as **Cryptolocker**.

This article will cover some of the ways you can protect your backups from becoming encrypted and thus allowing you to restore your systems.

Write-once Media Backups

The simplest way to protect your backups is to use backup storage that can only be written to once. These are usually optical media such as CD-R, DVD-R and BD-R. These discs can only be written to once i.e. at the time of backup and so even if a virus has access to the disc if it is still in the disc tray it cannot alter the data on the disc.

Be careful using **re-writable (RW)** backup media if you wish to protect against this kind of threat as the backups contained on the disc could be altered if attached to the computer when the virus strikes. In general, as long as the discs are removed immediately after backup and stored offline then they should be okay but the write-once media is generally preferable for backup.

Advantages

- **Cost-effective** - With the exception of Blue-ray discs, optical media is generally very cheap when compared to other storage formats
- **Physical protection** - Write-once media physically prevents alterations to the data which means it is fail-safe and not reliant on users following backup procedures

Disadvantages

- **Speed** - Optical media is considerably slower than other backup media
- **Capacity** - Storage capacity of optical media is much lower than the average capacity of SSD & HDD storage and so multiple discs will often be required for backups
- **Delicate** - Optical media is prone to scratches during handling. This can lead to data becoming unrecoverable which generally makes optical media an inadvisable choice for backups, especially when using incremental backups as one broken backup affects the rest of the backup chain.

Summary

Whilst write-once media is a quick and simple solution to protect against these kinds of threats it is not a method we can particularly recommend except in very trivial circumstances such as for the occasional full home backup. In all other circumstances you will want to be taking regular incremental/differential backups as part of a wider rotation scheme and optical media is ill-suited to these kinds of backup schemes.

Offline backup storage / Archiving

As mentioned earlier: ransomware often spreads throughout a network. Therefore a solution is to keep backups off the network. This presents a problem, however, as to backup an organisation you will generally have your storage available over a network connection.

The key to offline backup is to backup to a location inaccessible to any virus that may get onto the system. This can be achieved with Macrium Reflect by creating **backup scripts** that can copy a backup to another location via FTP / SCP once a backup completes. This is made easier in Macrium Reflect Version 6 with the introduction of Powershell scripted backups, in addition to the existing options of VBScript and Batch file backups.

Advantages

- **Flexibility** - As this involves scripting, you can tailor the solution to meet the needs of your network/system. It can also be incorporated into existing backup schemes you may already employ
- **Capacity** - Compared to optical media, discussed previously, you can use traditional HDDs for your backup. Allowing you take advantage of RAID arrays, SAN / NAS devices etc.

Disadvantages

- **Technical Requirements** - The use of scripting is not a solution that is readily available to non-technical users. However, as long as you have a technical person to create the scripts you can often automate script execution through scheduling to deploy this across an organisation

Summary

Hopefully it is clear that this solution is the recommended approach. Although it has clear technical barrier, one of the core aims of Macrium Reflect Version 6 was to improve our scheduling and scripting options to give our users maximum flexibility to create a backup scheme that works for them.