Mitigate the threat of Ransomware with QNAP NAS

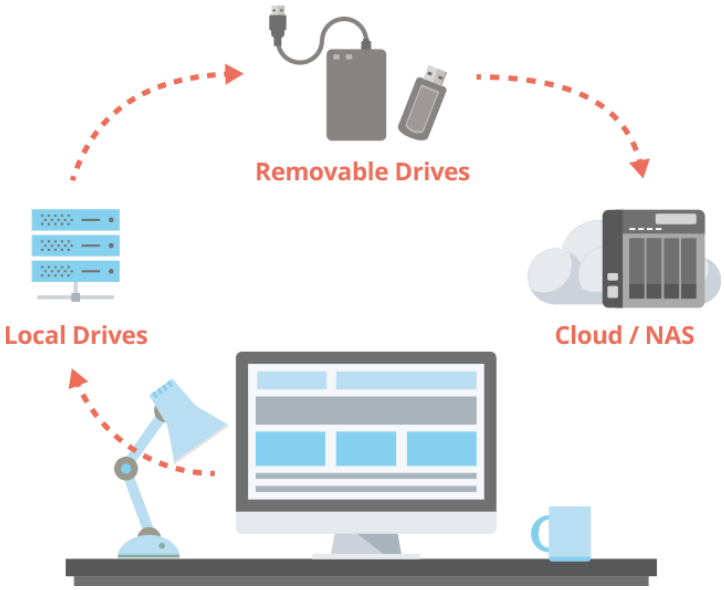
Protecting Your Data from Ransomware

Make a recovery plan against encryption-based locker viruses

Ransomware is a rising threat against both business and home users that targets computers and network-based devices. A simple yet effective method of mitigating the threat of ransomware is to ensure that you always have up-to-date, remotely-stored backups. QNAP NAS is an ideal backup center that includes comprehensive backup features and supports point-in-time snapshots to help individuals and organizations protect important data, restore files, and avoid downtime.

What is locker ransomware?

Locker is a file-encrypting ransomware (Cryptolocker, CTB Locker, TeslaCrypt, and others) that encrypts files found on local drives, removable drives, mapped network drives, and even Dropbox mappings. Victims will be extorted a ransom to decrypt the affected files, or they will be unable to open the affect files ever again.



Gateway Computer Resources Limited
Address: Unit 2305-06, 23/F, 1 Hung To Road, Kwun Tong, Kowloon
Tel.: 2318 5300
Email: enquiry@gcr.com.hk
Website: www.gcr.com.hk

… And why is locker ransomware so troublesome?

- Ransomware is typically spread through phishing emails, and mostly hidden in emails as attachments like .zip, .pdf, .doc, .exe, .js files, and more. It is difficult to identify, and self-spreading.
- Traditional antivirus may not detect next-generation ransomware.
- Locker ransomware uses asymmetric encryption or more advanced encryption methods which can be difficult (if not impossible) to break locally.
- Victims are forced to pay (normally by untraceable means) to restore their files, or they face losing them forever.

Back up with QNAP NAS to save your files

While the first line of defense against being affected by malicious software is being careful and practicing sensible usage habits (regularly updating your software, not opening untrustworthy emails, not visiting unknown websites, etc), you should always remember to back up your data.

QNAP NAS provides a simple solution for backing up/restoring files and data. Its Linux-based QTS operating system makes it more secure than Windows® systems that are more at risk from being attacked. Moreover, the native support for point-in-time snapshots that are operated separately from the file system makes QNAP NAS a reliable backup solution for reacting quickly for backing up and restoring important files and system data.

Snapshots: React quickly for backing up and restoring

Snapshots record the metadata of files outside the file system and allow users to preserve and restore multiple versions of the same file, folder or even the entire volume. If ransomware attacks or an unexpected situation arises on your system, you can quickly and easily revert back to the previous state that the snapshot has recorded.

Gateway Computer Resources Limited
Address: Unit 2305-06, 23/F, 1 Hung To Road, Kwun Tong, Kowloon
Tel.: 2318 5300
Email: enquiry@gcr.com.hk
Website: www.gcr.com.hk

- *Block-based snapshots*

QNAP's block-based snapshot supports incremental backups to save storage space. While copying only the changes made, it also saves time for backing up and restoring.

- *Restore in a click*

Data recovery through snapshots only takes a few minutes. As they are separated from the file system, snapshots allow users to restore the original, unencrypted files even if the volume is affected by ransomware.

- *Snapshot Replica*

After creating snapshots, you can efficiently copy them to another QNAP NAS for double protection.

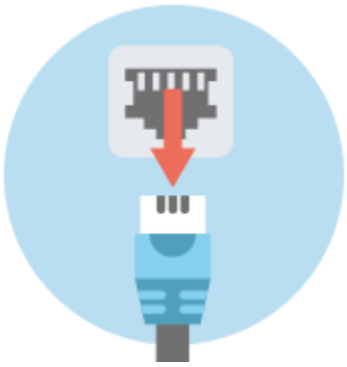
Note: Snapshots require a QNAP NAS with at least 4GB RAM.

Gateway Computer Resources Limited
Address: Unit 2305-06, 23/F, 1 Hung To Road, Kwun Tong, Kowloon
Tel.: 2318 5300
Email: enquiry@gcr.com.hk
Website: www.gcr.com.hk

Steps to restore your files with snapshots

QNAP Lab simulated a ransomware attack, and confirms that the following steps are suitable for recovering data with QNAP snapshots.

- Use QNAP NetBak Replicator (or another backup tool) to regularly back up files to the NAS with user accounts that only have limited access rights (highly recommended), and then configure the snapshot function with the administrator's account.



- If you notice ransomware activity or are presented with a ransom message, immediately disconnect your computer from the Internet, and remove the connection between the infected computer and NAS. If possible, disconnect the network cable from the NAS too to prevent the virus from spreading.

Gateway Computer Resources Limited
Address: Unit 2305-06, 23/F, 1 Hung To Road, Kwun Tong, Kowloon
Tel.: 2318 5300
Email: enquiry@gcr.com.hk
Website: www.gcr.com.hk

- If you have a NAS with HDMI output you can connect a mouse, keyboard and HDMI monitor to the NAS, and access the NAS using HD Station. If your NAS lacks HDMI output, then when connecting to the NAS please ensure that your computer does not mount any infected shared folders until the snapshot is restored.

- Click “Storage Manager”, and check the “Snapshot Manager” to see a list of snapshots.

Gateway Computer Resources Limited
Address: Unit 2305-06, 23/F, 1 Hung To Road, Kwun Tong, Kowloon
Tel.: 2318 5300
Email: enquiry@gcr.com.hk
Website: www.gcr.com.hk