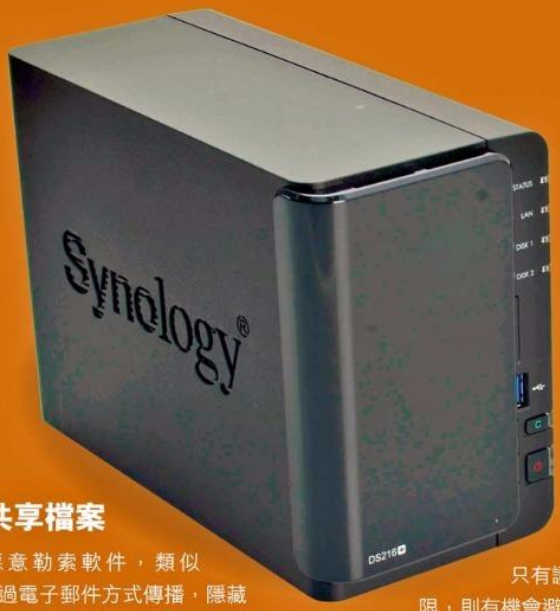
Locky 病毒無有怕！NAS 防勒索備份攻略

Locky 惡意勒索軟件肆虐全球，不少用戶皆「中招」，更會影響內聯網的其他電腦甚至 NAS。e-zone DIY 針對 NAS 系統，提供防止 Locky 勒索的備份攻略。



加密 SAMBA 共享檔案

Locky 是一種惡意勒索軟件，類似 CryptoLocker，主要通過電子郵件方式傳播，隱藏於 ZIP、PDF、DOC 等常見文件內，更可能扮成單據或要求簽署文件，使用家的警覺性降低而直接開啟，電腦便會立即「中招」。電腦內的文件檔案會被加密，要求用戶付款才可解鎖。由於檔案以 RSA4096 再配合 AES256 方式加密，其強度達軍用級數，用家難以靠一般方法自行解密。

惡意勒索軟件恐怖之處，在於它不只影響電腦本機磁碟內的文件檔案，更會感染已掛載（Mount）的網絡磁碟（Network Drive），更甚會在內聯網絡（Intranet）搜尋已啟用 SAMBA 共享服務的電腦及 NAS，加密提供寫入權限的共享檔案，使「受災」範圍不斷擴大。

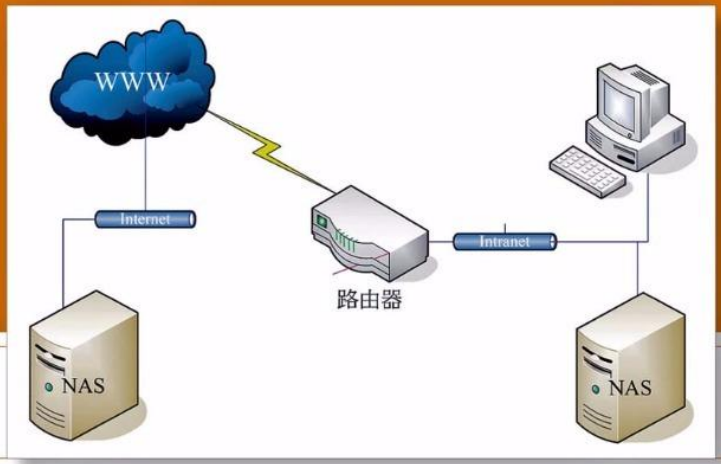
一般備份未必有用

由於惡意勒索軟件是透過已感染的電腦進行攻擊，故在 NAS 層面無法完全預防。它利用電腦已登入的帳號，使用其擁有的 SAMBA 存取權限，對 NAS 內的檔案進行加密。只要電腦所登入的帳號，擁有 NAS SAMBA 服務的寫入（Write）權限，NAS 內相關的檔案將會被加密。相反，如帳號只有讀取（Read Only）權限，則有機會避過影響。

正常情況下，保護重要資料的最佳方法，是經常備份至其他媒介如：外置硬碟或 NAS，不過對於 Locky 這類惡意勒索軟件，一般資料備份方式未必有效。因為，受 Locky 感染的電腦會主動搜尋已連接的內置、外置硬碟，甚至 NAS 進行攻擊，如備份目的位置是受感染電腦能直接存取，備份檔案同樣有機會受感染及加密。所以，針對 Locky 這類高度傳染性的惡意勒索軟件，只有使用特別備份方法，甚至是異地備份，將備份資料與受感染的電腦完全隔離。

三大備份方案

資料備份方案一般可分為三類，第一類為本地備份（Local Backup），即資料會儲存於同一 NAS 內建硬碟或外置硬碟上；第二類則是遠端備份（Remote Backup），即資料會經網絡傳送到第二部 NAS、電腦或雲端伺服器儲存；第三類則為快照備份（SnapShot），以回復任何一個時間點的檔案，並使用比傳統備份更少的儲存空間。



遠端備份將資料經網絡存於另一部 NAS 上，並只有專屬程式使用專屬帳戶才可進行備份。

Backup 01 本地備份強化

針對 Locky 一類惡意勒索軟件，本地備份的設定需特別修改，目的是讓受 Locky 病毒的電腦無法以 SAMBA 方式變更備份位置的檔案。以 Synology DS216+ 示範本地備份方法，其他牌子 NAS 的設定方法亦大同小異。

STEP 01 建立備份專用資料夾

首先要建立一個為備份而設的專用資料夾，並將它設為只有「Admin」帳號才擁有「讀寫」存取權限，而一般帳號包括：平日於電腦經 SAMBA 存取 NAS 的帳號則設為只有「唯讀」權限。

STEP 02 建立本地備份

要建立本地備份，進入 DSM NAS 設定介面，於「Hyper Backup」內選擇「新增」→「資料備份任務」，備份目的地類型，選擇「本地共用資料夾」。

STEP 03 選擇備份目的地、備份資料

跟着選擇備份資料儲存位置，需要備份的資料夾，用家可同時選擇多個資料夾。

STEP 04 設定備份密度

用家可選擇定時執行備份，不過在備份進行期間，NAS 會出現頻密的讀寫動作，並會影響 NAS 之 SAMBA 服務效能，同時更有機會將已感染及加密的檔案覆寫原有檔案。故建議每天深夜或凌晨才進行備份。

STEP 05 設定備份版本控制

部分新型 NAS，可支援備份版本控制功能，即在 NAS 內保留多個備份版本，即使原有資料被已被加密的檔案覆蓋，也能在舊有備份版本中尋回及還原，惟此會佔用更多儲存空間。

Backup 02 遠端備份攻略

與一般備份方法相比，遠端備份可透過網絡進行資料交換，用以確保兩個不同位置的資料能進行同步。由於已感染 Locky 的電腦無法直接經 SAMBA 方式存取遠端 NAS，故它無法對遠端已備份的檔案進行加密。

現時，不少 NAS 如：QNAP、Synology、Thecus 等皆支援遠端備份功能，除它們自家備份方式外，更對應「Rsync」備份技術。「Rsync」是《Unix》系統的應用軟件，它能同步更新兩個不同位置的檔案及目錄，並利用差分編碼（Delta Encoding）對備份數據進行分析，以減少數據傳輸。以下利用 Synology DS216+ 示範作「Rsync」進行 NAS ⟷ NAS 間之備份。

STEP 01 啟用 Rsync服務

大部分 NAS 內建「Rsync」服務預設為關閉，用家先要到「控制台」→「檔案服務」→「rsync」啟用相關功能，同時選擇或建立「Rsync」專用的帳號及密碼。此外，用家也可限制備份時所佔用的網絡頻寬。

STEP 02 客端建立備份任務

在本地 NAS 設定介面，於「Hyper Backup」內選擇「新增」→「資料備份任務」，備份目的地類型，選擇「遠端 rsync 伺服器」，輸入已啟用 Rsync 服務的 NAS I.P. 位址、連接埠及於 Step 01 建立的帳號。

STEP 03 設定備份

跟着，選擇需要備份的資料夾，以及選擇定時執行備份，使用網絡頻寬、是否壓縮等設定，還有是否啟用備份版本控制。

NAS 事前備份最重要

利用以上特別的備份方法，電腦即使被惡意勒索軟件入侵，也可快速地將已被加密的檔案還原至原有版本。不過，以上所有備份方法，必須在電腦被感染前進行，否則沒有效用。

Backup 03 快照備份

快照備份功能原只用於商用型號，但最近已有廠商引入至高階家用 NAS。NAS 快照備份是以 Block 的差異作為快照基準，將有異動的部分進行快照紀錄，而且快照亦會以增量備份的形式節省儲存空間，備份及還原所需時間大幅減少，用家可隨時將檔案還原至指定時間。

STEP 01 轉用 Btrfs 檔案系統

以 Synology NAS 為例，必須使用 Btrfs 檔案系統，才能啟用快照功能，如使用舊有 EXT4 的話，則要先備份資料，刪除及重新建立分區。

STEP 02 啟動快照

啟動「Snaphot Replication」，在「快照」內選擇要備份的資料夾，再按「設定」，選取「啟動快照排程」及執行日期、時間、密度等。

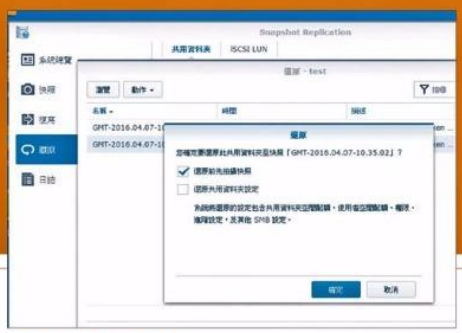
STEP 03 選擇快照版本

最後在「保留」內選擇要保留的快照版本，可選擇保留最新 256 個，已相當足夠。

感染後應對方法

以上是針對惡意勒索軟件的事前備份方法，當發現電腦已被感染，應如何救援檔案？首先，用家要以一部安全的電腦，以 Web 方式登入 NAS 介面，如使用首兩種備份方法，可在「Hyper Backup」內選擇備份任務，再以「備份瀏覽器」檢視已備份的檔案，如已啟動版本控制，可選擇較早的記錄然後還原。若使用快照備份，則可於「Snaphot Replication」內選擇「還原」，再點選要還原的時間點。

「備份瀏覽器」檢視已備份的檔案。



點選要還原的時間點。