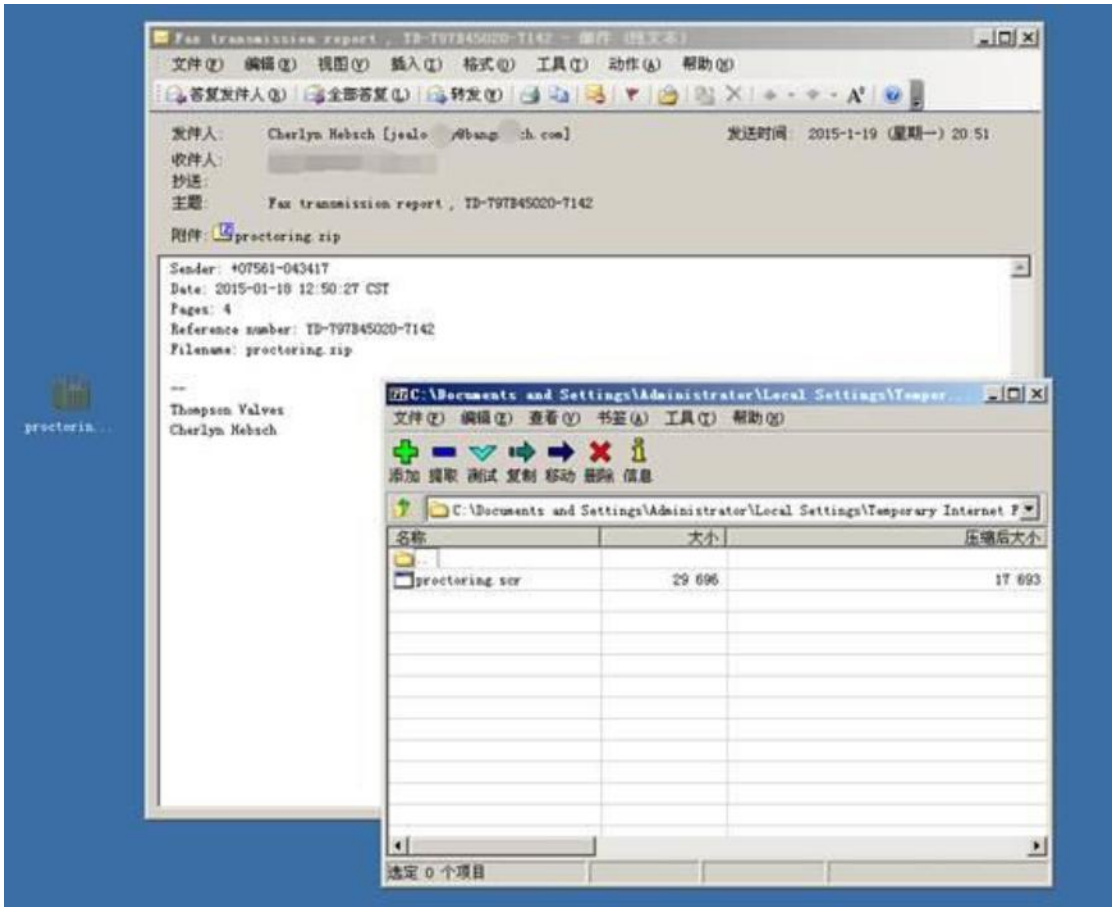
新勒贖軟體病毒警訊通知

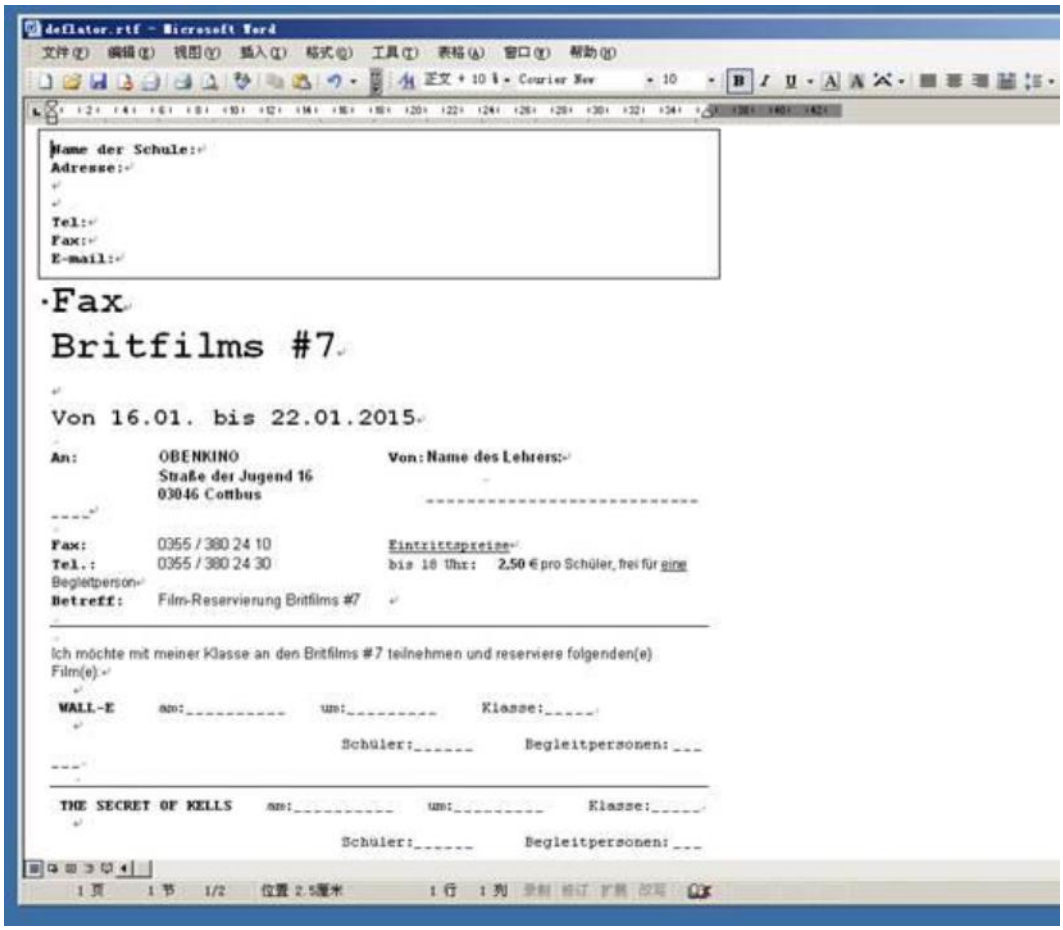
近期有種新的勒贖軟體爆發事件，與之前的勒贖軟體相同，此惡意程式會將自己偽裝成 Email 附加檔案。一旦執行此惡意程式，電腦上的檔案就會被加密鎖定而無法開啟使用，切勿輕易打開來源不明的信件。

此次勒索軟體相關資訊如下：

首先，惡意程式偽裝成一封垃圾信件的附加檔案：



如果使用者開啟（執行）了惡意附加檔案，會打開一個 rtf 類型檔案，用以欺騙使用者，讓使用者認為其為正常檔案：



當此勒贖軟體執行後，即會以勒贖資訊綁架受害者的桌面，使無法關閉該頁面：

如果按下左下角的「View」按鈕，會列出遭到加密的檔案：

此勒贖軟體還能夠任意恢復若干加密檔，以顯示其“真實性”：

目前建議採取的防護方法：

1. 將防毒軟體病毒碼更新至最新

2. **不要隨意開啟來源不明的郵件附加檔案**

3. 不要輕易瀏覽未知的國外網站，尤其是色情網站或是影片下載網站

4. 請隨時備份重要檔案注意備份