關於 LOCKY 的參考資訊

1. Locky 與電郵病毒

電郵病毒是透過不同的標題或內容吸引受害人開啓附件（如仿冒政府或機構發出電郵，要求用戶確認附件內容等），附件有可能是 WORD 文件、EXE 執行檔、壓縮檔（ZIP、RAR、7zip....）等不同的檔案格式，當受害人不慎開啓含有病毒的附件後，病毒程式便會運作，使電腦中毒。電郵病毒亦會透過用戶點擊含有惡意編碼的網站超連結而令電腦受感染。電郵病毒通常透過監聽電腦上進行的操作，從中竊取個人資料和登入密碼等，再利用有關資料牟取利益，或使電腦癱瘓等不同形式損害受害人的利益。

而 Locky 加密勒索軟件亦屬電郵病毒之一，當用戶打開電郵附件或點擊含有惡意編碼的網站超連結時，便會令電腦受感染，Locky 會加密受害者電腦的檔案，並為它們加上 ".locky" 副檔名，令檔案無法使用，黑客籍此要脅受害者以比特幣 (bitcoin) 支付贖金以換取解密密鑰以恢復數據。

2. 注意事項和預防方法：

即使已針對電郵病毒加以過濾攔截，但黑客經常會使用新技術來散播病毒，故過濾攔截並沒有辦法保證萬無一失。因此，須注意以下事項和預防方法：

- 電腦應安裝防毒軟件，並按實際情況配置含有 UTM(Unified threat management)模組的防火牆；
- 確保防毒軟件和防火牆的病毒資料庫作定期更新；
- 定期進行電腦掃描；
- 定期執行系統漏洞更新，避免因為系統漏洞令病毒有機可乘；
- 收到來歷不明的郵件時，不要開啟其附件檔案；
- 點選郵件的超連結前，留意該連結是否有可疑：
  - 如郵件是由某某銀行發出的通知，但其超連結卻不是該銀行的網址；
  - 奇怪的網址，如 yah00.com、gaogle.com 等；
  - 使用 IP 作為網址，如http://172.16.1.1/main.asp；
- 如要求索取帳號密碼等敏感資料時，宜先向機構確認其真確性；
- 如必需打開附件，可在打開前先使用防毒軟件進行掃描；
- 遇到郵件內容含糊的郵件，其中沒有任何識別你或寄件者的資訊時，請小心謹慎；
- 定期對重要資料進行備份和建立系統還原點。

3. 受感染後的處理措施：

當您懷疑或知道電腦已經受感染，可以按照以下建議步驟進行補救：

- 應立即斷開網絡，以免病毒透過網絡散播到其他電腦中；
- 為其他網絡中的電腦進行檢查；
- 刪除帶病毒的郵件；
- 使用另一台安全的裝置更改網絡和電郵等重要系統的登入密碼；
- 被加密的檔案暫未有有效方法復原，故建議按需要在備份中恢復有關檔案；
- 如中毒症狀仍然出現，可考慮進行系統還原，或對重要資料重行備份，再對系統進行格式化，重裝系統以杜絕病毒。

- 完 -