CryptoLocker

-簡介及應變措施

北區 ASOC 團隊 2014/4

1. CryptoLocker 簡介

CryptoLocker 是 2013 年下半年出現的新型態惡意軟體，多透過殭屍網路發送含有惡意程式的郵件，一旦使用者不慎執行附件中的程式後，CryptoLocker 便會開始搜尋系統本機內的特定格式檔案(*excel*、*word*、*ppt*、*AutoCAD 以及 jpg 圖檔等*)，並利用 RSA 以及 AES 方式，將這些檔案加密，而在完成加密作業之後，便會出現勒索訊息，要求將特定金額匯入特定帳戶內，以取得將檔案解密的私鑰，也由於 CryptoLocker 所使用的加密長度達 2048 位元，使得要採暴力破解方式解密幾乎是不可能，RSA 高強度的安全性反而成為惡意攻擊者進行攻擊的利器，顯得十分諷刺。CryptoLocker 所針對的目標檔案，都是使用者日常生活中時常利用的檔案格式，故有為數不少的使用者向攻擊者支付贖金以取得解密的私鑰，但由於 CryptoLocker 加密過程中的缺陷，某些情況下，即使取得解密的私鑰，也無法將加密過後的檔案 100%還原。清除 CryptoLocker 本身並不困難，但若讓惡意程式完成加密作業，即使清除惡意程式，也無法將檔案還原，故在發現系統感染 CryptoLocker 時，須立刻切斷網路，清除惡意程式，避免完成加密程序。

2. 攻擊手法

CryptoLocker 大多利用電子郵件散播，利用大量殭屍網路主機濫發郵件，附件中帶有一個偽裝為 PDF 檔案的可執行檔，誘騙用戶執行惡意程式，一旦系統感染後，CryptoLocker 會先修改系統相關安全性設定，及系統登錄檔，讓自身於系統開機時，自動被執行。同時與多數惡意程式一樣，會隱身於系統之中，並與中繼站 Server 聯繫，進行 RSA 加密金鑰的配對作業，取得公開金鑰後，便執行目標檔案的加密程序，等到使用者發現之時，多數目標檔案已完成加密程序，加上解密的私鑰掌握於攻擊者手中，除了支付贖金外，大多已難以挽回。而感染 CryptoLocker 的主機，亦會透過區域網路來意圖感染其他主機，造成內部主機大規模感染。

3. 建議措施

在了解 CryptoLocker 的背景及攻擊手法後，我們可歸納下列重點防禦事項，避免受到 CryptoLocker 這類型的勒索軟體攻擊;

- 定期更新防毒軟體的病毒碼
- 定期更新作業系統，修補系統漏洞
- 定期備份主機內重要檔案
- 對於來路不明的郵件，不要開啟任何附件

倘若被防毒軟體偵測出系統已感染CryptoLocker，在顯示出勒索訊息前，可先將系統檔案備份至異地，同時切斷主機網路，避免完成加密程序。同時也要確認區域網路內主機是否有遭感染跡象，在備份完成後，建議重新安裝作業系統，並執行系統更新與安裝防毒軟體。定期更新系統及防毒軟體病毒碼，及定期異地備份資料等。這幾個資安要點若能於組織中落實運作，不管是面對CryptoLocker或是其他類型的惡意程式，都能將風險降至最低，現今面對充滿惡意程式的網路環境，也唯有如此才能確保自身系統與資料的安全。

參考資料

http://www.ithome.com.tw/node/83212
http://www.ithome.com.tw/node/83226
http://zh.wikipedia.org/wiki/CryptoLocker

北區學術資訊安全維運中心