勒索軟體CryptoLocker

勒索軟體CryptoLocker大舉入侵
企業陷檔案滅亡危機

攻擊途徑

- 透過釣魚郵件挾帶惡意附件檔案，誘使受害者開啟惡意程式
- 在被挾持的傀儡電腦安裝惡意程式

攻擊特性

- 以AES、RSA 2048等高等級加密技術將受害電腦的檔案加密鎖死
- 勒索受害者9,000元（300美元），以贖回解密的密碼
- 限時3天內付款，否則銷毀可解密的私鑰，使得檔案無法救回
- 透過Bitcoin虛擬貨幣，以及MoneyPak、Ukash、cashU等匿名交易機制付款

受影響的電腦系統

- CryptoLocker只影響Windows作業系統

認識CryptoLocker

- 9月初，一隻名為**CryptoLocker**的勒索軟體（Ransomware）開始出現蹤跡，**它會悄悄地將受害者電腦裏的檔案加密，讓使用者無法開啟檔案，也沒辦法破解加密**，藉此勒索9,000元（300美元）的解密贖金。
- 此軟體**透過釣魚郵件入侵**，將受害者電腦的重要文件和檔案全數加密，導致檔案無法存取，而且**駭客採用高超的加密技術(RSA 2048 bit)，讓受害者無法自行復原**，並限期內支付贖金，否則將毀損解密金鑰。

滲透的方式

- CryptoLocker是透過典型的社交工程來散播惡意程式，像是**釣魚信件、聊天工具或惡意網站等。**
- **釣魚信件則是仿冒成知名的物流或是金融公司**，如FedEx、UPS、DHC等
- 並夾帶暗藏惡意軟體的壓縮檔附件，**附件檔的名稱還刻意偽裝成「xxxxxxxx.pdf.exe」，因作業系統隱藏副檔名的緣故，讓使用者誤以為是PDF文件檔，點選附件檔案而感染電腦。**

From: Dun & BradStreet
Date: Thursday, September 05, 2013 11:13 PM
To: [redacted]
Subject: FW: DNB Complaint - 2891375
Attach: DNB_Case_2891375.zip (12.7 KB)

Dun & BradStreet

New Inquiry

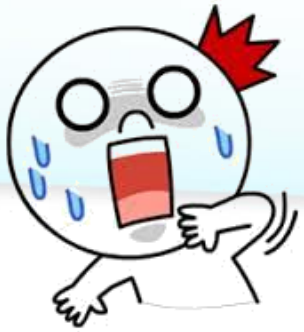
New Complaint : 2891375

Dun & Bradstreet has received the above-referenced complaint from one of your customers regarding their dealings with you. The details of the consumer's concern are included on the reverse. Please review this matter and advise us of your position.

In the interest of time and good customer relations, please provide the DnB with written verification of your position in this matter **by Sep 6, 2013**. Your prompt response will allow DnB to be of service to you and your customer in reaching a mutually agreeable resolution. Please inform us if you have contacted your customer directly and already resolved this matter.

The Dun & Bradstreet develops and maintains Reliability Reports on companies across the United States and Canada . This information is available to the public and is frequently used by potential customers. Your cooperation in responding to this complaint becomes a permanent part of your file with the Dun and BradStreet. **Failure to promptly give attention to this matter may be reflected in the report we give to consumers about your company.**

We encourage you to print this complaint (attached file), answer the questions and respond to us.



中毒後的情形

- 企業會發現被CryptoLocker破壞，**通常是受害者看到電腦跳出勒索贖金的畫面，或是發現檔案無法開啟，但已經來不及搶救了。**
- 一旦電腦中毒之後，CryptoLocker會自行複製到作業系統的「%AppData%」目錄下，以亂數命名檔名，讓人不易察覺，並且會在Windows的註冊檔中加入自動執行的項目「HKEY_CURRENT_USER\Software\CryptoLocker」，因而在電腦開機後即自動執行。

中毒後的情形

當受害人支付贖金之後，該程式不會教您如何一步步解開檔案，而是顯示一個大大的對話方塊要您輸入一個交易序號。

CryptoLocker勒索軟體入侵電腦過程

- 新型態的入侵方式仍是採用**釣魚信件**夾帶惡意附件，不過，**惡意附件會先去下載Zbot惡意程式，並不是直接下載CryptoLocker。植入Zbot惡意程式後，會自動下載CryptoLocker，CryptoLocker再連回C&C中繼站取得加密公鑰，利用RSA和AES技術加密受害者電腦中的檔案，完成後跳出勒索贖金畫面。**
- 至於Zbot惡意程式則會竊取受害者的個人資料，例如網路銀行的帳號密碼等。

攻擊檔案類型：

- *.3fr *.accdb *.arw *.bay *.cdr *.cer *.cr2 *.crt *.crw *.dbf *.dcr *.der *.dng ***.doc** ***.docm** ***.docx** *.dwg *.dxf *.dxg*.eps *.erf *.indd *.kdc *.mdb *.mdf *.mef *.mrw *.nef *.nrw *.odb *.odc *.odm *.odp *.ods *.odt *.orf *.p12 *.p7b *.p7c *.pdd *.pef *.pem *.pfx ***.ppt** ***.pptm** ***.pptx** *.psd *.pst *.ptx *.r3d *.raf ***.raw** *.rtf *.rw2 *.rwl *.sr2 *.srf *.srw *.wb2 *.wpd *.wps *.x3f *.xlk ***.xls** *.xlsb ***.xlsm** ***.xlsx**

解密方式：

- **受害者無法自行破解**，若無備份檔案，僅能支付贖金，駭客解密時間依據檔案數量大小，長短不一。

- 就資安公司**目前所截獲的CryptoLocker釣魚郵件，內容皆為英文**。或許是因為英文信，許多人因而躲過一劫。不過，XX科技近日察覺CryptoLocker已有變種病毒，以及透過木馬程式Zbot挾帶CryptoLocker。
- **CryptoLocker僅會對硬碟進行加密**
- **Zbot木馬程式則會竊取受害者的資料，像是網路銀行的帳號密碼。**

受害後的應變之道：

1. **立即切斷網路連線**，避免CryptoLocker拖垮網路連線速度，繼續加密未完成的檔案
2. **尋找有無備份檔案**，若是沒有備份，可透過**Windows內建的系統還原設定**、Shadow Explorer軟體嘗試還原先前的版本
3. **檔案還原完成後**，利用使用微軟Safety Scanner或是防毒軟體，執行完整掃描，清除惡意程式，或是**乾脆選擇重灌電腦**，擺脫CryptoLocker糾纏。

自保之道

1. **隔離受害電腦**，在閘道器上設定駭客可能連線的IP位置，禁止連線至這些地方
2. 更改本機安全性原則（Local Security Policy），讓CryptoLocker無法執行，更可以阻止使用者打開電子郵件中的附加檔案。
3. **加強宣導員工的資安觀念，提高資安意識**
4. **培養資料備份與良好的使用電腦習慣，來路不明的寄件者或是附件，千萬不要開啟**
5. **病毒碼、作業系統、軟體定期更新，落實掃毒**
6. 同步資料的權限僅開啟閱讀權限
7. 不要賦予使用者帳號特權管理者的權力

(一)自保方法：

1. 不要開啟來路不明的郵件。
2. 不要開啟可疑郵件的附件檔案。
3. 不點選不明的網頁及網站。
4. 定時更新防毒軟體。
5. 定時備份重要檔案，落實每天備份和掃毒。
6. 作業系統的安全更新。
7. Adobe、java漏洞要隨時更新。

(二)被駭後之緊急應變措施：

1. 立即切斷受駭PC的網路，避免災情擴大。
2. 更新防毒軟體，清查內網其他電腦，並採取自保措施。
3. 搶救還沒被加密的檔案。
4. 若有備份，開始復原檔案。(外接式HDD)
5. 評估受害災情，決定是否付贖金取得解密金鑰。
6. 用新版防毒軟體清除，或乾脆重灌電腦。

資料來源：

- 勒索軟體CryptoLocker大舉入侵，企業陷檔案滅亡危機。iThome。http://www.ithome.com.tw/node/83529。
- 勒索軟體是什麼？如何預防？(內有資料圖表)。TREND LABS 趨勢科技全球技術支援與研發中心。http://blog.trendmicro.com.tw/?p=12412。