資 訊 處
Office of Information Technology

資安專刊

勒索病毒簡介

中華民國114年4月

編號：029

大綱

一、勒索軟體簡介
二、勒索軟體中毒特徵
三、防禦方法

勒索軟體簡介

什麼是勒索軟體

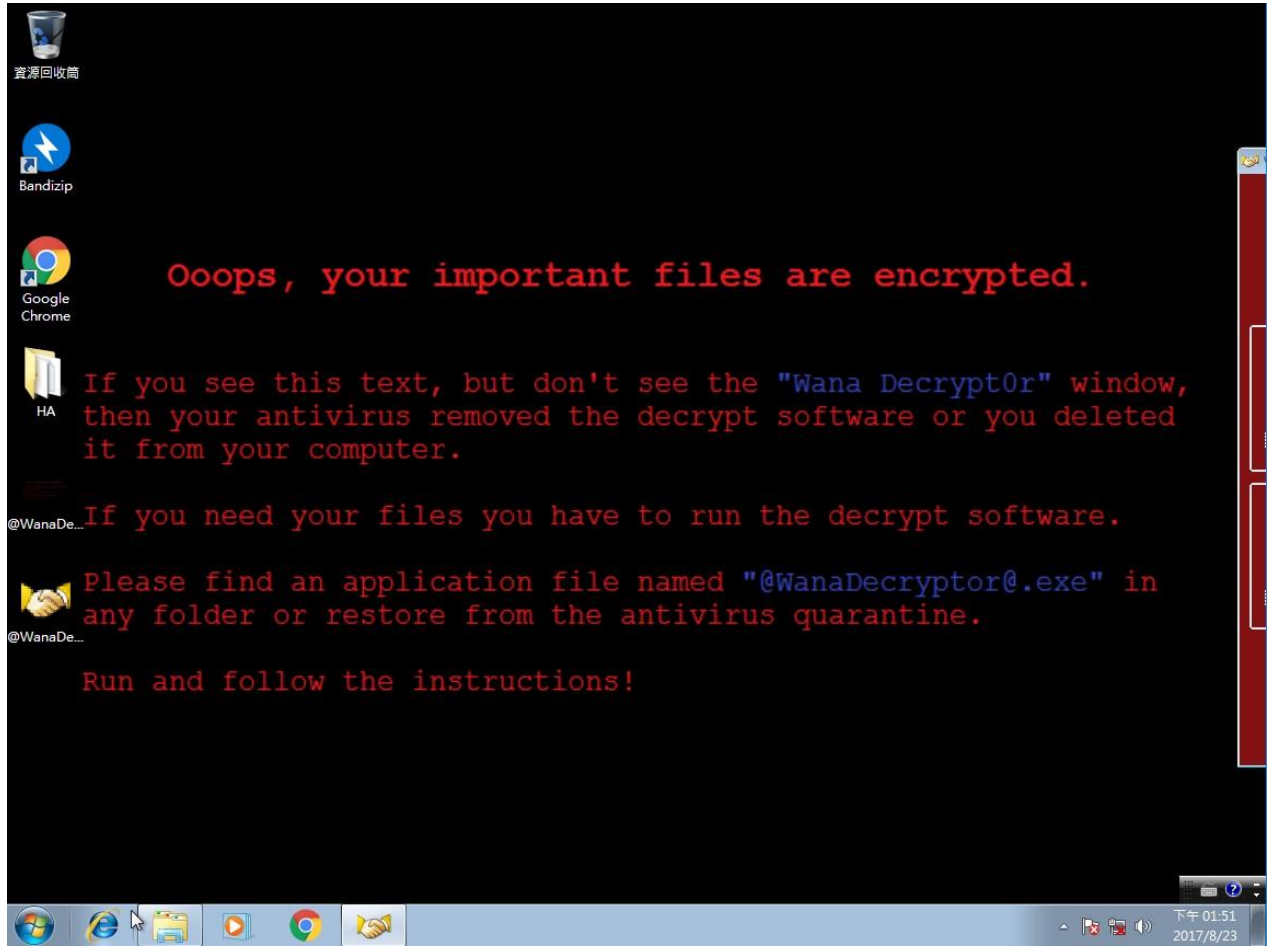
- 一種惡意軟體，會加密資料，並要求支付贖金來進行解密
- 可以透過網路釣魚電子郵件、惡意網站和惡意探索套件進行散佈
- 兩種主要類型
  - ✓ 加密敏感性資料和檔案的加密勒索軟體
  - ✓ 將受害者反鎖於裝置之外的保險箱勒索軟體

常見的勒索軟體

- WannaCry(2017)
  - 利用名為 EternalBlue 的漏洞利用程序在電腦之間傳播；2017 年 5 月 12 日，WannaCry 感染了 150 個國家的超過 200,000 台電腦。
- Ryuk（2018 年）
  - 主要用於針對大型企業。它的營運者向受害者索要巨額贖金。
- Colonial Pipeline攻擊(2021)
  - 美國最大的燃料管道在 2021 年 5 月被勒索軟體攻擊而導致關閉。
- CrazyHunter(2024)
  - 鎖定臺灣的組織與企業，攻擊學校、醫院、一般公司、電子公司甚至連資安廠商也遭受勒索軟體攻擊，駭客透過系統管理者電腦進行橫向攻擊。再利用網內其他主機散播勒索軟體加密檔案，導致多主機內的服務中斷與資料被加密。

勒索軟體中毒特徵

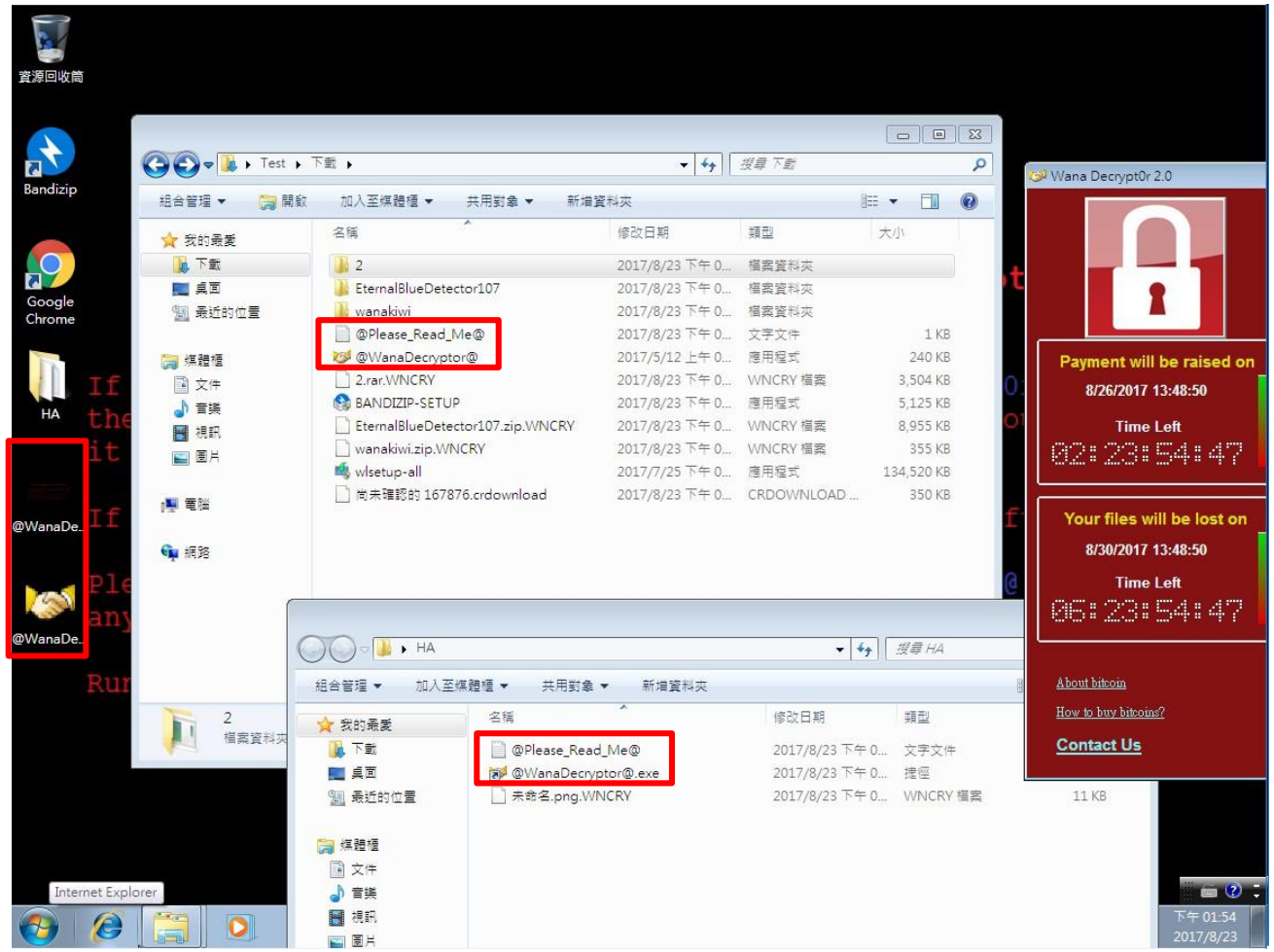
桌布被改為勒索訊息


資源回收筒
Bandizip
Google Chrome
HA
@WanaDe...
@WanaDe...
Ooops, your important files are encrypted.
If you see this text, but don't see the "Wana DecryptOr" window, then your antivirus removed the decrypt software or you deleted it from your computer.
If you need your files you have to run the decrypt software.
Please find an application file named "@WanaDecryptor@.exe" in any folder or restore from the antivirus quarantine.
Run and follow the instructions!
下午 01:51
2017/8/23

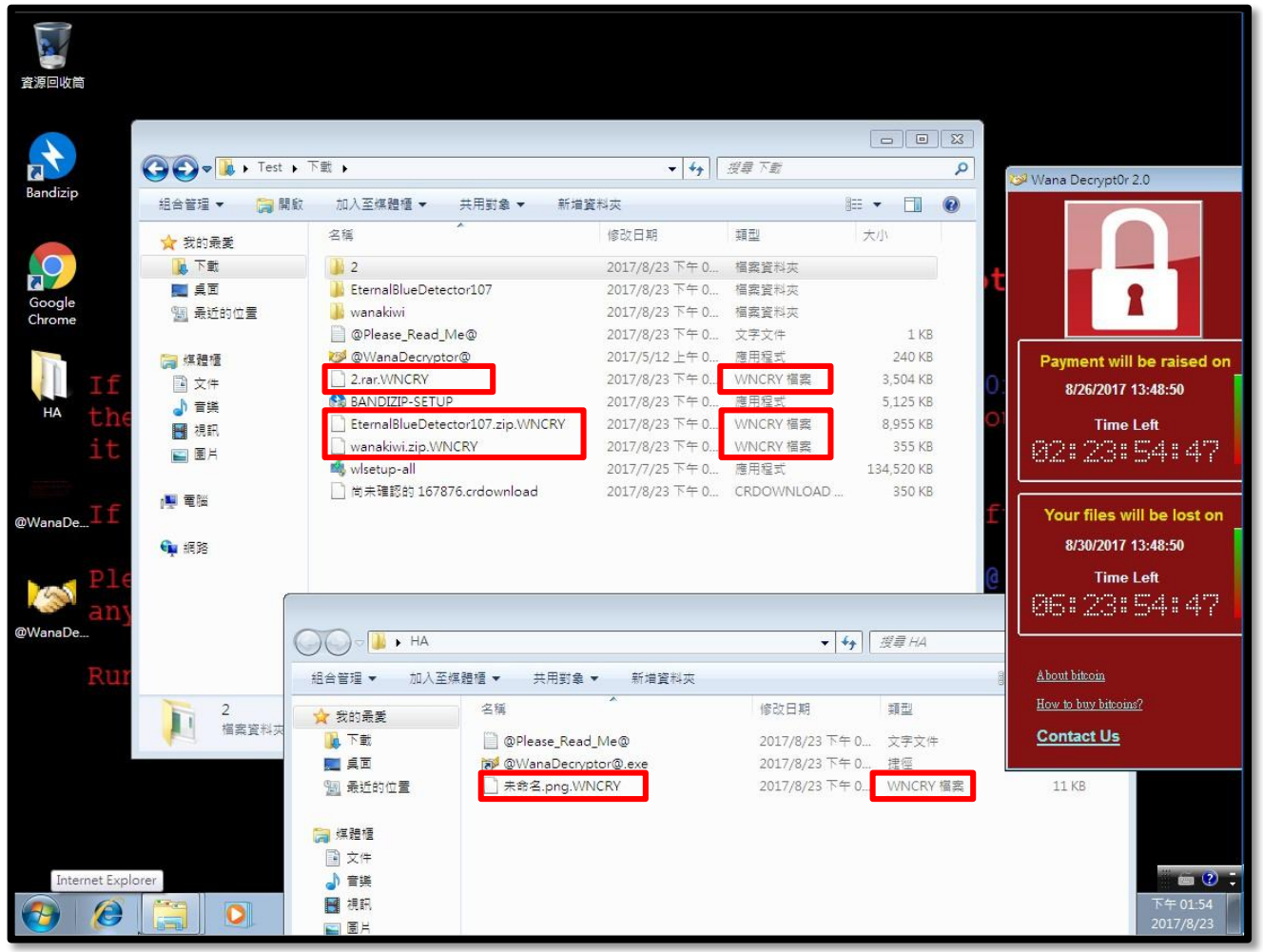
出現勒索訊息視窗


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
Chinese (traditiona
我的電腦出了什麼問題？
您的一些重要文件被我加密保存了。
照片、圖片、文檔、壓縮包、音頻、視頻文件、exe文件等，幾乎所有類型的文件都被加密了，因此不能正常打開。
這和一般文件損壞有本質上的區別。您大可在網上找找恢復文件的方法，我敢保證，沒有我們的解密服務，就算老天爺來了也不能恢復這些文檔。
有沒有恢復這些文檔的方法？
當然有可恢復的方法。只能通過我們的解密服務才能恢復。我以人格擔保，能夠提供安全有效的恢復服務。
但這是收費的，也不能無限期的推遲。
請點擊 <Decrypt> 按鈕，就可以免費恢復一些文檔。請您放心，我是絕不會騙你的。
但想要恢復全部文檔，需要付款點費用。
是否隨時都可以固定金額付款，就會恢復的嗎，當然不是，推遲付款時間越長對你不利。
最好3天之內付款費用，過了三天費用就會翻倍。
還有，一個禮拜之內未付款，將會永遠恢復不了。
對了，忘了告訴你，對半年以上沒錢付款的窮人，會有活動免費恢復，能否輪
Payment will be raised on
8/26/2017 13:48:50
Time Left
02:23:56:35
Your files will be lost on
8/30/2017 13:48:50
Time Left
06:23:56:35
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94
Copy
Check Payment
Decrypt

出現異常檔案


資源回收筒
Bandizip
Google Chrome
HA
@WanaDe..
@WanaDe..
Test ▸ 下載 ▸
組合管理 開啟 加入至媒體櫃 共用對象 新增資料夾
我的最愛
下載
桌面
最近的位置
媒體櫃
文件
音樂
視訊
圖片
電腦
網路
名稱 修改日期 類型 大小
2 2017/8/23 下午 0... 檔案資料夾
EternalBlueDetector107 2017/8/23 下午 0... 檔案資料夾
wanakiwi 2017/8/23 下午 0... 檔案資料夾
@Please_Read_Me@ 2017/8/23 下午 0... 文字文件 1 KB
@WanaDecryptor@ 2017/5/12 上午 0... 應用程式 240 KB
2.rar.WNCRY 2017/8/23 下午 0... WNCRY 檔案 3,504 KB
BANDIZIP-SETUP 2017/8/23 下午 0... 應用程式 5,125 KB
EternalBlueDetector107.zip.WNCRY 2017/8/23 下午 0... WNCRY 檔案 8,955 KB
wanakiwi.zip.WNCRY 2017/8/23 下午 0... WNCRY 檔案 355 KB
wlsetup-all 2017/7/25 下午 0... 應用程式 134,520 KB
尚未確認的 167876.crdownload 2017/8/23 下午 0... CRDOWNLOAD ... 350 KB
HA
@Please_Read_Me@ 2017/8/23 下午 0... 文字文件
@WanaDecryptor@.exe 2017/8/23 下午 0... 捷徑
未命名.png.WNCRY 2017/8/23 下午 0... WNCRY 檔案 11 KB
Wana Decrypt0r 2.0
Payment will be raised on
8/26/2017 13:48:50
Time Left
02:23:54:47
Your files will be lost on
8/30/2017 13:48:50
Time Left
05:23:54:47
About bitcoin
How to buy bitcoins?
Contact Us
Internet Explorer
下午 01:54
2017/8/23

被加密檔案出現異常副檔名



其他特徵

- 電腦出現藍色當機畫面，在電腦重新開機時顯示勒索訊息。
- 受害電腦會自動攻擊其它電腦，大量散播勒索病毒
- 即便電腦沒有連上惡意網站，只要接著網路便有遭到感染的風險

防禦方法

養成良好的電腦使用習慣

- 重要資料定期離線備份
- 定期更新作業系統及應用軟體最新修補程式
- 定期更新防毒軟體病毒碼
- 不安裝來路不明的軟體程式
- 不開啟來路不明的Email
- 不瀏覽盜版或可疑網站

萬一感染了

如果真的感染了？病毒感染後的處置方式

1. 拔除網路線，重新安裝作業系統後將安全性更新至最新版，並檢視預防處理措施是否落實。
2. 如尚未重新安裝系統，請勿將硬碟拿至別台電腦連接以防止病毒蔓延至其他電腦。
3. 嘗試使用信任來源的解密工具解密，並保存受駭主機以提供分析環境。
4. 系統重灌，讓主機回復成乾淨的原始狀態。重灌前確認受駭當時主機本身的風險與狀態，以避免重灌後因同樣漏洞再感染。

資 訊 處
Office of Information Technology

感謝閱讀