區網網管會議

臺灣大學計資中心
李美雯
mli@ntu.edu.tw
3366-5010

大 綱

- 資安案例分享
  - WannaCry勒索病毒
  - 挖礦事件處理
  - 壞兔兔勒索病毒
- 行動應用App檢測

大 綱

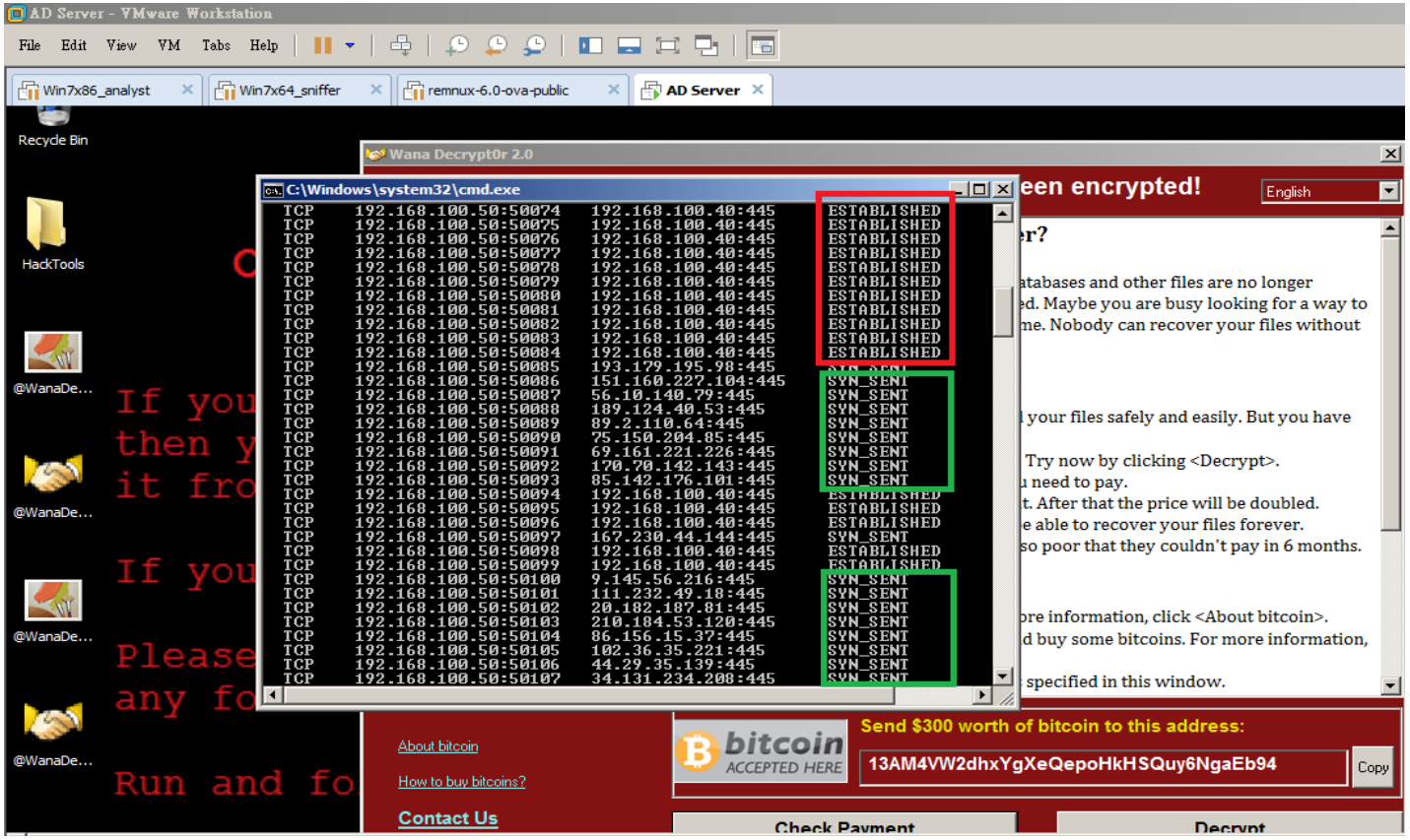
- 資安案例分享
  - WannaCry勒索病毒
  - 挖礦事件處理
  - 壞兔兔勒索病毒
- 行動應用App檢測

WannaCry勒索病毒分析

- 利用CVE-2017-0144(SMB漏洞)
- 大範圍掃描port 445，擴大感染範圍
- 執行勒索加密程式，保存加密後的檔案，刪除原始文件檔
- 跳出勒索畫面與訊息

WannaCry勒索病毒分析

內網IP優先掃描，接著亂數掃描其他IP，如下圖所示紅色框代表掃描到可以建立SMB shell的主機，綠色框則是持續發送封包試圖感染其他主機



WannaCry防範建議措施

- ✓盡快開啟Windows Update更新微軟官方釋出的系統漏洞
- ✓備份資料檔案(不須備份系統檔案)
- ✓謹慎開啟網站連結與檔案
- ✓安裝防毒軟體並維持病毒碼更新
- ✓關閉主機TCP port 445

挖礦事件處理

挖礦事件處理

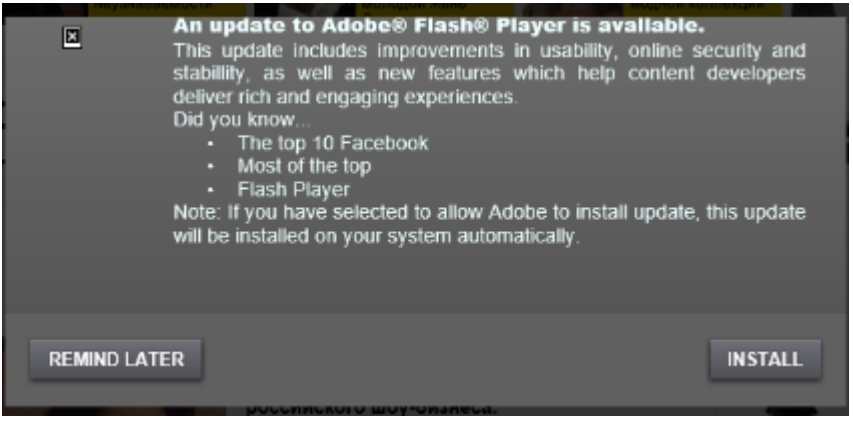
- 8月份教育通知挖擴Server list
- ASOC 建立偵測規則開立資安單

攻擊名稱	事件單狀態	事件名稱	攻擊開始時間	問題IP Addres	開單時間	所屬區網中心
主機進行惡意程式連線	通報處理完成	MALWARE-CNC Win.Trojan.Zeus variant outbound connection	08/05/2017 08:21:55 上午	[redacted]	08/07/2017 09:27:08 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 04:27:47 下午	[redacted]	08/28/2017 08:04:58 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 05:46:13 下午	[redacted]	08/28/2017 08:07:18 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 06:07:53 下午	[redacted]	08/28/2017 08:07:37 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 08:56:29 下午	[redacted]	08/28/2017 08:12:14 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 08:58:56 下午	[redacted]	08/28/2017 08:12:23 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 09:03:22 下午	[redacted]	08/28/2017 08:12:38 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 09:21:39 下午	[redacted]	08/28/2017 08:13:07 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/25/2017 10:41:40 下午	[redacted]	08/28/2017 08:16:04 上午	[redacted]
主機疑似進行挖礦程式連線	通報處理完成	Mining Server	08/26/2017 12:08:51 上午	[redacted]	08/28/2017 08:20:32 上午	[redacted]
主機進行惡意程式連線	通報處理完成	INDICATOR-COMPROMISE DNS request for known malware sinkhole domain iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com - WannaCry	08/28/2017 10:38:37 上午	[redacted]	08/28/2017 10:39:56 上午	[redacted]

挖礦事件建議措施

- ✓ 駭客變更挖礦程式名稱及行為，逃避防毒軟體偵測，使用者不易察覺
- ✓ 建議使用者更新防毒軟體或檢查工作管理員，檢視CPU效能是否正常

壞兔兔勒索病毒



- 壞兔兔 (Bad Rabbit) 勒索病毒勒索歐美企業
- 水坑式攻擊及散播
- 知名網站被駭，注入一個JavaScrip，導向一個網址
- 跳出假的Flash安裝程式
- 使用者下載惡程式後自動開始加密檔案系統

大 綱

- 資安案例分享
  - WannaCry勒索病毒
  - 挖礦事件處理
  - 壞兔兔勒索病毒
- 行動應用App檢測

行動應用App檢測

- App資安檢測作業
  - 行政院規定各機關開發之App須通過經濟部工業局訂定行動應用App之檢測項目後始得提供民眾下載使用
  - 依經濟部工業局訂定之「行動應用App基本資安檢測基準」V2.1
  - 每年12月31日前彙整其所屬機關(構)之績效及資通安全檢測報告，送交國家發展委員會進行管考

行動應用App檢測

- 教育部行動化服務調查統計表
  - App績效符合下架指標，但仍須維持上架者，須簽報單位資訊長或校長(如該校無資訊長)同意
    - 下架指標
      - 上架逾1年下載次數未達1萬次以上
      - 系統版本逾1年或內容逾3個月未更新
      - 功能或性質相同
  - 完成資安檢測時程，高級:106年12月底前，中級:107年3 月底前，初級:107年5月底前

Q & A