**TLP:WHITE**

# 應用 CVE 漏洞的
# 社交工程事件分析報告

**臺灣學術網路危機處理中心團隊(TACERT)製**

**2024 年 02 月**

# 一、事件簡介

**1.** CVE-2017-11882 漏洞（CVSS 評分：7.8）是 Microsoft Office 方程式編輯器中的 RCE 漏洞，與處理 RAM 中的物件失敗有關。要利用這個漏洞，攻擊者必需建立一個惡意檔案，然後說服受害者打開它，通常是透過電子郵件或被入侵的網站發送。

**2.** 成功利用漏洞後，會導致方程式編輯器（EQNEDT32.EXE）處理程序發生了記憶體中斷的現象，使得攻擊者能透過處理程序挖空手法，擁有打開惡意檔案的使用者的權限去執行任意代碼。如果使用者持有管理員權限，攻擊者更可以完全控制系統，包括安裝程式、檢視、修改或破壞資料，甚至是建立新帳戶。

**3.** CVE-2017-11882 漏洞自 2017 年被揭露後，在 2018 年成為 Microsoft Office 最經常被利用的安全漏洞。它陸續被駭客應用至今，而這期間駭客利用該漏洞進行的攻擊手法變化萬千。整理近幾年與該漏洞有關的資安事件(如下)，發現該漏洞利用可以散播間諜軟體或竊密軟體感染受害主機，進而竊取憑證與個人資料。

(1)2017/12/10 惡意 RTF 檔案利用漏洞 CVE-2017-11882 來散播間諜軟體 Loki。

(2)2022/5/23 駭客以電子郵件寄送一個 PDF 文件，於文件中嵌入惡意的 Word 檔案，並開採微軟的 Office 漏洞 CVE-2017-11882，以於受害者系統上安裝鍵盤側錄工具 Snake Keylogger。

(3)2023/09/07 惡意程式 Agent Tesla 透過 5 年前 Office 漏洞:CVE-2017-11882、CVE-2018-0802 發動攻擊。

(4)2023/12/21 駭客利用 CVE-2017-11882 作為網路釣魚活動的一部分來散播 Agent Tesla。

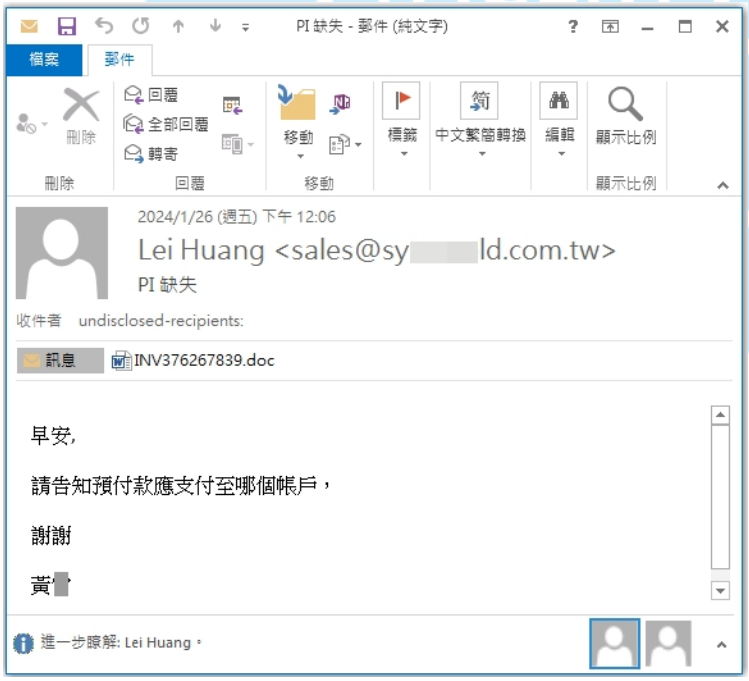
**4.** 在 2024 年 1 月底，TACERT 服務信箱陸續收到兩封含有附件而且主旨類似的信件，為了解兩封信對於收件者的危害程度，故對信件進行檢測。

(1) 信件 1 – 寄件者:Lei Huang ，主旨:PI 缺失，於 2024/01/26 下午 12:22 收到。

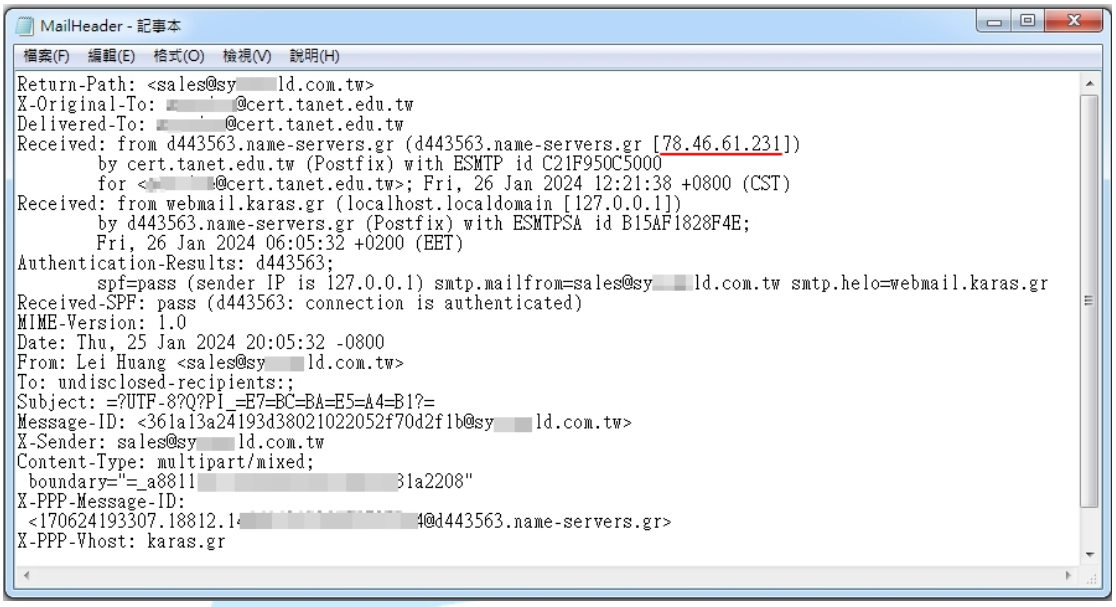
(2) 信件 2 – 寄件者:Ricky Chiou， 主旨:新 PI，於 2024/01/31 下午 1:32 收到。


## 二、 事件檢測

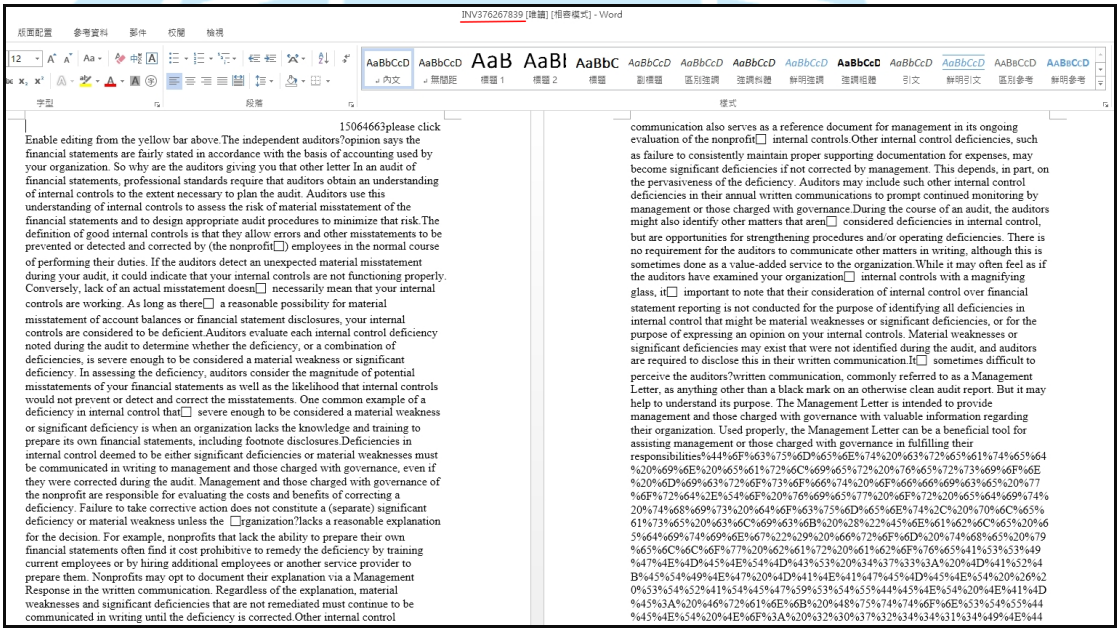
**1.** 打開信件 1 後，發現寄件者 Lei Huang 偽裝成臺灣某模具製造公司的銷售部門寄出信件。由收件者 undisclosed-recipients 可知道信件 1 以密件副本寄出，收件者無法知道該信件還寄給哪些人。檢視信件 1 的郵件內容以繁體中文撰寫，內容為一般銷售過程中客戶詢問付款帳戶的資訊，收件者若為公司業務人員將不會覺得有異常。

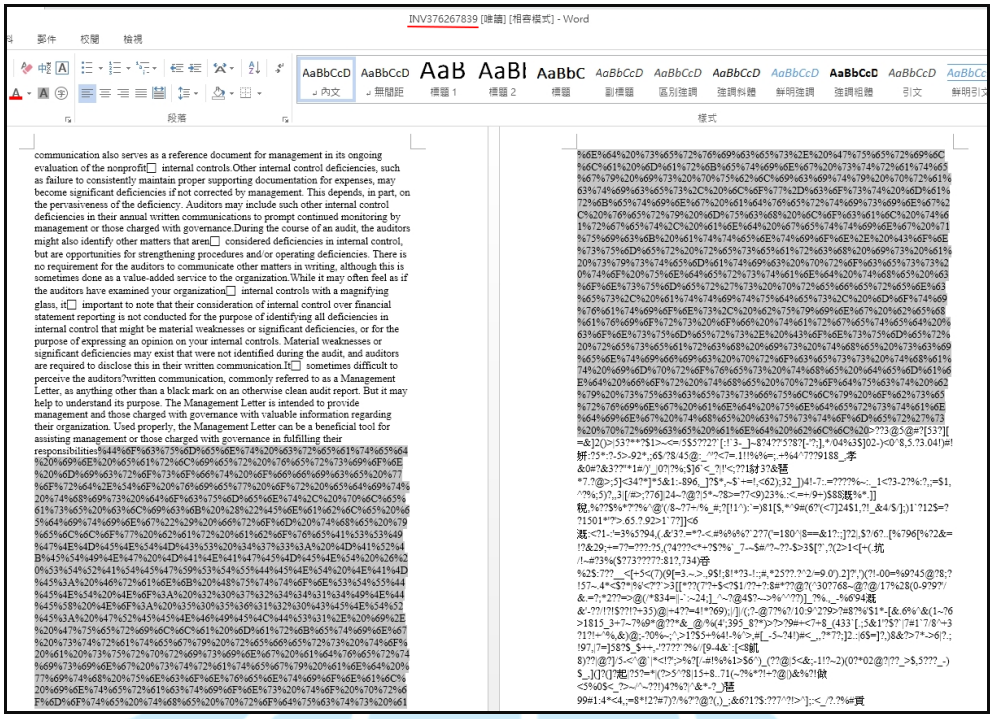



**2.** 檢視信件 1 的 Mail Header ，發現該信件從德國 IP:78.46.61.231 伺服器寄出。




**3.** 打開附件 INV376267839.doc (MD5:95E1D42FACA462FEB431AD62F2BF1C3D)，發現內容有 10 頁。除了英文文章外，還有兩段不同類型的亂碼。






4. 檢視主機對外網路連線，發現 EQNEDT32.EXE 在打開信件附件後對外連線美國 IP: 104.21.21.189 之 443port。

| | | | | |
|---|---|---|---|---|
| 2024/2/15 上午 11:22:31 | Added | EQNEDT32.EXE | TCP 192.168.137.131:1130 | 104.21.21.189:443 |
| 2024/2/15 上午 11:22:31 | Added | EQNEDT32.EXE | UDP 127.0.0.1:51012 | *:* |
| 2024/2/15 上午 11:22:51 | Removed | EQNEDT32.EXE | TCP 192.168.137.131:1130 | 104.21.21.189:443 |
| 2024/2/15 上午 11:22:51 | Removed | EQNEDT32.EXE | UDP 127.0.0.1:51012 | *:* |

5. 檢視主機背景程式的運作，發現 EQNEDT32.EXE 為方程式編輯器，這是微軟 Office 用來在文件中插入或編輯 OLE 物件的工具。

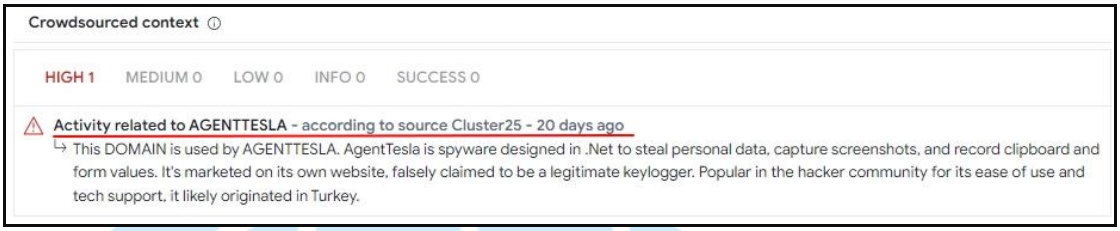
| Process | Description | Command | Company |
|---|---|---|---|
| EQNEDT32.EXE (1188) | Microsoft Equation Editor | "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding | Design Science, Inc. |

6. 檢視主機連線美國 IP:104.21.21.189 之封包，得知美國 IP 所對應的主機網址為「amassmodel.top」，而傳輸內容因為加密呈現亂碼。

(1) 該美國 IP 經 Virustotal 檢測為 0/90。

(2) 網址「amassmodel.top」經 Virustotal 檢測為 20/92，為惡意網址。


(3) 此網址在 2024 年 1 月底被用來散播 AgentTesla。



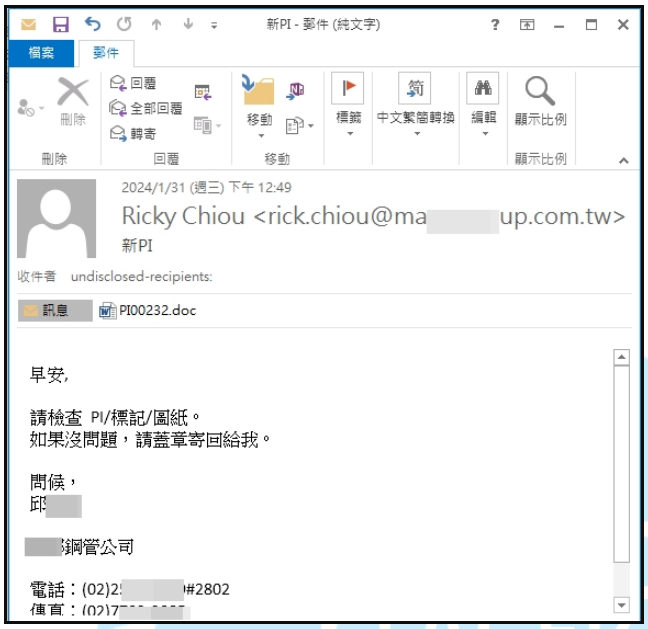

**7.** 信件 1 附件 INV376267839.doc 經 Virustotal 檢測，其惡意比例為 34/59。防毒軟體公司判定該附件與三個微軟 office 漏洞利用有關(如下表)，這三個漏洞是由於物件在記憶體中的處理方式，導致 Microsoft Office 的方程式編輯器存在遠端程式碼執行漏洞，也稱為「Microsoft Office 記憶體損壞漏洞」。

| 漏洞編號 | 防毒軟體以漏洞編號命名之數量 |
|---|---|
| CVE-2017-11882 | 4 |
| CVE-2018-0798 | 3 |
| CVE-2018-0802 | 3 |

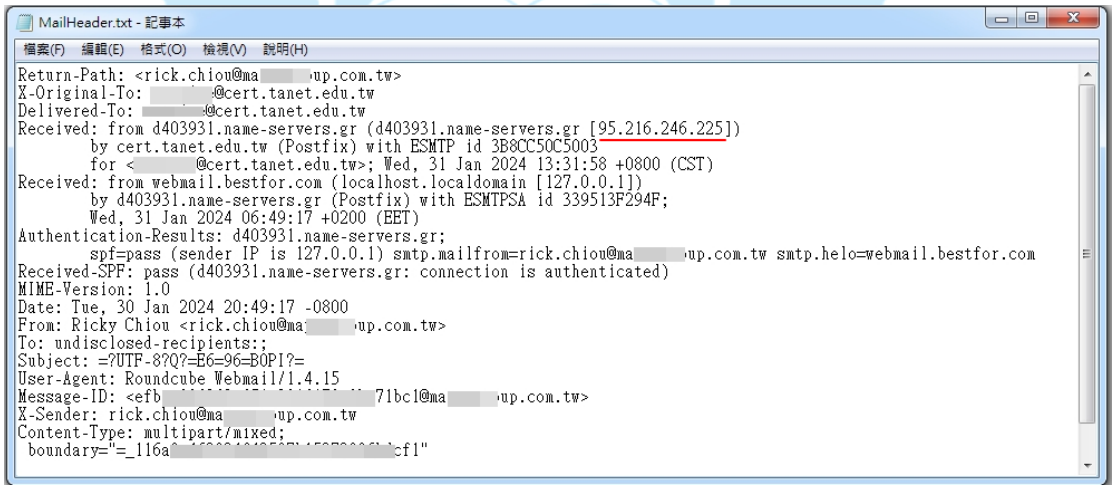
其中有 4 家防毒軟體判定其利用 CVE-2017-11882 漏洞，並以該漏洞編號命名此附件的惡意軟體名稱。


**8.** 打開信件 2 後，發現寄件者 Ricky Chiou 偽裝成臺灣某鋼管公司的聯絡信箱代表人員寄出信件，而其於信件中所告知的聯絡資訊與該公司該位人員相同。

由收件者 undisclosed-recipients 可知道信件 2 以密件副本寄出，收件者無法知道該信件還寄給哪些人。檢視信件 2 的郵件內容以繁體中文撰寫，內容為與客戶確認產品規格的資訊，收件者若為負責處理採購業務的人員將不會覺得有異常。




**9.** 檢視信件 2 的 Mail Header ，發現該信件從芬蘭 IP:95.216.246.225 伺服器寄出。該芬蘭 IP 在 AbuseIPdb 上被檢舉 4 次，而被濫用的可信度為 18%。其最近一次被檢舉是在 2024/02/01 因為網路釣魚與垃圾郵件被舉報。



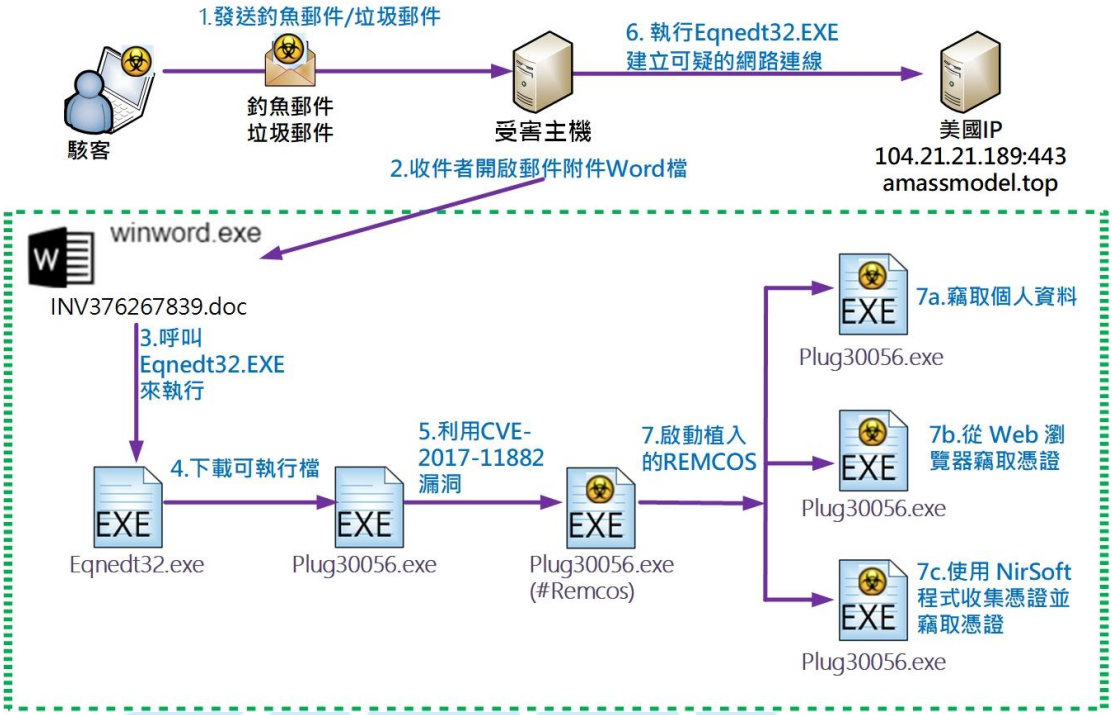

**10.** 彙整信件 1 與信件 2 的檢測結果如下表，發現其攻擊手法相似。

| 項目 | 信件 1 | 信件 2 |
|---|---|---|
| 寄件者郵件 | 德國 IP:78.46.61.231 | 芬蘭 IP:95.216.246.225 |

| 項目 | 信件 1 | 信件 2 |
|---|---|---|
| 伺服器 IP | | (在 AbuseIPdb 被舉報為惡意 IP) |
| 信件附件 | INV376267839.doc<br>(1)Virustotal:34/59<br>(2)漏洞利用:<br>CVE-2017-11882、<br>CVE-2018-0798、<br>CVE-2018-0802 | PI00232.doc (內容與信件 1 附件相似)<br>(1)Virustotal:37/60<br>(2)漏洞利用:CVE-2017-11882、CVE-2018-0798、CVE-2018-0802 |
| 啟動的程式 | Eqnedt32.exe | Eqnedt32.exe (方程式編輯器) |
| 對外連線 IP | 美國 IP:104.21.21.189:443，<br>(1)其對應網址為「amassmodel.top」。<br>(2)該網址經 Virustotal 檢測為 20/92，為惡意網址。<br>(3)此網址在 2024/1 月底被用來散播 AgentTesla。 | 美國 IP:172.67.183.155:443<br>(1)在 AbuseIPdb 被舉報為惡意 IP，最近一次被檢舉是在 2023/11/01 因為暴力攻擊被舉報。<br>(2)該 IP 經 Virustotal 檢測為惡意 IP，而且為 Lokibot 的 C2 server。<br>(3)其對應網址為「blueyonderllc.top」。<br>(4)該網址經 Virustotal 檢測為 21/92，為惡意網址。<br>(5)此網址在 2024/2/1 被用來散播 AgentTesla。 |
| 下載的檔案 | plug30056.exe | Plugman39506.exe |

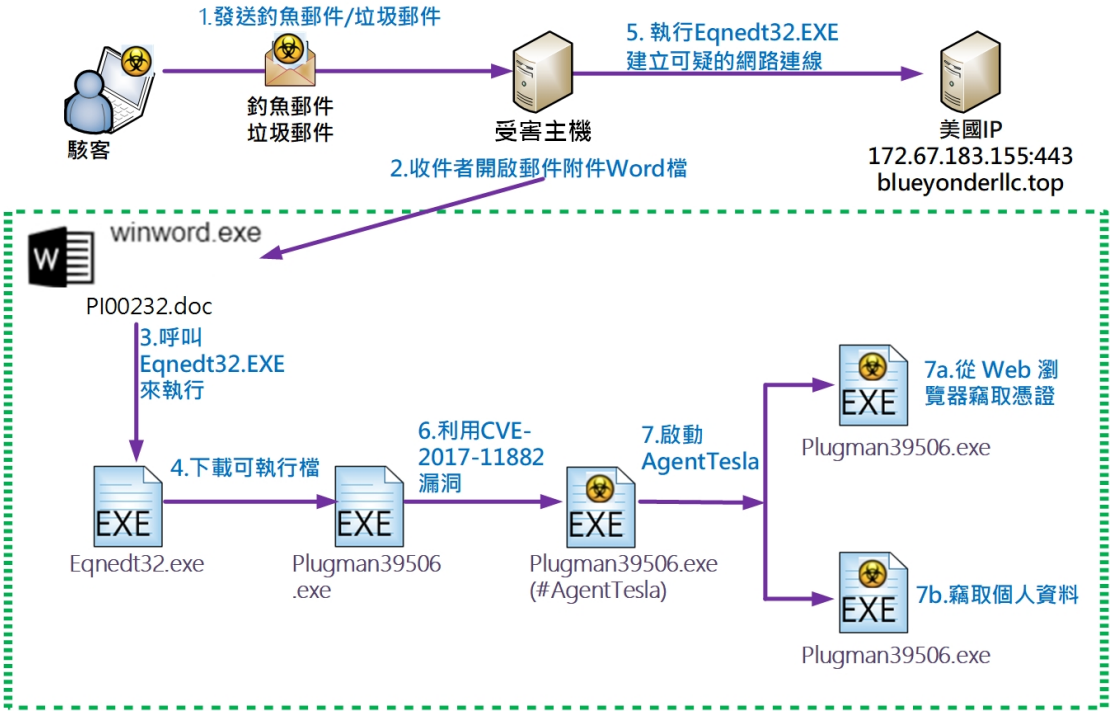
## 三、 事件攻擊行為

**1.** 信件 1 附件 INV376267839.doc 經檢測後發現其攻擊行為如下圖所示。首先，在附件被開啟後會呼叫 EQNEDT32.EXE 來執行。接著在它執行後下載可執行檔。在 EQNEDT32.EXE 啟動後開始 CVE-2017-11882 的漏洞利用，並且建立可疑的網路連線。當下載回來的可執行檔 plug30056.exe 執行後，啟動植入的 REMCOS(遠端存取木馬程式)。最後，竊取個人資料、從 Web 瀏覽器竊取憑證與使用 NirSoft 程式收集憑證並竊取憑證。




**2.** 信件 2 附件 PI00232.doc 經檢測後發現其攻擊行為如下圖所示。

首先，在附件被開啟後會呼叫 EQNEDT32.EXE 來執行。在它執行後下載可執行檔。之後 EQNEDT32.EXE 建立可疑的網路連線，並在它啟動後開始 CVE-2017-11882 的漏洞利用。當下載回來的可執行檔 plugman39506.exe 執行後啟動 AgentTesla。最後，從 Web 瀏覽器竊取憑證與竊取主機內個人資料。



## 四、 總結與建議

1. 經檢測兩封信件後發現該類信件之攻擊行為相同。攻擊者偽裝成台灣公司的人員寄出信件給收件者，當收件者收信並開啟惡意附件的 Word 檔後，將會觸發 CVE-2017-11882 的漏洞利用。接著會執行竊密軟體，如 Agent Tesla，進而且竊取個人資料與憑證。
2. 在可能影響方面，本案的兩封信件內容很真實，容易引誘收件者開啟附件 Word 檔，造成個人資料與憑證被竊， 侵害了隱私權，因此對 CIA 中的機密性造成衝擊。
3. 關於此類攻擊的處理方式，可先使用防毒軟體對受害主機進行掃描，並移除惡意程式，也可使用微軟 Process Explorer 工具來檢視背景程式中是否有惡意程式執行。
4. 對於此類案件的預防方式有下列兩點:
   (1) 由於本案的郵件攻擊手法是透過社交工程來散播惡意郵件，建議收件者勿隨意開啟不明來源之附件。
   (2) 因該類攻擊利用 CVE-2017-11882 等系列相關的 office 漏洞，建議使用者定期更新 Office 軟體 ，以避免遭受漏洞利用的攻擊。

## 參考資料

1. **CVE-2017-11882: five years of exploitation**
   https://www.kaspersky.com/blog/cve-2017-11882-exploitation-on-the-rise/48768/
2. **惡意程式 Agent Tesla 透過 5 年前 Office 漏洞發動攻擊**
   https://www.ithome.com.tw/news/158641
3. **17 年的微軟 Office 漏洞（CVE-2017-11882）,仍繼續搞破壞**
   https://blog.trendmicro.com.tw/?p=53726

**4. 研究人員警告小心夾帶惡意 Word 檔的 PDF**

https://www.ithome.com.tw/news/151069

**5. PHISHING ATTACKS USE AN OLD MICROSOFT OFFICE FLAW TO SPREAD AGENT TESLA MALWARE**

https://securityaffairs.com/156246/cyber-crime/agent-tesla-phishing-cve-2017-11882.html#google_vignette