假冒寄件者回信之網路釣魚攻擊事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2019 年 11 月

一、事件簡介

1. 本中心在 2019/9/27 收到來自 hsxx99@edu.tw 寄件者的回信，信件主旨為「RE:(事件單編號:AISAC-1XXX97)(1 級)事件單結案通知信」，內容以一段英文撰寫，並且包含一個下載連結與 2019/7/17 某事件單結案通知信內容。

2019/9/27 (週五) 上午 12:23
hs[redacted]99@edu.tw
RE: (事件單編號:AISAC-1[redacted]97)(1級)事件單結案通知信
收件者 service

We need this reviewed, categorized and filed as soon as possible. Take a look and let me know how soon can you finish it.

ATTACHMENT DOCUMENT

Thank you

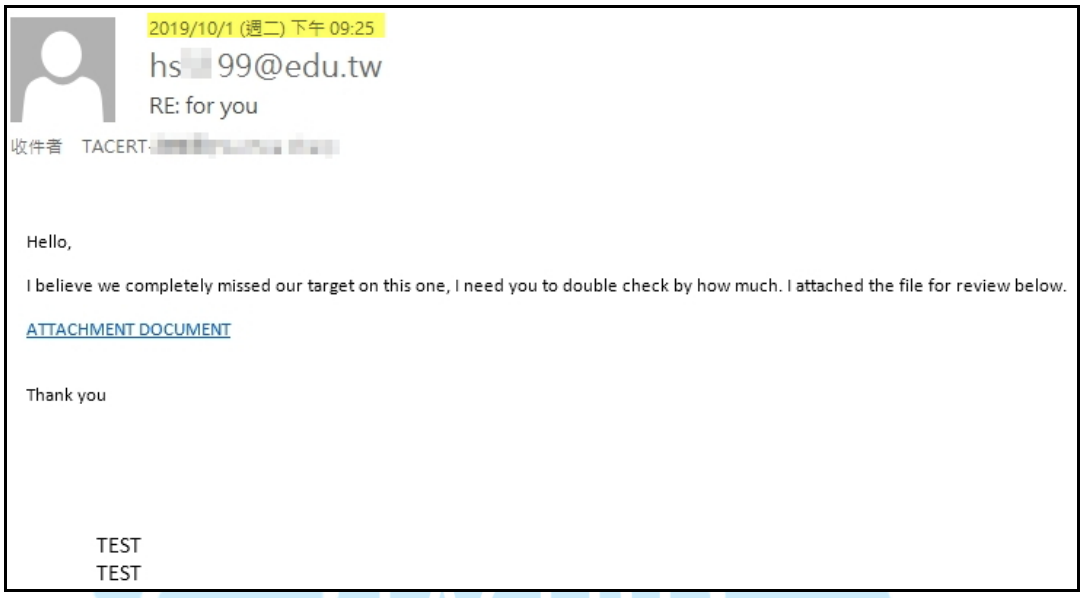
您好
此為教育機構資安通報平台所寄發之通知信，旨在確認TACERT資安團隊已完成事件通報審核流程。

通報時間:	2019-07-17 19:18:53
事件單編號:	AISAC-1[redacted]97
通報機關名稱:	[redacted]國民小學
主管機關	[redacted]網路中心
影響等級:	1級
事件分類:	INT
事件說明:	資訊設備疑似遭受弱點攻擊
資安通報小組通報審核結果	通過
資安通報小組通報審核意見	

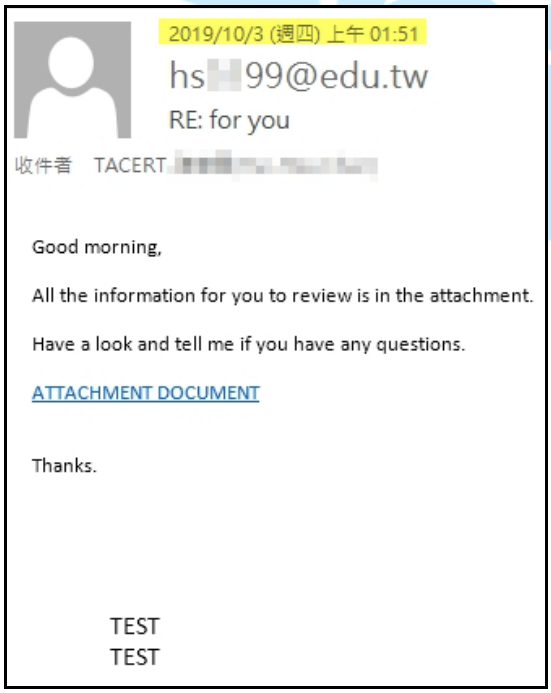
2. 使用 hsxx99@edu.tw 於網路上搜尋，發現某國小的公務信箱 hsxx99@mail.edu.tw 與此類似，也發現 hsxx99@mail.edu.tw 信箱來自教育部校園雲端電子郵件系統(https://mail.edu.tw)，而且本中心所收到來自 hsxx99@edu.tw 寄件者的事件單結案通知信也是該國小的資安事件單。
3. 為檢測 hsxx99@mail.edu.tw 信箱是否有 Auto Reply 功能，本中心在 2019/09/27 上午 11:09 以信件主旨:for you 寄測試信至 hsxx99@mail.edu.tw 信箱，測試後確定該信箱並無自動回信功能，而信箱所有者告知有收到測試信，並且未發

現信箱有異常。

4. 在 2019/10/1 下午 09:25 本中心寄測試信的信箱收到來自 hsxx99@edu.tw 寄件者的回信，而信件主旨為 RE: for you，信件內容為一段英文(含下載連結)與測試信內容。



5. 在 2019/10/3 上午 1:51 本中心寄測試信的信箱再次收到來自 hsxx99@edu.tw 寄件者的回信，信件主旨仍然為 RE: for you，而信件內容為一段新的英文(含下載連結)與測試信內容。



6. 在 2019/10/03 同一天有另一個教網中心也收到來自 hsxx99@edu.tw 信箱的回信，而且信件時間為上午 1:58，與 2019/10/03 上午 1:51 信件主旨 RE: for you 的信寄信時間接近。

寄件者：<hs[redacted]99@edu.tw>
Date: 2019 年 10 月 3 日 週四 上午 1:58
Subject: RE: Fwd: 163.[redacted].196，的 mac
To: 教網中心[redacted] <[redacted]@[redacted].edu.tw>

Hello,

Please see attached and confirm.
Let me know if you have any questions.

ATTACHMENT DOCUMENT

Thank you,

[redacted]老師好：
[redacted]上午貴校由 IP 163.[redacted].196 所發資安事件 MAC 如件，請參閱

7. 依照收到回信的時間，整理整個事件發生的時間順序如下圖。為了解這些可疑郵件的攻擊行為與對收信者的危害程度，本中心對四封來信進行檢測。

二、事件檢測

1. 首先，使用微軟的 Message Header Analyzer 分析第一封 2019/9/27 來信的網際網路標題，從 Received headers 內容發現該信由 atl4mhob11.registeredsite.com(美國 IP:209.17.115.49)所寄出，非來自寄件者所在地台灣(.tw)，表示寄件者名稱 hsxx99@edu.tw 是偽造的。

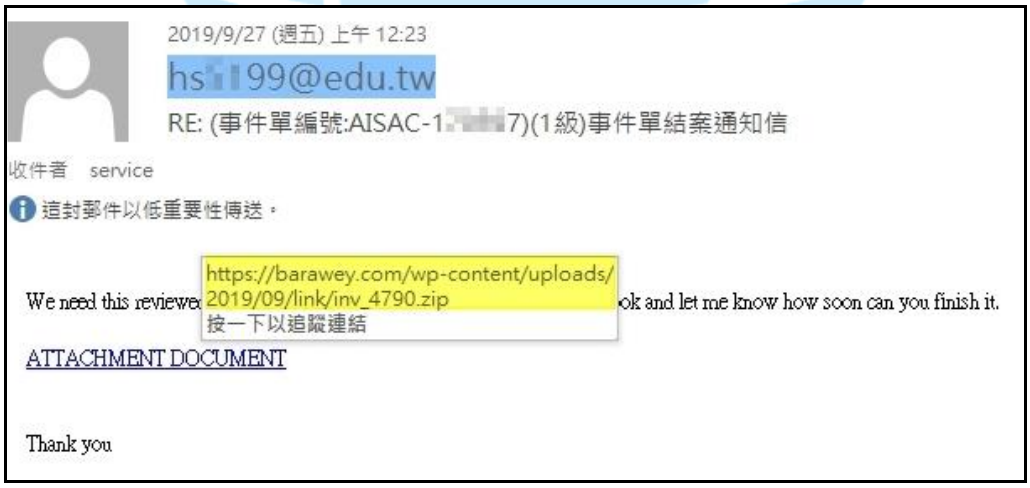
Summary

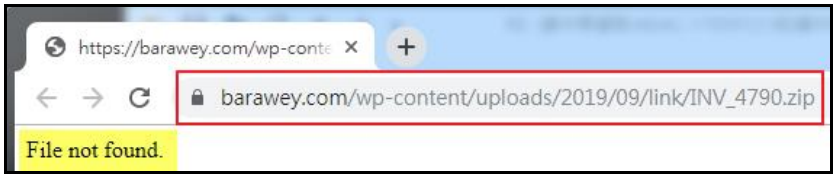
Subject	RE:_(事件單編號:AISAC-1 7)(1級)事件單結案通知信
Message Id	<a7cb05cd-d1ff-41e0-8579-5cad656269e8@local>
Creation time	2019/9/27 上午12:23:08 (Delivered after -17 minutes 49 seconds)
From	hs 99@edu.tw
To	service <service@cert.tanet.edu.tw>

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1	unknown (HELO localhost) (janet@conceptlabs.us@24.217.29.219)	0	2019/9/27 上午12:25:09		ESMTPA
2		uid 0)	2019/9/27 上午12:25:10	1 second	
3	mailpod.hostingplatform.com (atl4qobmail01pod1.registeredsite.com [10.30.71.113])	atl4mhob11.registeredsite.com (8.14.4/8.14.4)	2019/9/27 上午12:25:10	0 seconds	ESMTP
4	atl4mhob11.registeredsite.com (atl4mhob11.registeredsite.com [209.17.115.49])	cert.tanet.edu.tw (Postfix)	2019/9/27 上午12:07:20	-17 minutes 50 seconds	ESMTP

2. 查看信件內容發現一個連結 ATTACHMENT DOCUMENT，點擊後會開啟網址 https://barawey.com/wp-content/uploads/2019/09/link/inv_4790.zip，但是檔案找不到。





3. 檢視第二封 2019/10/1 來信的網際網路標題，從 Received headers 內容發現該信由 qproxy2.mail.unifiedlayer.com (美國 IP:69.89.16.161) 所寄出，非來自寄件者所在地台灣(tw)，表示寄件者名稱 hsxx99@edu.tw 是偽造的。

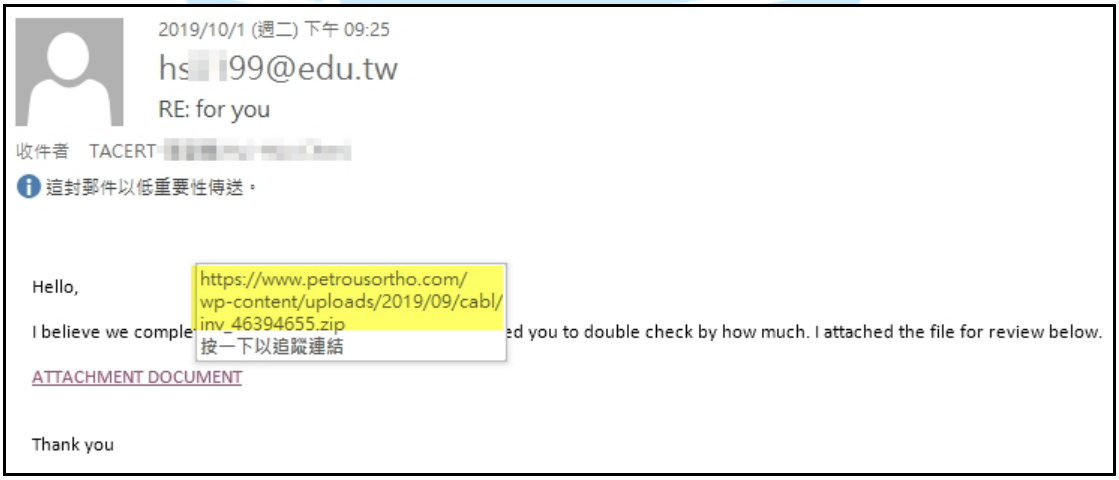
Summary

Subject	RE: for you
Message Id	<6f217f6a-5808-47ce-83f6-473f6ed1ee01@local>
Creation time	2019/10/1 下午9:24:49 (Delivered after -17 minutes 54 seconds)
From	hs[redacted]99@edu.tw
To	TACERT-[redacted] <[redacted]@cert.tanet.edu.tw>

Received headers

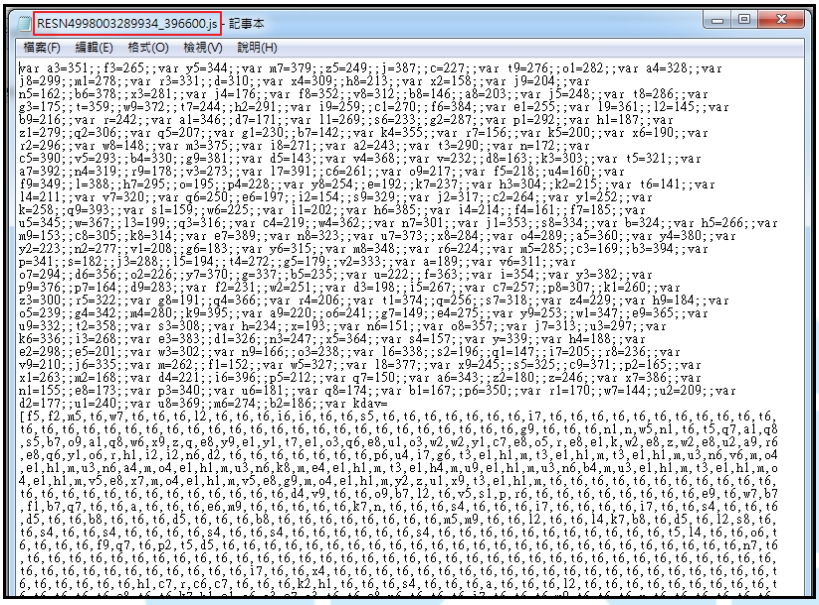
Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1	host-2te.network.hiqip.net ([192.199.222.66]:36103 helo=localhost)	host279.hostmonster.com	2019/10/1 下午 9:26:16		esmtpsa (TLSv1.2:ECDHE-RSA-AES256-GCM-SHA384:256) (Exim 4.92) (envelope-from <hs[redacted]99@edu.tw>)
2	host279.hostmonster.com ([74.220.215.79])	cmsmtp	2019/10/1 下午 9:26:16	0 seconds	ESMTP
3	cmgw15.unifiedlayer.com (unknown [10.9.0.15])	qproxy2.mail.unifiedlayer.com (Postfix)	2019/10/1 下午 9:26:16	0 seconds	ESMTP
4	qproxy2.mail.unifiedlayer.com (qproxy2-pub.mail.unifiedlayer.com [69.89.16.161])	cert.tanet.edu.tw (Postfix)	2019/10/1 下午 9:08:22	-17 minutes 54 seconds	ESMTP

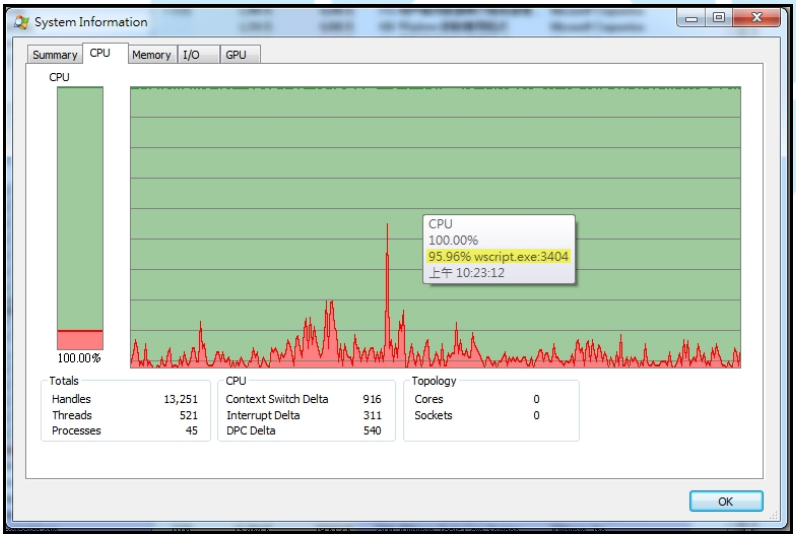
4. 由第二封 2019/10/1 來信的內容，發現與第一封來信相同，存在一個連結 ATTACHMENT DOCUMENT ，點擊該連結會開啟網址 https://www.petrousorth.com/wp-content/uploads/2019/09/cabl/inv_46394655.zip 。



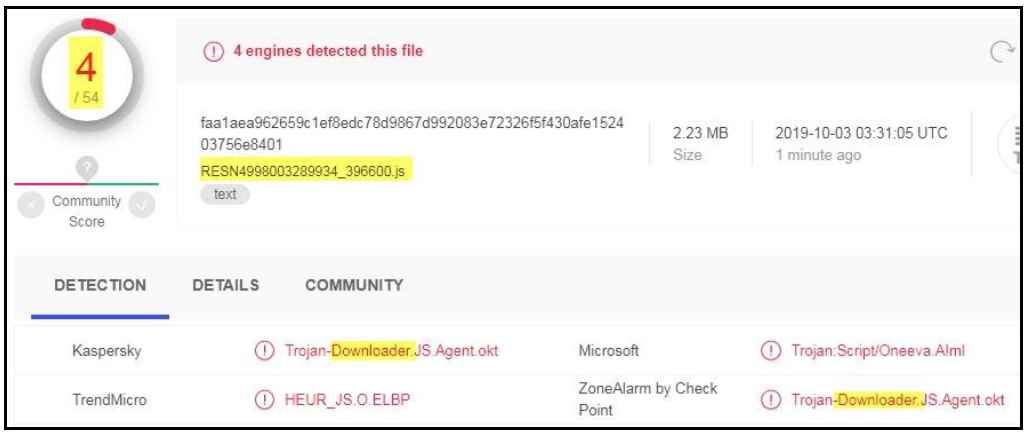
接著會下載一個檔名為 RESN4998003289934_396600 的 zip 壓縮檔，解壓縮後會看到一個檔名為 RESN4998003289934_396600.js 的 Jscript 指令檔。

以記事本開啟 RESN4998003289934_396600.js 後會看到一堆變數設定，而當此檔案被讀取時，程式 wscript.exe 的執行會使 CPU 使用率高達 100%。

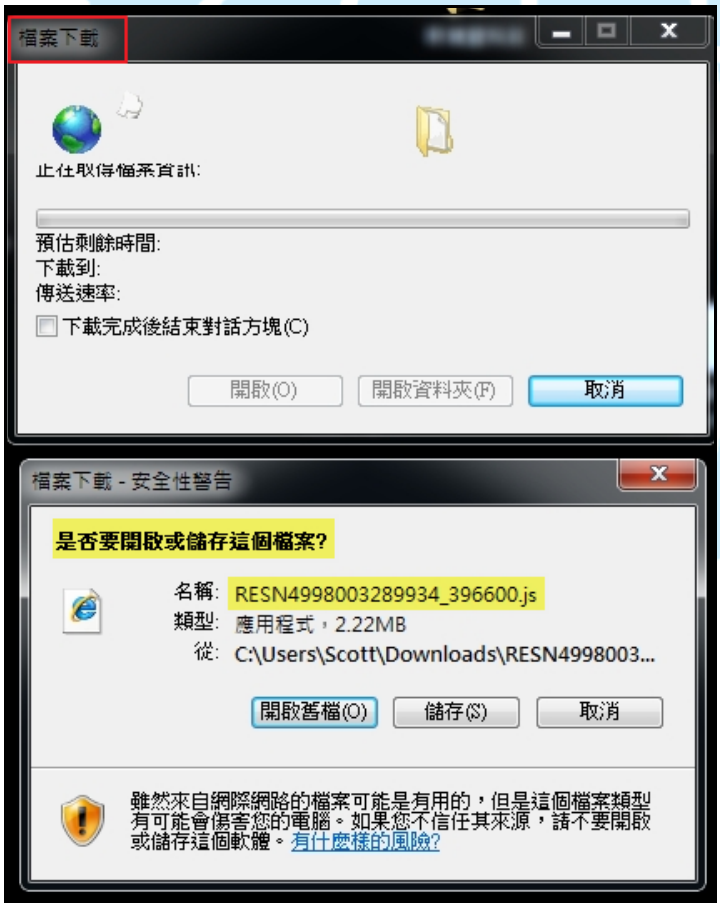




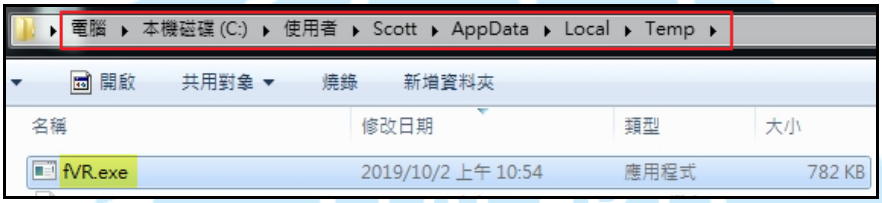
5. RESN4998003289934_396600.js 經 Virustotal 檢測，其惡意比例為 4/54，僅有少數防毒軟體可以識別它的存在，而且它被防毒軟體公司視為一個 Downloader(下載器)。

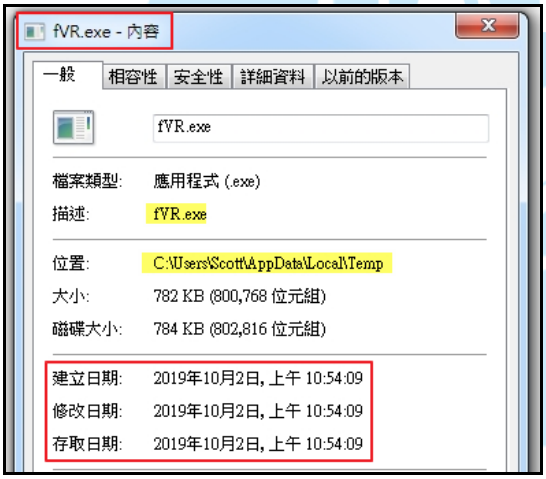


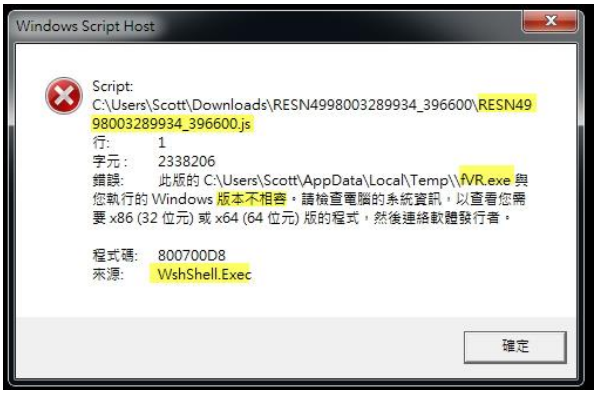
6. 以 IE 開啟 RESN4998003289934_396600.js 後會出現檔案下載的視窗，隨後出現詢問是否要開啟或下載 RESN4998003289934_396600.js 的視窗，若選擇開啟舊檔，則會出現「fVR.exe 與 Windows 64 位元版本不相容，無法啟動或執行」的視窗。



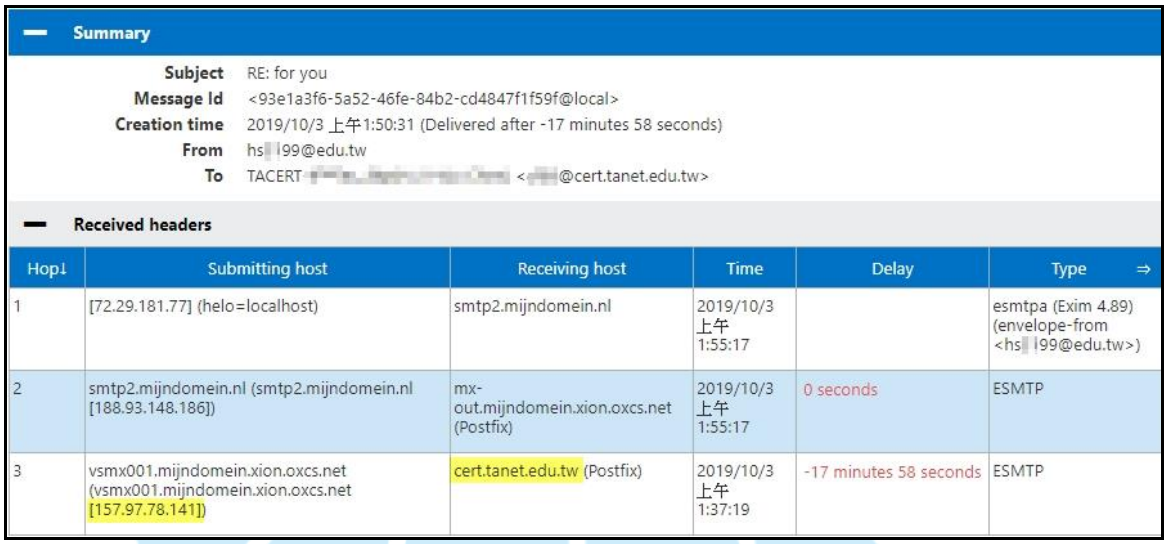
7. 在 C:\使用者\...\AppData\Local\Temp 資料夾內，發現 fVR.exe，它經 virustotal 檢測，其惡意比例為 0。從隨後出現的 Windows Script Host 視窗內容，得知 RESN4998003289934_396600.js 的 Script 內容有錯誤發生，因 fVR.exe 與 Windows 64 位元版本不相容，因此可以判定 fVR.exe 為執行 RESN4998003289934_396600.js 後所產生。







8. 檢視第三封 2019/10/3 來信的網際網路標題，從 Received headers 內容發現該信由 vsmx001.mijndomein.xion.oxcs.net(德國 IP:157.97.78.141) 所寄出，非來自寄件者所在地台灣(tw)，表示寄件者名稱 hsxx99@edu.tw 是偽造的。



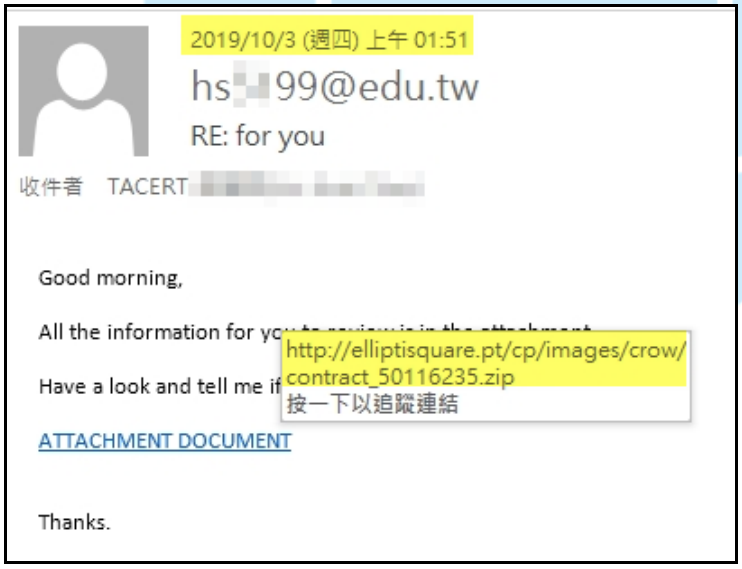
Summary

Subject	RE: for you
Message Id	<93e1a3f6-5a52-46fe-84b2-cd4847f1f59f@local>
Creation time	2019/10/3 上午1:50:31 (Delivered after -17 minutes 58 seconds)
From	hs[illegible]99@edu.tw
To	TACERT [illegible] <[illegible]@cert.tanet.edu.tw>

Received headers

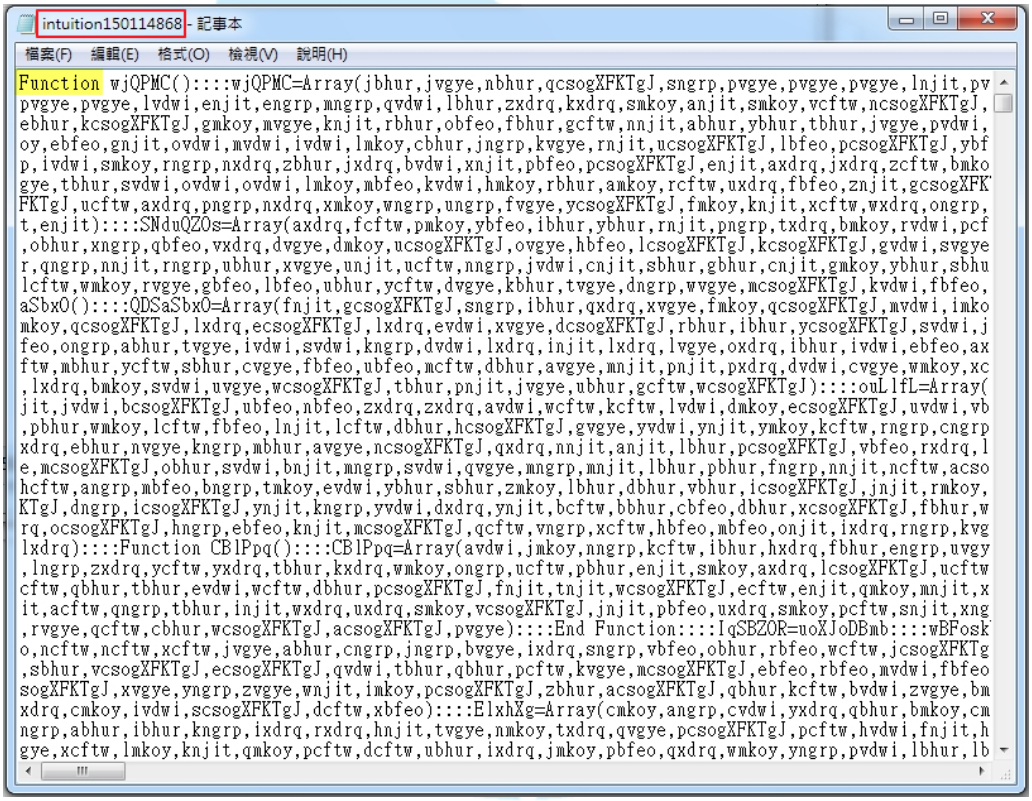
Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1	[72.29.181.77] (helo=localhost)	smtp2.mijndomein.nl	2019/10/3 上午 1:55:17		esmtpa (Exim 4.89) (envelope-from <hs[illegible]99@edu.tw>)
2	smtp2.mijndomein.nl (smtp2.mijndomein.nl [188.93.148.186])	mx-out.mijndomein.xion.oxcs.net (Postfix)	2019/10/3 上午 1:55:17	0 seconds	ESMTP
3	vsmx001.mijndomein.xion.oxcs.net (vsmx001.mijndomein.xion.oxcs.net [157.97.78.141])	cert.tanet.edu.tw (Postfix)	2019/10/3 上午 1:37:19	-17 minutes 58 seconds	ESMTP

9. 查看第三封 2019/10/3 來信的內容，發現與前兩封來信相同，存在一個連結 ATTACHMENT DOCUMENT ，點擊該連結會開啟網址 http://elliptisquare.pt/cp/images/crow/contract_50116235.zip。

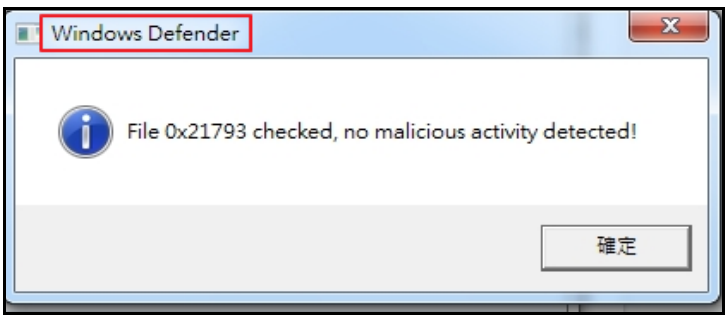


10. 接著會下載一個檔名為 intuition150114868 的 zip 壓縮檔，解壓縮後會看到一個檔名為 intuition150114868 的 VBscript 指令檔，而且該檔案是在第三封信寄出的前一天 2019/10/2 下午 10:35 被修改完成。

11. 編輯 intuition150114868.vbs 的內容，會看到一堆 Function wjQPMC 的變數設定。

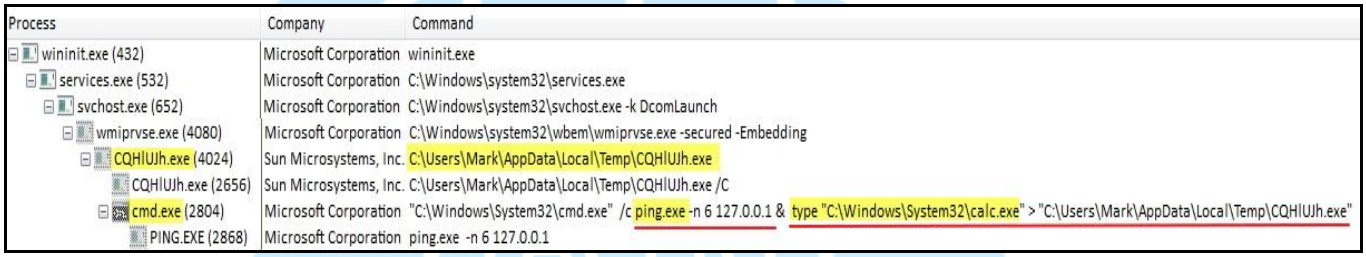


直接執行 intuition150114868.vbs 會出現 Windows Defender 所給的提醒視窗，提到檢查檔案 0x21793，沒有偵測到惡意行為。

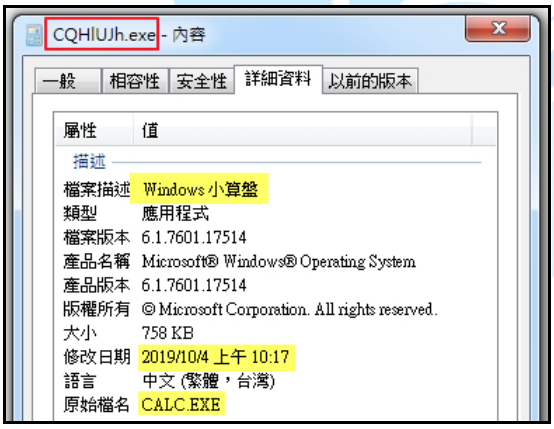


點擊「確定」後，出現另一個來自 MS Excel 的視窗，提到 reogXFKTgJest 不能被執行，請稍後再試(0x21793)。

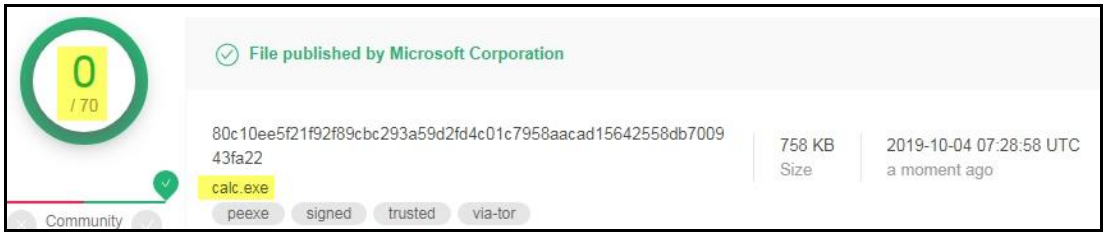
12.檢視主機背景程式運作情形，發現 C:\Users\...\AppData\Local\Temp 資料夾內有一個 CQHIUJh.exe 正在執行，而且此檔案會呼叫 cmd.exe 來執行 Ping.exe 檢查主機的網卡與用 calc.exe 替換原舊有的 CQHIUJh.exe。



檢視 CQHIUJh.exe 的內容，發現該檔案在執行當下時間被修改成一個 Windows 小算盤。



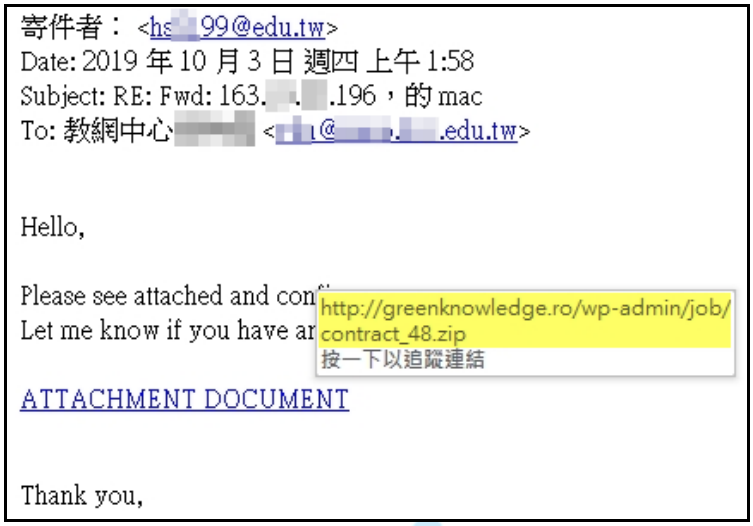
13.CALC.EXE 與 CQHIUJh.exe 經 Virustotal 檢測，其惡意比例為 0/70。



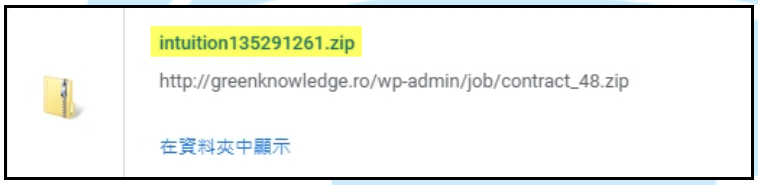
intuition150114868.vbs 經 Virustotal 檢測，其惡意比例為 3/55，僅少數防毒軟體公司能識別該檔案之惡意行為。

14. 在執行 intuition150114868.vbs 之後，最後會開啟小算盤，該小算盤不會產生惡意行為，推測此作法可能是駭客在測試如何將惡意程式透過郵件散播到主機內。

15. 查看 2019/10/3 教網中心所收到來信的內容，發現與前面三封來信相同，存在一個連結 ATTACHMENT DOCUMENT ，點擊該連結會開啟網址 http://greenknowledge.ro/wp-admin/job/contract_48.zip。

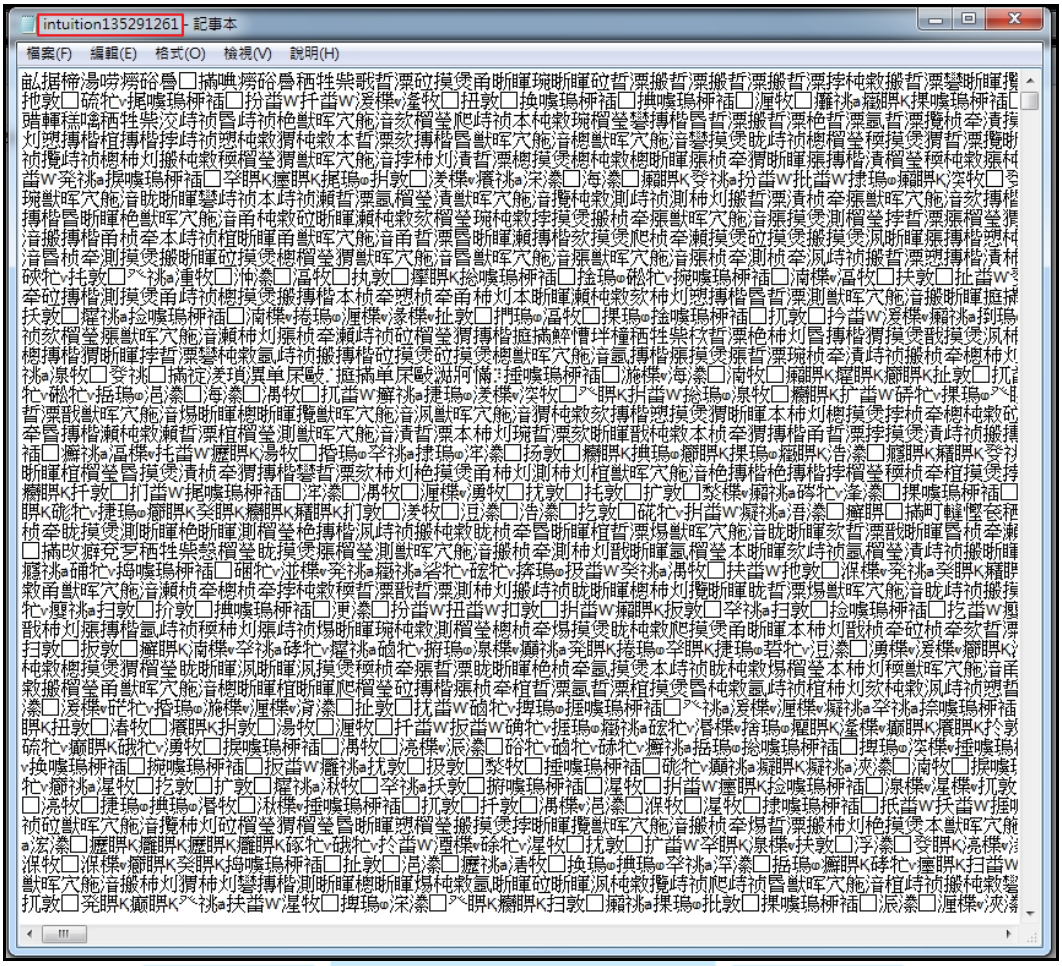


接著會下載一個檔名為 intuition135291261 的 zip 壓縮檔，解壓縮後會看到一個檔名為 intuition135291261 的 VBscript 指令檔，而且該檔案是在該封信寄出的前一天 2019/10/2 下午 10:35 被修改完成，與第三封信下載的 intuition150114868.vbs 的檔案修改時間相同。

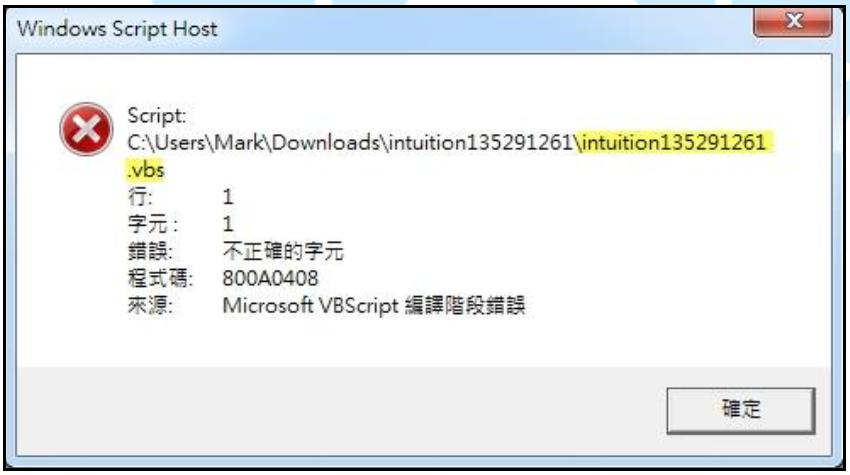


16. intuition135291261.vbs 經 Virustotal 檢測，其惡意比例為 2/55，僅少數防毒軟體公司能識別該檔案之惡意行為。

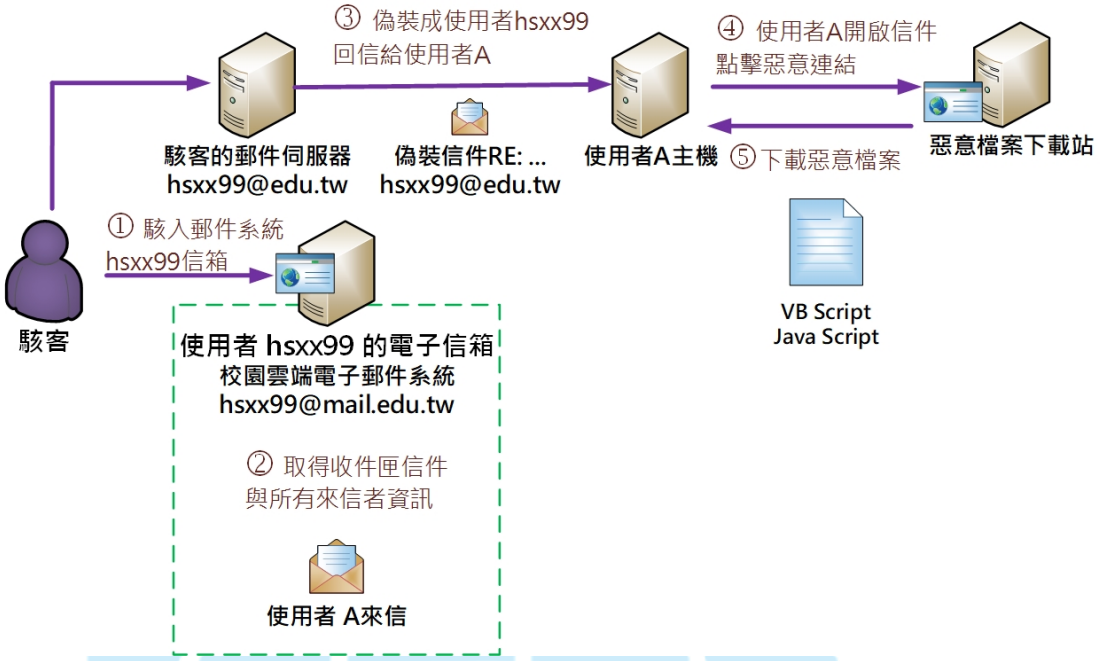
17.編輯 intuition135291261.vbs 的內容，會看到一堆亂數排列的中文。



18.當執行 intuition135291261.vbs 一段時間後，會出現 Script 錯誤的視窗訊息。



三、事件攻擊行為示意圖



1.駭客駭入校園雲端電子郵件系統的 hsxx99 信箱。

2.駭客取得使用者 hsxx99 信箱內收件匣信件與所有來信者資訊。

3.依照收件匣信件內容偽裝成使用者 hsxx99 回信給使用者 A。

4.使用者 A 開啟回信後點擊惡意連結 ATTACHMENT DOCUMENT。

5.透過惡意連結引導使用者 A 下載惡意檔案至使用者 A 主機內。

四、總結與建議

1. 經信箱所有者與信箱管理單位確認公務信箱 hsxx99@mail.edu.tw 的狀態，得知該信箱曾有來自國外 IP 的異常存取紀錄，確認該信箱有被駭現象。
2. 從駭客的攻擊行為得知，本案非一般的隨機釣魚攻擊事件，駭客在取得受駭信箱內所有信件後，以回信方式對所有來信者進行釣魚攻擊，想透過這些人曾經寫過的信件內文來誘騙收到釣魚信的收件者。
3. 從第 2~4 封信件所附連結 ATTACHMENT DOCUMENT 下載至主機的 Java

Script 檔與 VB Script 檔執行情形，推測駭客可能在測試如何將惡意程式透過郵件散播到主機內。

4. 針對本類型的釣魚攻擊事件，有下列預防措施提供使用者參考。

(1) 不隨意開啟不明來源的信件(/附件檔)或點擊不明來源的夾帶連結。

(2) 定期更換電子郵件信箱的登入密碼，並加強密碼強度。

(3) 若收到可疑的信件內容，建議親自與寄件者確認信件內容的正確性。

(4) 定期進行防毒軟體的病毒碼更新，確保主機能第一時間阻擋病毒攻擊。

(5) 定期進行電子郵件信箱的重要信件備份。

(6) 定期進行電腦主機資料備份。