

教育機構 ANA 通報平台

發佈編號	TACERT-ANA-2024121711121717	發佈時間	2024-12-18 09:30:17
事故類型	ANA-攻擊預警	發現時間	2024-12-17 11:10:17
影響等級	低		

[主旨說明:]【攻擊預警】社交工程攻擊通告：請加強防範以業務需求或時事議題為由，以及偽冒資安院之社交工程郵件攻擊！

[內容說明:]

轉發 國家資安資訊分享與分析中心 NISAC-400-202412-00000036

資安院近期發現，攻擊者利用業務需求、時事議題、資安攻擊預警或偽冒資安院名義，發動社交工程郵件攻擊，誘導收件者開啟與執行惡意附檔，並記錄開信人員之帳號資訊。建議加強防範與通知各單位提高警覺，注意檢視寄件者與內容正確性，資安院不會使用商用信箱發送通知，更不會於電子郵件中要求執行任何軟體，請各單位提高警覺，如感覺有異請先洽資安院查證，並請避免勿點擊信件連結與執行附檔，以免受駭。

已知攻擊郵件特徵如下，相關受駭偵測指標請參考附件。

1.偽冒寄件者帳號：「A23031@nics.nat.gov.tw」

2.已知遭駭客利用寄件者帳號：

「russell.wei@msa.hinet.net」、

「aimer.chai@msa.hinet.net」、

「chtda@ms72.hinet.net」、
「student.book@msa.hinet.net」、
「nannies@ms22.hinet.net」、
「tmdcu.ken@msa.hinet.net」、
「khcity-rc26416@umail.hinet.net」、
「y7133@ms48.hinet.net」、
「victor.chiou22@msa.hinet.net」、
「hong.each@msa.hinet.net」、
「harvest.rotary@msa.hinet.net」、
「im.imwork@msa.hinet.net」

3.駭客寄送之主旨：

「**【攻擊預警】** 近期勒索軟體活動頻繁，請提高警覺」、
「陳情書」、
「**【求助】** 護照出現異常！」、
「需求幫助：當地官員表示護照或個人資料有異常」、
「有黑料，大爆料」、
「《新川普時代的台灣》，思路的不錯，邀君一覽」、
「閣下鈞閱《台灣自救運動宣言》」、
「《新川普時代的台灣》，邀君一覽」、
「閣下鈞閱《台灣獨立建國請願書》」、
「關於“新北割頸案”十大訴求。」、
「項目投標」

4.惡意附檔名稱：

「trojan_killer.rar」、
「1028.rar」、
「20241030.rar」、
「投標標案資料.rar」、
「Proof_documents.rar」、
「台在新川普時代的思考.rar」、
「wufi.org.tw.rar」、
「護照.doc」、
「1121.html」、
「陳情書.doc」

5.惡意中繼站:

165[.]154[.]227[.]52
165[.]154[.]226[.]163
ssl[.]hinets[.]tw
www[.]team-microsoft[.]top
www[.]smb-microsoft[.]top

6.惡意附檔 SHA1 雜湊值：

c5e85ecf68ff99d069740826c0cce7cb016df756 、
610406c73cdedc33835649d54da6889b7abeb275 、
a06e4246c0085c843f8b010257e77dffdb018969 、
4da9af68626fefaa65bfb6d47874cd6602140e20 、

c255c31f11d1269429949313124594bc91523e6d 、
6438cf9f1def6cbcc225f14e5442655cfd7aae2 、
a06e4246c0085c843f8b010257e77dffdb018969 、
0f94659d1d715ffc122128a098349221ab634b00

註：相關網域名稱為避免誤點觸發連線，故以「[.]」區隔。

情資分享等級: **WHITE**(情資內容為可公開揭露之資訊)

此訊息僅發送到「區縣市網路中心」，煩請貴單位協助公告或轉發

[影響平台:]

N/A

[建議措施:]

- 1.網路管理人員請參考受駭偵測指標，確實更新防火牆，阻擋惡意中繼站。
- 2.建議留意可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔。
- 3.安裝防毒軟體並更新至最新病毒碼，開啟檔案前使用防毒軟體掃描郵件附檔，並確認附檔檔案類型，若發現檔案名稱中存在異常字元(如 exe.pdf, exe.doc, pdf.zip, lnk, rcs, exe, moc 等可執行檔案附檔名的逆排序)，請提高警覺。
- 4.加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。

[參考資料:]

附件-社交工程攻擊_IOC : https://cert.tanet.edu.tw/pdf/soc_ioc_1216.csv