近期惡意程式範例探討

劉得民 Te-Min, Liu (劉得明 Diamond Liu)
dmliu99999@gmail.com
中華民國網路封包分析協會 理事長
大映科技 Huge Diamond Network Service CEO

大綱

01 惡意程式的基本認識

02 Python型態的惡意程式

03 PDF型態的惡意程式

04 SVG, LNK, VHD 型態的惡意程式

05 問題與答覆 Q&A

惡意程式的近期發展與範例

常見

- 惡意程式類型: EXE, DLL, SCR
- 惡意程式類型: VBS, VBE, PS1

罕見

- 惡意程式類型: **LNK**, BAT, CMD
- 惡意程式類型: MSI, SYS, DRV

難防

- 惡意程式類型: **PDF**, VHD+LNK
- 惡意程式類型: **SVG**, MP4, PYC

Google github byob

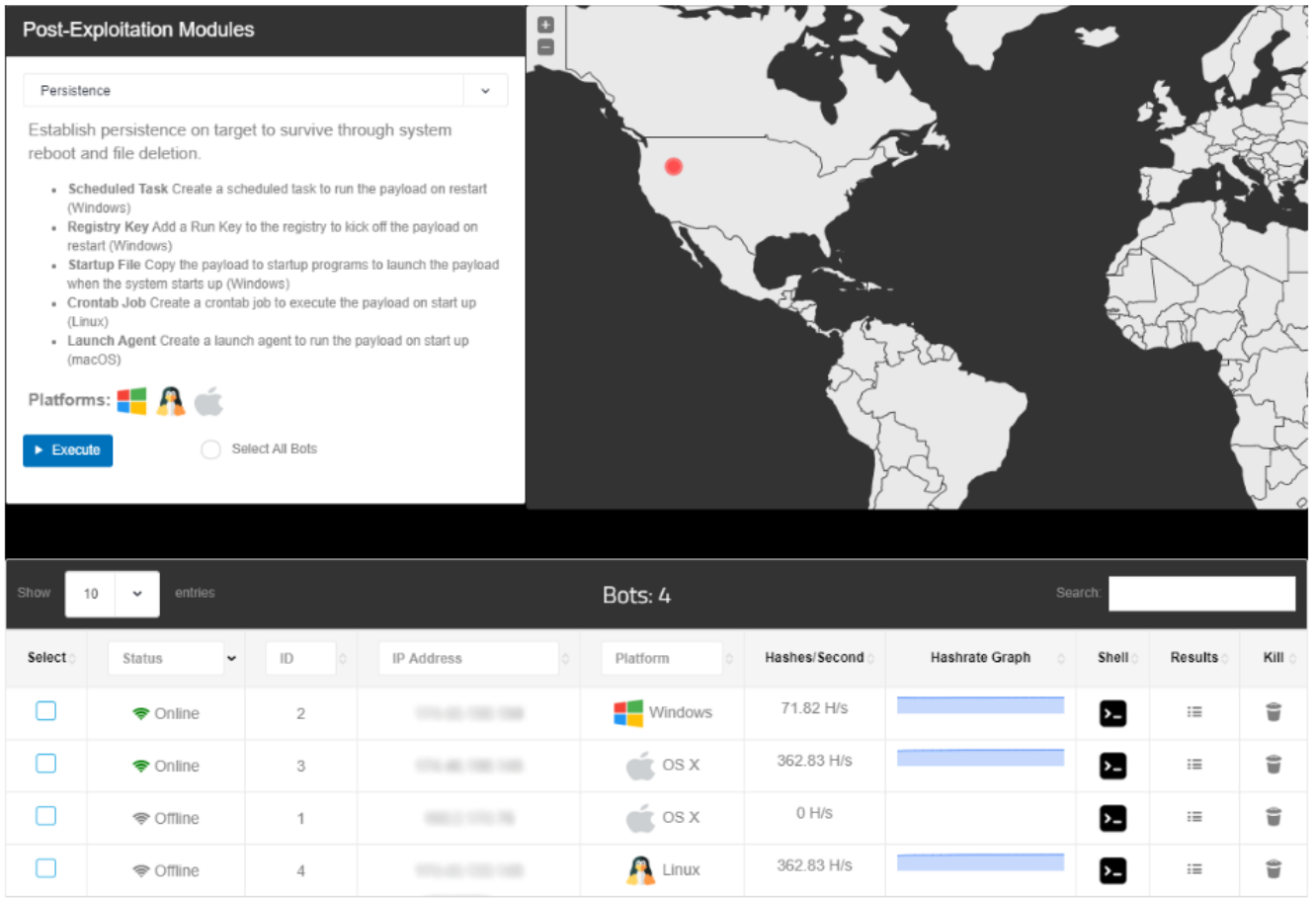
AI 模式 全部 圖片 影片 新聞 購物 短片 更多 工具

GitHub
https://github.com › malwaredllc › byob · 翻譯這個網頁

malwaredllc/byob: An open-source post-exploitati

BYOB is an open-source post-exploitation framework for students, rese
includes features such as: Command & control server with ...

A control panel for your C2 server with a point-and-click interface for executing post-exploitation modules. The control panel includes an interactive map of client machines and a dashboard which allows efficient, intuitive administration of client machines.



Python 的惡意程式範例特性

1. py檔案與pyc檔案
2. 需要安裝 python 環境
3. iOS 預設安裝 python
4. 從PyPI進行攻擊(Python模組的供應鏈)


Google
惡意程式 SVG
AI 模式
全部
圖片
影片
新聞
購物
短片
更多
工具
OPSWAT
https://traditional-chinese.opswat.com › blog › weaponiz...
武器化的SVG：攻擊者如何利用圖片散播惡意軟體
2025年5月8日 — 武器化的SVG 檔案會嵌入JavaScript 來繞過電子郵件安全性並傳送惡意軟體。瞭解攻擊者如何利用SVG 以及如何偵測這些威脅。
iThome
https://www.ithome.com.tw › news
向量圖檔SVG被駭客用於偷渡惡意軟體QBot、臉書貼文 ...
2022年12月16日 — 駭客利用PNG、JPG、GIF等圖片檔案挾帶惡意軟體的手法，不時有事故傳出，但現在有研究人員發現，駭客開始運用SVG格式的向量圖片檔案做為媒介。
Facebook · Technews 科技新報
超過 20 個回應 · 4 個月前
JavaScript 重新導向攻擊超危險！惡意程式透過SVG 圖片檔 ...
JavaScript 重新導向攻擊超危險！惡意程式透過SVG 圖片檔注入合法網頁，強制瀏覽器導向惡意網站，讓你成為釣魚詐騙、間諜軟體受害者。

Authenticate

e authenticated.

MALWA

from ABUSE.ch | SPAMH

About Login

Using the form belov

ily.

Browse Da

file_type:pdf

Search

已儲存資訊

file_type:pdf

file_type:svg

file_type:lnk

tag:Specter

md5:eb9e4955ed

tag:Sweet

Date

DL

2025

2025-10-21 16:05

WT

2025-10-20 09:12

2025-10-07 11:57

Google

惡意程式 PDF

AI 模式 全部 圖片 影片 購物 新聞 短片 更多 工具

Adobe

https://www.adobe.com › 首頁 › Adobe Acrobat

PDF 是否有機會挾帶病毒？確保檔案安全

惡意程式碼則經常用來對機器造成損害。 病毒、木馬程式和惡意程式碼可透過許多方式隱身在PDF 中，且經常出沒於電子郵件下載內容或附件內(...

零壹科技Zero One Tech.

https://www.zerone.com.tw › opswat › news › bulletin

76%的惡意軟體都透過PDF檔案傳播！五招教你辨別 ...

2025年1月6日 — 76%的惡意軟體都透過PDF檔案傳播！五招教你辨別惡意PDF檔案 · 1.自動運行的腳本. PDF 中嵌入的JavaScript 允許攻擊者註入在開啟檔案時執行的惡意程式碼。 · 2 ...

恆逸教育訓練中心

https://www.uuu.com.tw › Public › content › article

PDF檔案之資安鑑識調查

2024年10月7日 — PDF是一種最常用的共享文件形式。攻擊者可以在PDF檔案中隱藏惡意腳本，當使用者嘗試開啟該檔案時，這些腳本就會被執行。此類惡意腳本可以輕鬆規避系統與 ...

12
/ 70

Community Score

DETECTION DETAILS

Security vendors' analysis

Avast

Cyren

K7AntiVirus

Kaspersky

McAfee-GW-Edition

SecureAge

Acronis (Static ML)

EXE

adw]

anDropper.Agent....

08

B!ml

A (PUA)

Google

惡意程式 VHD

AI 模式 全部 圖片 影片 新聞 購物 短片 更多 工具

網管人
https://www.netadmin.com.tw › ... › 市場新知 › 產業脈動

惡意郵件偽裝手法翻新壓縮夾帶虛擬硬碟.vhd檔

2025年6月23日 — vhd檔 ... 透過電子郵件夾帶惡意附件，並利用該漏洞，即可繞過Windows系統的MotW（Mark of the Web）安全機制，受害者可能受騙而在電腦上執行外來惡意程式，最終 ...

iThome
https://www.ithome.com.tw › news

卡巴斯基：VHD勒索軟體出自北韓駭客集團Lazarus之手

2020年7月29日 — 資安業者卡巴斯基（Kaspersky）本周揭露了被用來執行目標式攻擊的VHD勒索軟體，分析後發現該勒索軟體應是出自北韓駭客集團Lazarus之手，而且與勒索軟體 ...

明志科技大學
https://lis.mcut.edu.tw › ...

【資安公告】微軟發布3月份例行更新（Patch Tuesday），修補7 ...

2025年3月13日 — 避免開啟來路不明的VHD、MSC、Access 檔案，以降低惡意程式碼執行風險。 強化系統存取控管，減少駭客透過實體接觸或社交工程手法發動攻擊的機會。 應 ...

?

Community Score

12 security vendors and no sandboxes flagged this file as malicious

feb019239e9e9a77cf4a958897cec89ba154bd471f7981d56868d233dad8a197

1dfb213cb60883047e082c8411f1af96.virus

peexe overlay

1.08 MB
Size

2023-01-10 18:25:11 UTC
11 minutes ago

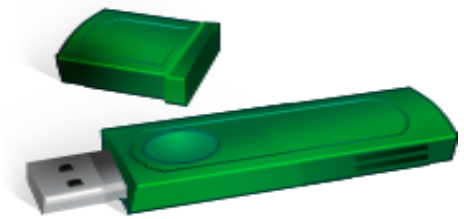
EXE

DETECTION DETAILS BEHAVIOR COMMUNITY

Security vendors' analysis

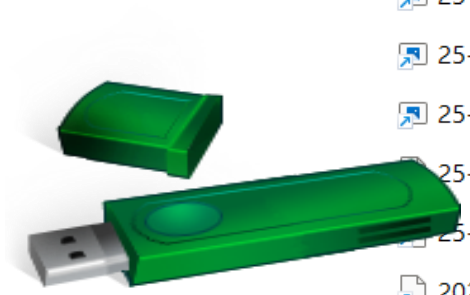
Avast	Win32:AdwareX-gen [Adw]	AVG	Win32:AdwareX-gen [Adw]
Cyren	W32/Trojan.FXKG-0991	ESET-NOD32	A Variant Of Win32/TrojanDropper.Agent....
K7AntiVirus	Trojan (005722f11)	K7GW	Trojan (005722f11)
Kaspersky	UDS:Trojan.Win32.Injuke	McAfee	Artemis!1DFB213CB608
McAfee-GW-Edition	BehavesLike.Win32.Dropper.tc	Microsoft	Trojan:Win32/Wacatac.B!ml
SecureAge	Malicious	Sophos	Generic Reputation PUA (PUA)
Acronis (Static ML)	Undetected	AhnLab-V3	Undetected

名稱	修改日期	類型	大小	建立日期	屬性
1500信託所得電子申報作業說明.pdf	2025/2/23 下午 05:05	Microsoft Edge PDF Docume...	1,026 KB	2025/2/23 下午 05:10	N
1140103講座證書-劉得民老師.pdf	2025/1/6 下午 07:10	Microsoft Edge PDF Docume...	197 KB	2025/1/6 下午 07:11	N
App靜動態解析與測試_教材版.pdf	2024/9/30 上午 11:05	Microsoft Edge PDF Docume...	28,867 KB	2025/6/25 下午 03:24	N
App靜動態解析與測試_教材版_黑白.pdf	2024/10/16 下午 12:29	Microsoft Edge PDF Docume...	6,784 KB	2025/6/25 下午 03:24	N
CBROPS教材檔案.pdf	2024/11/28 下午 06:27	Microsoft Edge PDF Docume...	95,975 KB	2025/6/25 下午 03:24	N
Cobalt-ATM-En.pdf	2016/11/25 下午 07:37	Microsoft Edge PDF Docume...	2,551 KB	2025/4/13 下午 08:46	N
CompTIA Security+上課講義.pdf	2024/11/28 上午 11:52	Microsoft Edge PDF Docume...	24,020 KB	2025/6/25 下午 03:24	N
Docker Container與Kubernetes系統_2025.pdf	2025/5/21 下午 04:01	Microsoft Edge PDF Docume...	19,757 KB	2025/6/25 下午 03:24	N
DOCKER_12 _20241121.pdf	2024/11/20 下午 03:15	Microsoft Edge PDF Docume...	15,214 KB	2025/6/25 下午 03:25	N
MS-4004-ENU-PowerPoint_01.pdf	2025/6/11 下午 04:29	Microsoft Edge PDF Docume...	4,234 KB	2025/6/25 下午 05:54	A
MS-4004-ENU-PowerPoint_02.pdf	2025/6/11 下午 04:30	Microsoft Edge PDF Docume...	10,605 KB	2025/6/25 下午 05:54	A
MS-4004-ENU-PowerPoint_Conclusion.pdf	2025/6/11 下午 04:31	Microsoft Edge PDF Docume...	204 KB	2025/6/25 下午 05:54	A
MS-4004-ENU-PowerPoint_Introduction.pdf	2025/6/11 下午 04:32	Microsoft Edge PDF Docume...	310 KB	2025/6/25 下午 05:54	A
MS-4005-ENU-PowerPoint_01.pdf	2025/6/11 下午 04:34	Microsoft Edge PDF Docume...	4,181 KB	2025/6/25 下午 05:54	A
MS-4005-ENU-PowerPoint_02.pdf	2025/6/11 下午 04:35	Microsoft Edge PDF Docume...	5,357 KB	2025/6/25 下午 05:54	A
MS-4005-ENU-PowerPoint_Conclusion.pdf	2025/6/11 下午 04:36	Microsoft Edge PDF Docume...	204 KB	2025/6/25 下午 05:54	A
MS-4005-ENU-PowerPoint_Introduction.pdf	2025/6/11 下午 04:36	Microsoft Edge PDF Docume...	62		
五個AI模型(安娜們)的聊天會議討論紀錄.PDF	2025/4/24 上午 02:46	Microsoft Edge PDF Docume...	29		
民間傳說鴨肉有毒嗎.pdf	2025/2/23 下午 05:05	Microsoft Edge PDF Docume...	9		
技術士檢定CNC車床.pdf	2025/2/23 下午 05:05	Microsoft Edge PDF Docume...	2,09		
侵占罪之基本概念.pdf	2025/2/23 下午 05:05	Microsoft Edge PDF Docume...	2,37		
惡意程式探討-6hr-中文(含附錄).pdf	2025/4/24 下午 12:50	Microsoft Edge PDF Docume...	18,816 KB	2025/4/24 下午 12:50	N



正常USB磁碟的檔案清單

名稱	修改日期	類型	大小	建立日期	屬性
24-英文-提詞-The concept of cyber security revol.txt	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
25-0706-Malwares.pcap	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2a.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2b.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2c.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2d.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2e.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2f.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2g.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2h.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-0706-Malwares-2i.PNG	2025/7/12 下午 01:34	捷徑	1 KB	2025/7/12 下午 01:34	A
25-內部資安攻擊的實務案例.pptx	2025/7/12 下午 01:17	捷徑	2 KB	2025/7/12 下午 01:17	A
25-端點偵測回應警訊判讀.pptx	2025/7/12 下午 01:17	捷徑	2 KB	2025/7/12 下午 01:17	A
2021-0304-09-DDOS-210.61.114.241.pcap	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
2021-0304-09-DDOS-210.61.114.241-Map.PNG	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
2021-0304-09-DDOS-210.242.186.93.pcap	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
NG	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
	2025/7/12 下午 01:33	捷徑	1 KB	2025/7/12 下午 01:33	A
pdf	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A
	2025/7/12 下午 01:17	捷徑	1 KB	2025/7/12 下午 01:17	A



異常USB磁碟的檔案清單(病毒)

【攻擊預警】近期勒索軟體活動頻繁，請提高警覺

國家資通安全研究檢測防禦中心 <A23031@nics.nat.gov.tw>
收件者

按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

trojan_killer.rar
442 KB

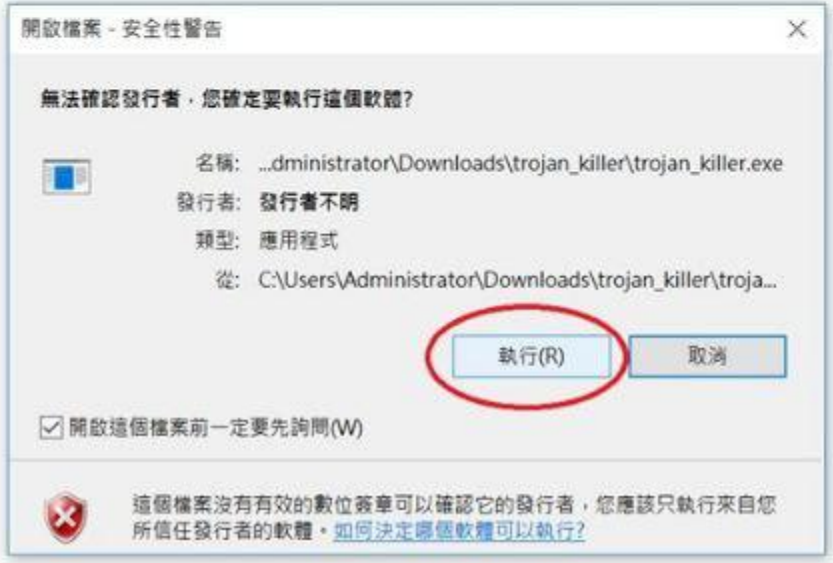
[內容說明:]
轉發國家資通安全研究檢測防禦中心 資安訊息警訊

近期加密勒索軟體活動異常活躍。
加密勒索軟體使用RSA-2048與AES-128 加密機制來加密檔案資料，所以遭到加密的檔案資料幾乎無法自行復原。國家資通安全科技中心根據被害者電腦的索軟體活樣本，製作了勒索軟體專殺工具。請注意查收附檔。

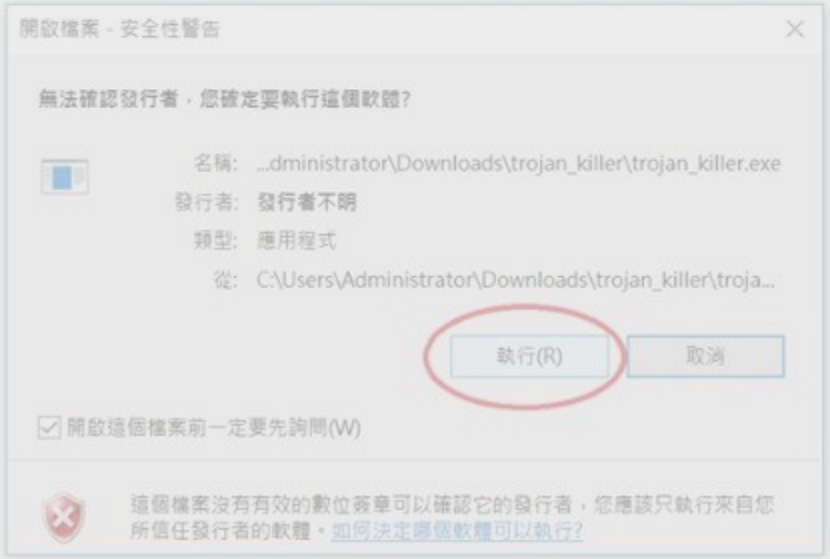
附件解壓密碼：123456

解壓后，雙擊“專殺軟體：trojan_killer”，出現如圖所示時，點擊【執行】。如未中勒索軟體，不會有任何提示；如若發現，則會提示殺毒軟體進行查殺。

異常資安郵件特徵
1.附件檔案為**壓縮檔案**，需要密碼才能解壓縮。
2.該**密碼**以明碼**明示**於電郵內容。



偽冒資安通知的社交工程攻擊



偽冒資安通知的社交工程攻擊

【攻擊預警】近期勒索軟體活動頻繁，請提高警覺

國家資通安全研究檢測防禦中心 <A23031@nics.nat.gov.tw>
收件者

按一下這裡下載圖片。為了協助保護您的隱私，Outlook 不會自動下載郵件中的某些圖片。

trojan_killer.rar
442 KB

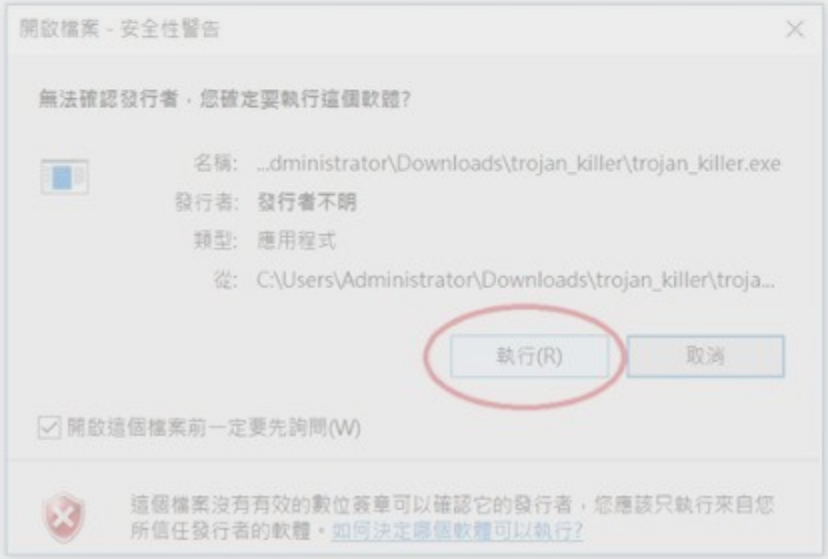
[內容說明:]
轉發國家資通安全研究檢測防禦中心 資安訊息警訊

近期加密勒索軟體活動異常活躍。
加密勒索軟體使用RSA-2048與AES-128 加密機制來加密檔案資料，所以遭到加密的檔案資料幾乎無法自行復原。國家資通安全科技中心根據被害者電腦的索軟體活樣本，製作了勒索軟體專殺工具。請注意查收附檔。

附件解壓密碼：123456

解壓后，雙擊“專殺軟體：trojan_killer”，出現如圖所示時，點擊【執行】。如未中勒索

不會有任何提示；如若發現，則會提示殺毒軟體進行查殺。



偽冒資安通知的社交工程攻擊

異常資安郵件特徵
1.附件檔案為**壓縮檔案**，需要密碼才能解壓縮。
2.該**密碼**以明碼**明示**於電郵內容。

偽冒會議通知的社交工程攻擊

[redacted]工業總會敬邀[redacted]老師擔任「2025國際經貿新局對台灣的機會及挑戰研討會」主講人

[redacted]@hopperwing.com.tw>
收件者 [redacted]

您已於 2025/3/4 上午 11:39 回覆此訊息。

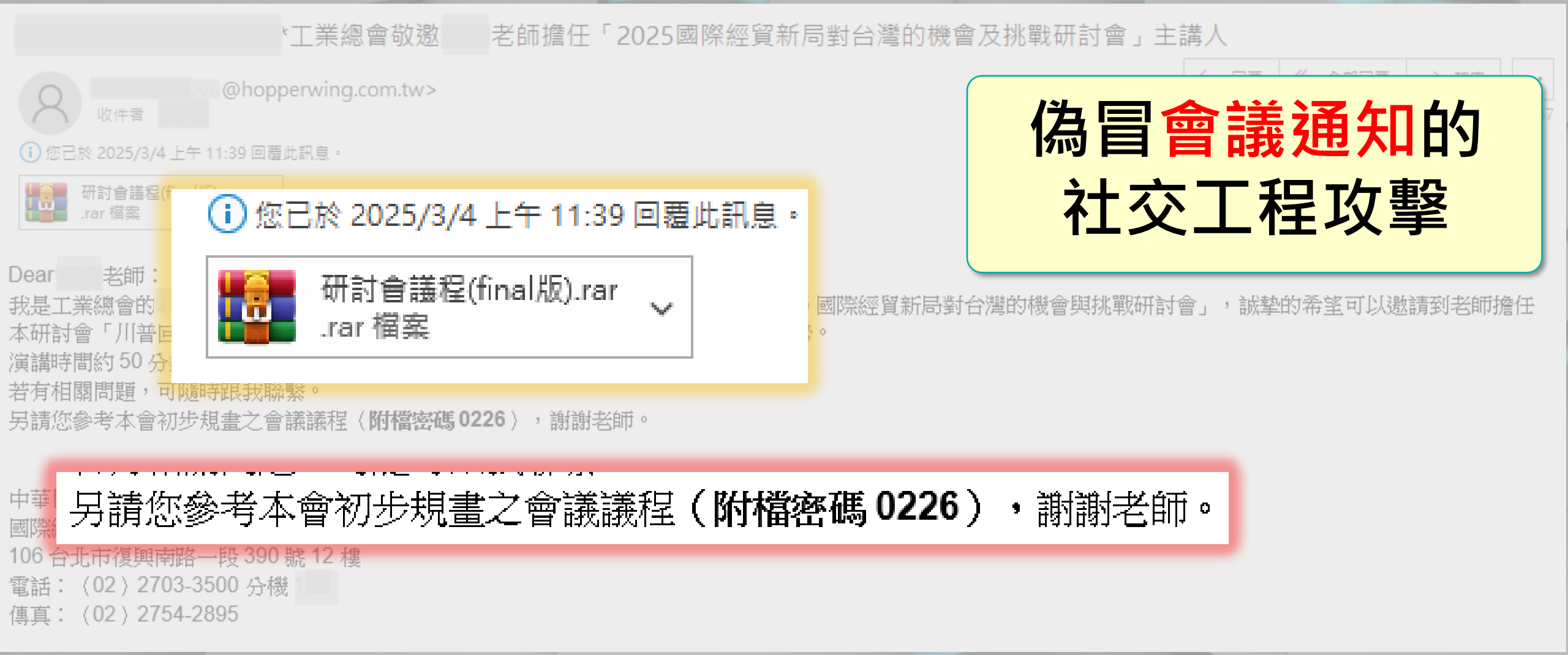
研討會議程(final版).rar
.rar 檔案

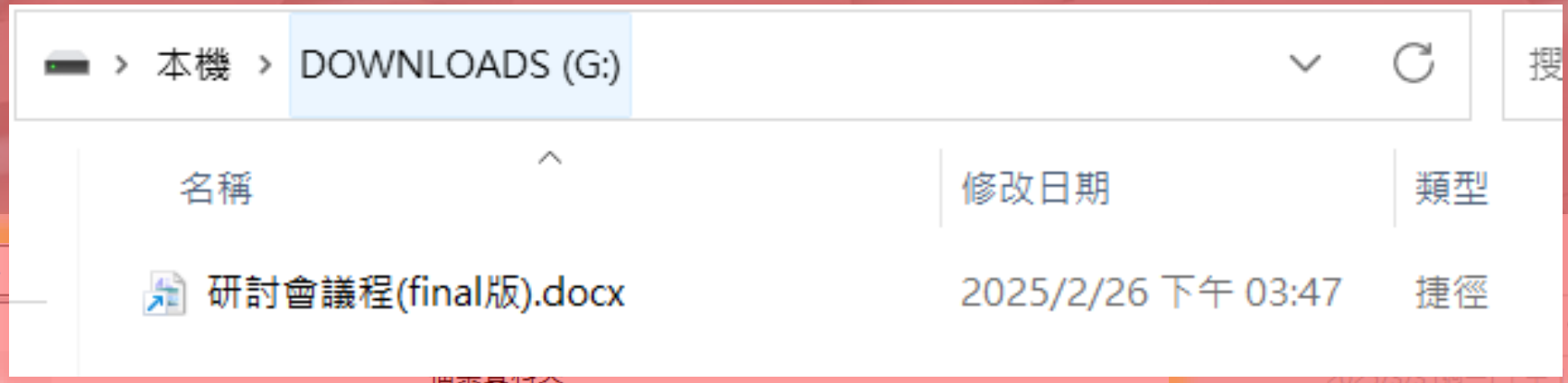
Dear [redacted]老師：
我是工業總會的[redacted]，今年**4 月 26 日（周六）**本會將於台北國際會議中心舉辦「2025 國際經貿新局對台灣的機會與挑戰研討會」，誠摯的希望可以邀請到老師擔任本研討會「川普回歸之美中台三角情勢發展」議題之主講人，與廠商們分享最新的情勢。
演講時間約 50 分鐘(含 QA 約 5-10 分鐘)，並附上薄酬(公務機關統一價格 2,000 元)
若有相關問題，可隨時跟我聯繫。
另請您參考本會初步規畫之會議議程（**附檔密碼 0226**），謝謝老師。

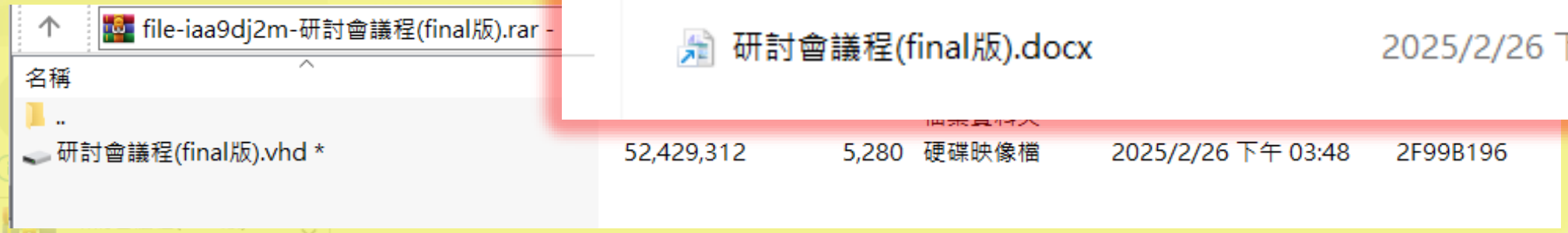
中華民國全國工業總會
國際經貿組 [redacted]
106 台北市復興南路一段 390 號 12 樓
電話：（02）2703-3500 分機 [redacted]
傳真：（02）2754-2895

異常資安郵件特徵
1.附件檔案為壓縮檔案，需要密碼才能解壓縮。
2.該密碼以明碼明示於電郵內容。

偽冒會議通知的社交工程攻擊







另請您參考本會初步規畫之會議議程（**附檔密碼 0226**），謝謝老師。

RtkAudUService64.e...	3804	"C:\WINDOWS\System32\DriverStore\FileRepository\realtekservice.inf_amd64_1e9988599adb3e80\RtkAudUService64.exe"
RtkAudUService64.e...	6800	"C:\Windows\System32\DriverStore\FileRepository\realtekservice.inf_amd64_1e9988599adb3e80\RtkAudUService64.exe" -background
SecurityHealthSystr...	7152	"C:\Windows\System32\SecurityHealthSystray.exe"
Taskmgr.exe	8676	"C:\WINDOWS\system32\taskmgr.exe" /1
wscript.exe	7268	"C:\WINDOWS\system32\wscript.exe" C:\Users\EAE9D~1.BOO\AppData\Local\Temp\39yjnolsu6abj5wd.vbe
WUDFHost.exe	1228	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunica...
WUDFHost.exe	4252	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunica...
WUDFHost.exe	1460	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunica...
WUDFHost.exe	4484	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunica...
WUDFHost.exe	9748	"C:\Windows\System32\WUDFHost.exe" -HostGUID:{193a1820-d9ac-4997-8c55-be817523f6aa} -IoEventPortName:\UMDFCommunica...

159	122.305929	167.99.78.230	192.168.200.55	Singapore	HTTP	351	HTTP/1.1 301 Moved Permanently (text/plain)
163	122.372687	167.99.78.230	192.168.200.55	Singapore	HTTP	475	HTTP/1.1 301 Moved Permanently (text/plain)
177	127.842312	192.168.200.55	107.163.176.248	United States	HTTP	770	POST /posg/ HTTP/1.1 (application/x-www-form-urlencoded)Continuation
185	127.986825	192.168.200.55	107.163.176.248	United States	HTTP	223	GET /posg/?UlX4x4=ubXZc8Lw4mJc3xUwsA2Fom6vfxMHktTeIqidpoEfiJedYlC0ujJ2/IRf3uuS4CuWAY
202	134.634891	192.168.200.55	172.67.209.181	United States	HTTP	782	POST /posg/ HTTP/1.1 (application/x-www-form-urlencoded)Continuation
208	134.764816	192.168.200.55	172.67.209.181	United States	HTTP	227	GET /posg/?UlX4x4=2ftWexiB9YB3GoJR+FGSurtkSkg9dV5rFAxPxgQ9sNj4gV41Wiy8zimP5YDHLJYBYS
212	134.915602	172.67.209.181	192.168.200.55	United States	HTTP	867	HTTP/1.1 301 Moved Permanently
222	140.466875	192.168.200.55	99.83.154.118	United States	HTTP	767	POST /posg/ HTTP/1.1 (application/x-www-form-urlencoded)Continuation
227	140.468698	192.168.200.55	99.83.154.118	United States	HTTP	222	GET /posg/?UlX4x4=1S/HE5r3wKSfbjkU36HwoFEi3ZCAzOv45zmOyYOiZaD7Wz8TU1BTseiXxq1BVP8Zt5
233	140.923643	99.83.154.118	192.168.200.55	United States	HTTP	366	HTTP/1.1 403 Forbidden (text/html)
251	146.286994	192.168.200.55	34.102.136.180	United States	HTTP	782	POST /posg/ HTTP/1.1 (application/x-www-form-urlencoded)Continuation
257	146.290343	192.168.200.55	34.102.136.180	United States	HTTP	227	GET /posg/?UlX4x4=oDXz3AL/E/dKmohDjdkpJVWy7gxCn4GBvOR6hingcS0p0n15GJBdyvMMF+NlqOtDtS
260	146.390734	34.102.136.180	192.168.200.55	United States	HTTP	604	HTTP/1.1 405 Not Allowed (text/html)
264	146.393313	34.102.136.180	192.168.200.55	United States	HTTP	515	HTTP/1.1 403 Forbidden (text/html)
305	165.573459	192.168.200.55	154.23.170.189	United States	HTTP	767	POST /posg/ HTTP/1.1 (application/x-www-form-urlencoded)Continuation
311	165.704549	192.168.200.55	154.23.170.189	United States	HTTP	222	GET /posg/?UlX4x4=m14LeIzuznjoF/Hgs2vsjZgHPXp4mwyToPngn0s
312	165.705403	154.23.170.189	192.168.200.55	United States	HTTP	468	HTTP/1.1 404 Not Found (text/html)
317	165.838735	154.23.170.189	192.168.200.55	United States	HTTP	468	HTTP/1.1 404 Not Found (text/html)
333	171.151267	192.168.200.55	92.205.7.199	France	HTTP	782	POST /posg/ HTTP/1.1 (application/x-www-form-urle
340	171.392639	192.168.200.55	92.205.7.199	France	HTTP	227	GET /posg/?UlX4x4=2SDgxewiAHIHeb9NVep0fYVz+/nb9U2

結論 Q&A

Diamond 資訊安全規則

1.絕對不在自己的手機電腦，做任何危險的手機電腦操作。
2.當防毒軟體表示該檔案有「毒」，它一定是惡意程式。
　而防毒軟體表示沒有「毒」的時候，只代表沒有掃到病毒，並不表示該檔案是乾淨的無毒檔案！
3.做好資訊安全工作，不用花大錢，只要養成電腦網路的好習慣！

dmliu99999@gmail.com

劉得民