TWCERT/CC 資安情資電子報

2023 年 1 月份

電子報序言

台灣電腦網路危機處理暨協調中心(以下簡稱 TWCERT/CC)在數位發展部指導下，推動企業資安通報協處、產品資安漏洞通報、惡意檔案檢測服務及資安情資分享等工作，以提升國家資安聯防能量，並維護整體網路安全。

TWCERT/CC 本月份所發布之資安情資電子報，為透過官方網站、電子郵件及電話等方式接收資安情資，並與國內外 CERT/CSIRT、資安組織、學研機構、民間社群、政府單位及私人企業間資安情資共享，將接收與共享之情資進行彙整、分析與分享，主要分成以下 8 章節：

第 1 章、封面故事：主題式資訊安全專題分享。

第 2 章、資安小知識：提供資安基礎概念、資安防護指南等知識，以提升大眾資安素養。

第 3 章、資訊安全宣導：針對近期資安議題、TWCERT/CC 服務或配合政府資安政策等進行資安宣導，以提升大眾資安意識。

第 4 章、資安活動紀事：TWCERT/CC 主辦或參與之資安活動及訓練課程等。

第 5 章、國內外重要資安事件：研析國內外相關資安情報，及彙整上述方式接收之資安情資，進行分析與分享。範疇包含資安趨勢、國際政府組織資安資訊、社群媒體資安近況、行動裝置資安訊息、軟體系統資安議題、軟硬體漏洞資訊及新興應用資安。

第 6 章、資安研討會及活動：近期舉辦之國內外資安相關研討會、訓練課程及資安競賽等活動資訊分享。

第 7 章、TVN 漏洞公告：TWCERT/CC 為 CVE 編號管理者 (CVE Numbering Authorities, CNA)，協助國內外廠商處理產品漏洞並完成漏洞修補，此章說明上月發布於台灣漏洞揭露 (Taiwan Vulnerability Note, TVN) 平台之漏洞嚴重程度前五的產品漏洞資訊。

第 8 章、資安情資分享概況：將上月份 TWCERT/CC 每日接收及分享之資安情資，針對對外資安情資分享地區及各項資安攻擊類型進行統計。

目錄

第 1 章、 封面故事

殭屍網路資安威脅與防護

- 殭屍網路可發起多種攻擊，使目標網路崩潰，注入惡意軟體，收集資訊或執行 CPU 密集型任務等，已演化出 2 種主要架構與 7 種類型。
- 在 2020 Q1 與 2021 Q1 的國際殭屍網路趨勢分析中，remote access tool 與 credential stealer 為最具規模、危害最大的兩種類型，而 Emotet 被列為最危險的殭屍惡意軟體之一，IcedID、Dridex、Quakbot、TrickBot 類似 Emotet，皆於發送大量惡意垃圾郵件入侵後，再用勒索軟體加密資料以達攻擊目的。
- 我國殭屍惡意軟體的感染數量，已呈現收斂下降的趨勢，例如 mirai、sality、kratos 皆大量感染一段時間後，數量降至極低，本報告也探討其它曾排入統計前 10 名的惡意軟體，並分析其趨勢及特點。
- 我國與國際趨勢排行榜差異，主要是因比較基準有所不同，但仍具參考意義，其次為攻擊目標差異，例如以挖礦為目標，便不會因攻擊而被通報，而在環境、產業、常見設備等存在差異，也導致結果不同。
- 除了一般性的防範殭屍惡意軟體建議，並根據趨勢分析結果，再提出特別注意之建議事項，包含應重視安全性更新，關注行動裝置、物聯網之安全性議題，以及挖礦惡意軟體的增長趨勢等。

一、簡介

殭屍網路是由 C&C（command and control）伺服器控管的受感染設備所組成的網路，其規模可能超過一百萬台設備，其中 C&C 伺服器又稱惡意中繼站，由攻擊者操縱殭屍網路發起攻擊，旨在使目標網路崩潰，注入惡意軟體，收集資訊或執行 CPU 密集型任務等。

不管是技術或是成本層面，運行殭屍網路的門檻都不高，在暗網(dark net)上已提供各種租售方案，數十美金即可由駭客組織代為發動殭屍網路攻擊。在許多合法網站和 YouTube 上都有大量技術教學，導致殭屍網路難以阻絕。

利用殭屍網路發起的攻擊，包括：

1. 分散式阻斷(DDoS)攻擊：DDoS 攻擊需要發起大量的流量或是服務請求，故殭屍網路最為適合被用於 DDoS 攻擊。
2. 挖礦：加密貨幣是通過求解加密的數學方程式而取得，需要大量的 CPU 運算或是磁碟空間，故透過殭屍網路的建立，讓眾多設備協助參與挖礦，增加其成功率。
3. 資訊窺探：殭屍網路可用於監視網路流量，可以被動地收集資訊，也可以主動地將惡意代碼注入 HTTP 流量中。
4. 阻塞(Bricking)攻擊：阻塞攻擊會刪除 IoT 設備的軟體模組，使其變得無用或阻塞，攻擊者可能會在多階段攻擊中使用阻塞攻擊，以隱藏發起主要攻擊時可能留下的線索。
5. 垃圾郵件：殭屍網路會從用戶常輸入其電子郵件地址的地方收集資料，用於創建帳戶和發送垃圾郵件。

隨著偵防技術的發展，殭屍網路亦隨之演進，主要可分為兩種架構：

1. 集中式：傳統的殭屍網路運作結構是由客戶端與惡意中繼站組成，以 C&C 伺服器運行整個殭屍網路，因為架構簡單，如今仍是主要的殭屍網路結構方式。其缺點在於存在單點故障的問題，只需將 C&C 伺服器做重點清除，即可使殭屍網路失效。

2. 去中心化類型：新一代的殭屍網路是 P2P(point to point)的方式，殭屍網路中的各個節點設備彼此共享命令和訊息，不與 C&C 伺服器直接聯繫。P2P 殭屍網路實施技術難度較高，但更具彈性，而且每個殭屍程序都獨立的擔任客戶端和服務端，清除難度很高。

從殭屍惡意軟體的行為區分，則可分為以下 7 種類型，近年來的趨勢統計中，remote access tool 與 credential stealer 為規模、危害最大的類型。

表 1、殭屍惡意軟體行為類型

種類	說明
Credential stealer	憑據偷取，資訊蒐集
Remote access tool	讓攻擊者可遠端存取受害設備，功能完整，具強大控制力
E-banking trojan	針對銀行金融的木馬程式
Dropper	木馬的一種，功能是安裝其它惡意軟體
Backdoor	可讓攻擊者遠端存取受害設備，功能有限，可建立連線、收送資料等
Keylogger	記錄使用者的輸入行為，蒐集資訊
Miner	以控制設備進行挖礦為主，獲取加密貨幣

二、國際殭屍網路趨勢分析

關於殭屍網路的公開統計資料並不多，主要以利用殭屍網路所發起的攻擊資料為主。而從殭屍網路規模的統計來看，參考 2020 Q1 與 2021 Q1(如圖 1)的國際殭屍網路排行進行趨勢比較，表中的排名變化是與前一季相比，2020 Q1 是與 2019 Q4 相比，2021 Q1 是與 2020 Q4 相比。

	2020 Q1			2021 Q1		
	名稱		類型	名稱		類型
1	Lokibot	－	Credential Stealer	Emotet	N	Dropper
2	AZORult	－	Credential Stealer	RemcosRAT	↑	Remote Access Tool(RAT)
3	Gozi	↑	e-banking Trojan	Lokibot	↓	Credential Stealer
4	NanoCore	↓	Remote Access Tool(RAT)	AsyncRAT	↑	Remote Access Tool(RAT)
5	RemcosRAT	↑	Remote Access Tool(RAT)	NanoCore	↓	Remote Access Tool(RAT)
6	Emotet	↑	Dropper	RedLine	↓	Credential Stealer
7	Adwind	↑	Remote Access Tool(RAT)	AgentTesla	↓	Remote Access Tool(RAT)
8	Njrat	↑	Remote Access Tool(RAT)	Raccoon	N	Credential Stealer
9	Arkei	↑	Credential Stealer	Arkei	↑	Credential Stealer
10	QuasarRAT	↑	Remote Access Tool(RAT)	Gozi	↓	e-banking Trojan

N：本季新入榜 －：排名與上季相同 ↑：排名比上季提高 ↓：排名比上季下降

圖 1、2020 與 2021 Q1 國際殭屍惡意網路排行

2020 年第一季，前 10 名的殭屍網路幾乎都是遠端訪問工具（RAT, Remote Access Tool）或憑據竊取(Credential Stealer)程序類型，只有 Gozi（電子銀行木馬）和 Emotet（Droppers / Backdoors）例外，而到了 2021 Q1，主要類型依然是遠端訪問工具或憑據竊取程序類型。

兩種主要類型反映出的是，皆做為攻擊的前置步驟之用，透過大規模的蒐集受駭主機資訊與使用者憑據，將資訊再次販賣，亦或是從中篩取具有價值的目標，再進階的攻擊。由此可知殭屍網路除了發起 DDoS 等直接的攻擊

外，大部分的功能也因應近年來駭客集團以賺取錢財為目的，因此轉變做為攻擊的前奏。

其中銀行木馬(e-banking trojan)在榜上雖然僅有一個上榜，但影響力不容小看，銀行木馬多數透過垃圾郵件散播傳染，其主要特性為竊取銀行帳號密碼，更有甚者，在 2021 年 3 月國內曾發現有 10 款運行於行動電話的銀行木馬 APP，嚴重者可直接遠端操控轉移帳戶資金，直接的造成財產損失。

以下特別就較為嚴重之惡意軟體加以說明：

- Raccoon Stealer：2019 年底此惡意軟體出現，在 2020 Q1 上榜，它通過受害者主機上已存在的惡意軟體、垃圾郵件，漏洞攻擊工具等途徑傳播到主機中，主要目的是竊取資訊和使用者憑據。
- Lokibot：Lokibot 在 Spamhaus 這個資安單位的統計中已占據了排行第 1 名的地位長達 2 年，以殭屍網路規模來說，在國際上為近年來影響最大的惡意軟體之一。
- AZORult：在過往 AZORult 是很嚴重的殭屍網路，2020 發現 AZORult 殭屍網路活動略為減少，但仍是 Q1 的第二大威脅。
- NanoCore 和 Remcos：這 2 個家族是 RAT(遠端訪問)類型殭屍網路中，具有主導地位的惡意軟體，其功能也有互相參考演進的趨勢。
- Emotet：主要針對全球的電子銀行客戶，隨時間演進其惡意行為，在 2019 年開始即被認為是最危險的殭屍網路之一，因為 Emotet 具有下載其它惡意軟體的功能，而且具有強大的閃避傳統特徵偵測機制的能力。
- IcedID、Dridex、Quakbot、TrickBot：這些殭屍網路發送了大量包含惡意檔案的垃圾郵件，手法與 Emotet 相似，靠垃圾郵件入侵到企業網路後，再用勒索軟體對資料加密，以達攻擊目的。

三、我國電腦遭感染的威脅狀況

如前所述，殭屍網路為許多資安攻擊的發起基礎，但在趨勢分析上，國內缺乏殭屍電腦感染狀況的相關統計資料，故本報告採用國外通報資料進行分析。

(一)情資來源

本報告主要依據 TWCERT/CC 的情資來源，Shadow Server 與 Team Cymru 通報的殭屍網路情資。統計期間自 2020 年 9 月到 2021 年 4 月共 8 個月，國外情資單位所通報之資料為我國受殭屍惡意軟體感染的 IP，殭屍惡意軟體共 177 種，以 android 行動裝置為目標的有 18 種，其它電腦與物聯網設備為目標的共 159 種，但主要的殭屍惡意軟體(感染超過 1 萬個 IP 以上)則只有 10 種。

從通報數量上看，Shadow Server 約通報了 80%的數量，Team Cymru 約佔 20%，各有側重的領域，其通報之惡意軟體種類幾乎沒有重複，只有 mirai 為兩個單位皆有通報，故本報告之分析是整合 2 個情資來源以完整涵蓋。

表 2、情資單位通報的殭屍惡意軟體種類

情資單位	Team cymru	Shadow server
殭屍惡意軟體名稱	Conficker	Mirai
	Mirai	Qsnatch
	Minerpanel	Android-hummer
	Isrstealer	Wannacrypt
	Quant	Sality
	kratos	Lethic
	Ponyloader	Virut
	Gumblar	Avalanche-andromed
	Smokeloader	Mozi
	lokibot	emotet

(二)國內統計排名分析

本報告藉由通報情資進行國內感染狀況之分析，以下會從感染數量以及感染趨勢進行分析。

圖 2 為統計期間之感染數量排名，以前 10 名來說，2020 年 9 月到 2021 年 4 月的逐月排名變動幅度不大，僅有少數新增的惡意軟體。

2020 / 09		2020 / 10		2020 / 11		2020 / 12		2021 / 01		2021 / 02		2021 / 03		2021 / 04	
mirai	N	mirai	▬	mirai	▬	mirai	▬	mirai	▬	conficker	↑	android-hummer	↑	android-hummer	▬
minerpanel	N	minerpanel	▬	qsnatch	↑	qsnatch	▬	android-hummer	↑	android-hummer	▬	qsnatch	↑	qsnatch	▬
isrstealer	N	isrstealer	▬	Conficker	↑	conficker	▬	qsnatch	↓	mirai	↓	conficker	↓	conficker	▬
quant	N	quant	▬	wannacrypt	↑	android-hummer	N	conficker	↓	qsnatch	↓	wannacrypt	↑	wannacrypt	▬
kratos	N	kratos	▬	sality	↑	wannacrypt	↓	wannacrypt	▬	wannacrypt	▬	lethic	↑	virut	↑
qsnatch	N	qsnatch	▬	minerpanel	↓	sality	↓	sality	▬	lethic	↑	emotet	↑	lethic	↓
conficker	N	conficker	▬	isrstealer	↓	lethic	↑	lethic	▬	avalanche-andromeda	↑	virut	↑	emotet	↓
wannacrypt	N	wannacrypt	▬	quant	↓	virut	N	virut	▬	emotet	N	avalanche-andromeda	↓	avalanche-andromeda	▬
sality	N	sality	▬	kratos	↓	avalanche-andromeda	N	avalanche-andromeda	▬	virut	↓	android-darksilent	↑	mozi	N
ponyloader	N	lethic	N	lethic	▬	android-darksilent	N	android-darksilent	▬	android-darksilent	▬	android-uupay	N	android-uupay	▬

N：本月新入榜　▬：排名與上月相同　↑：排名比上月提高　↓：排名比上月下降

圖 2、2020 年 9 月到 2021 年 4 月感染數的逐月 10 大排名

將統計期間的感染總數量做排名則會得到圖 3 的前 15 名排行榜，前幾名的惡意軟體為國內被通報的主要殭屍軟體，例如 mirai 從 2020 年 9 月即為第一名，並持續了 5 個月，感染 IP 數量超過 10 萬，而 11 到 15 名則只有不到 5 千的感染數量。

名次	名稱	名次	名稱	名次	名稱
1	mirai	6	sality	11	lethic
2	qsnatch	7	minerpanel	12	virut
3	conficker	8	isrstealer	13	avalanche-andromeda
4	android-hummer	9	quant	14	emotet
5	wannacrypt	10	kratos	15	mozi

圖 3、曾出現在前 10 名的殭屍惡意軟體

以下逐一分析惡意軟體的趨勢與特點：

- 第 1 名的 mirai 主要以運行 linux 的物聯網設備為攻擊目標，會持續的在網路上掃描 IP，並以常用的預設帳號密碼進行嘗試登入，待登入後再進行惡意軟體安裝等入侵行為。從圖 2 可見 mirai 的威脅已大幅降低。
- 與 mirai 有相似狀況的第 6 名 sality、第 10 名 kratos 皆曾有過大量感染，而後經過通報國內相關單位處理後，感染數量降至極低。
- 第 2 名的 qsnatch 主要是利用 QNAP 的 NAS 設備弱點進行感染，感染數量

雖有下降趨勢，但仍應持續關注。

- 第 3 名的 conficker 原本主要感染 windows 系統，但隨著不斷演進，已擴展到較為大型的物聯網設備，尤其是以醫療為主的 MRI 機器、CT 掃描器等，是一種被駭客廣泛使用的惡意軟體家族。
- 第 4 名的 android-hummer 則是入榜唯一的行動裝置惡意軟體，裝置遭此惡意軟體感染後，即可依感染目的下載各種軟體，其特性是移除困難，在國內危害甚深。
- 第 5 名的 wannacrypt 即為知名的 wannacry，與第 10 名 kratos 皆為勒索軟體，都是針對 windows 系統進行感染。
- 第 6 名的 sality 其特色為，受感染主機除了連回 C2C 伺服器更新資訊外，相互間還會建立 P2P 網路，互相分享傳遞資訊，增加攻擊行為的複雜度，這點在第 15 名的 mozi 也有相同設計。
- 第 7 名 minerpanel 是唯一進入排行的挖礦用殭屍軟體，具備極強的藏匿躲避偵測功能，推測國內應仍有不少單純被用來挖礦的受駭主機。
- 第 8 名 isrstealer 以鍵盤側錄竊取機密資料，主要透過 email 附件傳遞，第 11 名的 lethic 亦以信件為主要傳播手段。
- 第 9 名 quant 是一種專門用來下載惡意軟體的 loader 工具，感染初期因無攻擊行為，故難以察覺，許多攻擊性強的惡意軟體利用 quant 作為前置步驟，造成極大危害。
- 第 12 名的 virut 主要是將惡意程式碼注入到可執行文件中，也會將惡意的 iframe 注入到 HTML、PHP 等網頁中，它的傳播途徑極難防範，也是排行榜中唯一與網站程式有關的。
- 第 13 名 avalanche-andromeda 與第 14 名的 emotet 雖然在國內感染排名不高，也是值得關注的 2 個惡意軟體。

總體而言，15 個惡意軟體，挖礦用的僅有一個，其它多為攻擊性強烈的類型，亦符合因對國外攻擊而被偵測的資料特性，故此分析較適合瞭解國內受此類型殭屍惡意軟體感染的狀況。

(三)國內與國際趨勢差異分析

由圖 4 可觀察到，通報排行榜上的惡意軟體出現的時間通常為 2 年以

前，甚至是十幾年前，而在國際趨勢看來，惡意軟體的變化很快，新出現的惡意軟體很快會上榜，與國際上的統計有極大差異。

名次	名稱	出現時間	名次	名稱	出現時間	名次	名稱	出現時間
1	mirai	2016	6	sality	2003	11	lethic	2008
2	qsnatch	2014	7	minerpanel	2013	12	virut	2006
3	conficker	2008	8	isrstealer	2016	13	avalanche-andromeda	2016
4	android-hummer	2016	9	quant	2017	14	emotet	2014
5	wannacrypt	2017	10	kratos	2016	15	mozi	2019

圖 4、前 15 名的殭屍惡意軟體出現時間

與國際趨勢比較，其差異的原因有三：

一是因國內排行榜是依據對國外發起攻擊的 IP 進行統計，國外則為資安業者透過產品偵測或直接由偵察到的 C&C 伺服器得知，比較基準有所不同，但仍具參考意義。

二是因為惡意軟體攻擊目標差異，例如以挖礦為目標的殭屍惡意軟體較少會再向外發動攻擊，亦或是針對特定產品或對象，例如銀行、物聯網等具有區域或產業特性，導致我國的分析數據中較少此類型的惡意軟體。

三是整體環境差異，例如 sality 與 virut 等國外曾經造成重大威脅的惡意軟體，在國外排行榜已近乎消失，國內卻仍能名列前矛，可見國內環境仍適合其傳播感染。

四、分析與建議

殭屍網路是發起多種大規模攻擊的基礎，亦是攻擊步驟中惡意工具下載的一個過程，若能適當防範將可降低後續更為嚴重的資安危害。

防範殭屍惡意軟體的建議為：

1. 定期的安全意識培訓，教導使用者/員工識別惡意連結或附件。
2. 建立完善軟體更新程序，防範漏洞所產生的風險。
3. 針對病毒的解決方案，保持防毒軟體最新狀態並定期掃描網路。

4. 在網路上部署入侵偵測系統（IDS）。
5. 建立端點保護方案，盡可能包括 rootkit 檢測能力。

再依據本報告所分析之主要的殭屍惡意軟體特性，提供以下建議。

1. 幾個較早期的惡意軟體對國內危害仍大，這些惡意軟體可能持續在更新變種，唯有持續重視安全性更新，並且淘汰不再被維護的作業系統或軟體才是最有效的方法。
2. 行動裝置的安全性議題，使用者可選擇購買通過資安標準檢測的手機，並注意惡意連結，謹慎下載 APP，即可避免手機變成殭屍設備。
3. 物聯網裝置通常具有同類型大量部署的特性，一旦物聯網裝置已超過產品生命週期無法取得更新，就應啟動產品汰換機制。而且選購新產品時，以選擇通過資安標準認證的產品較有保障。
4. 對於挖礦用的殭屍惡意軟體亦需加以關注，因其隱匿功能不斷增強，在防護方法上，可由效能消耗狀況這個觀點切入觀察。

- 資料來源：

1. Botnets Explained
2. Spamhaus Botnet Threat Update: Q1-2020
3. Spamhaus Botnet Threat Update: Q1-2021
4. 臺灣遭受惡意程式攻擊現況揭露，竟是 Botnet 攻擊最多國家

第 2 章、 資安小知識

行動裝置資安威脅及防護

隨著行動裝置的逐漸普及，為使用者的生活帶來極大便利，卻也伴隨更多資安威脅與風險。越來越多駭客將目標從電腦轉移到各式行動裝置上，以達到竊取資料之目的，甚至作為殭屍網路使用。不少企業或組織也允許個人以自備裝置(Bring Your Own Device, BYOD)，連入組織網路處理公司事務。然而，這樣的趨勢也隨著駭侵行為及病毒散佈的增加，導致企業或組織遭到的資安威脅逐漸擴大。

身為行動裝置的使用者，應加強對於行動裝置的資安防護與意識，以下提供相關資安防護與建議：

一、應用程式安全

- 不明的應用程式下載來源

下載安裝應用程式應透過官方軟體商店如 App Store、Google Play Store 等正規管道，避免在第三方或不明來源處下載安裝，例如透過 P2P 或社群媒

體安裝來路不明的盜版軟體或破解工具，特別是以檔案型式下載安裝的 APK 尤其危險，以免導致行動裝置資料遭竊、或被安裝後門程式等惡意軟體之風險。

- 應用程式檢測

美國 Web 應用安全組織 OWASP，提出了開發行動應用時應注意並避免的 10 個安全項目 Mobile Top 10，開發者可據以檢視自身開發之行動應用是否需修正或補足其防護能量，提升行動應用的資安強度。數位發展部及國內資安專家也參考國內外檢測標準，提出行動應用 APP 基本資安規範、動應用 App 基本資安檢測基準，提供使用者進行應用程式資訊安全檢測及評估其安全水準之依據。

- 應用程式更新

透過官方管道將應用程式更新至最新版本，並定期進行更新，以避免駭客利用應用程式的安全性漏洞進行駭侵行為。

- 應用程式權限要求

不少使用者在應用程式的要求下，便允許多餘權限予免費的應用程式，給予駭客入侵的機會。建議評估該應用程式要求的權限是否合理，並僅准許最小權限設定，例如關閉社群軟體上的自動下載功能，或是只允許通訊錄人員通訊，以及不允許非必要資料存取。

二、連線功能安全

- Wi-Fi

許多人習慣在車站、機場、飯店等公共場所用行動裝置連 Wi-Fi 上網，但免費 Wi-Fi 常隱藏釣魚陷阱，可能會監測使用行為、盜取個資，甚至造成錢財損失。建議使用免費公用 Wi-Fi 時，應使用安全的 VPN、僅在安全且加密的網站(網址為 HTTPS 開頭)登入，關閉行動裝置上的所在地偵測功能。

- 藍牙

建議使用者主動提防來自不明行動裝置的藍牙配對要求，只和信任的裝置進行配對連線。不使用時也建議將其關閉，以避免行動設備遭有心人士利用藍牙進行追蹤、駭入裝置並竊取資訊。

三、裝置使用/設定安全

- 密碼設定

建議行動裝置應設定螢幕鎖定密碼及 PIN 碼，避免遭未經授權的第三方人士入侵。密碼設定應注意複雜度(如中英文混合)、不使用簡單字元組合(如1111、abcdef)，以及不要在多個帳戶使用相同密碼。

- 行動裝置破解

行動裝置原廠會設定安全措施，以保護裝置的安全性。部分使用者為取得更高權限功能，會選擇進行破解，破解後的裝置易受到資安威脅，影響安全運作並導致安全措施失效，建議不要破解行動裝置原廠的安全設置。

四、資料保護

在下載並安裝應用程式前，仔細閱讀其授權聲明，避免提供非該應用程式所必需的授權，以免洩漏行動裝置中的機敏資料。

建議將行動裝置的資料進行備份，以利裝置遺失損壞時能夠將資料進行復原。

- 資料來源：

1. 行動應用程式資安威脅及防護
2. 惡意 APP 破解雙因子驗證，竊取交易認證碼
3. 免費無線網路服務 潛藏資安風險

4. 美國聯邦調查局提出警訊：在外旅遊時勿使用免費 Wi-Fi 服務

5. 藍牙 4.0 與 5.0 被發現嚴重漏洞

6. 資安風險、距離短 藍芽難用不得不用

7. 行動裝置資通安全注意事項

8. 美國國家安全局提供遠距工作者無線設備資安防護指南

9. 好記又難猜的密碼設定技巧

第 3 章、 資訊安全宣導

行動應用程式資安威脅及防護

一、簡介

APP 是應用程式(Application)的縮寫，是一種軟體應用程式，主要是在智慧型手機或行動裝置中使用。

行動應用 APP 依其功能可區分為遊戲類、教育類、商業類、生活風格類、娛樂類，以及工具類等數種類型。

正因為行動應用 APP 的廣受歡迎，使得駭客逐漸將駭侵或病毒散佈的目標從電腦轉向行動裝置的 APP 上，並且藉由使用者對 APP 的信任，透過行動應用 APP 進行惡意行為，從而獲取不法利益。

二、行動應用資安威脅

(一)行動應用 APP 資安威脅分析

行動應用 APP 的資安威脅，統稱為惡意行動應用程式(Malicious Mobile

Applications)，透過吸引使用者的某些功能或活動，誘使使用者下載並安裝該 APP，進而自動安裝惡意程式以竊取行動裝置中的資訊，甚至修改裝置內相關設定。

根據賽門鐵克 ISTR 報告，單純的惡意 APP 數量有逐漸下降之趨勢，然而勒索性的 APP 卻上升了，尤其是針對企業的勒索攻擊。因此，不論是企業或個人，對於行動裝置的安全防護，必須保持一定的警覺。

在所有的惡意 APP 中，比例最高的為工具類型，其次為生活風格類型，再其次為娛樂類型之 APP。工具類型的 APP 通常會要求給予較高的使用權限，駭客即利用此較高的授權，進行資料竊取、修改設定等惡意行為。

(二)行動應用 APP 資安威脅及案例

隨著 APP 數量以及使用者將機敏資訊存於行動裝置的比例增加，惡意 APP 對使用者的威脅以及損害程度逐漸上升。除了個人使用者外，企業同樣也遭受惡意 APP 的入侵，這些惡意 APP 可被分為以下五種類型：

1. 廣告(Adware)：經常偽裝成一般合法應用程式，並涉及購買行為。美國的移動安全防護及分析公司 Wandera，曾發現 Google Play 商店中的兩款美肌 APP 會跳出惡意廣告，並且加速行動裝置的電量流失。因此，當使用者下載行動應用 APP 後，若有廣告出現或是行動裝置的運行速度變慢，電池耗用增加，極可能是下載並遭到惡意 APP 的侵襲。

2. 網路釣魚(Phishing)：此種類型之惡意 APP 主要是將使用者導入釣魚網站，並且誘導使用者輸入相關資訊，以竊取個人資料。趨勢科技發現在 Google Play 商店中，有多款美肌相機 APP 會將使用者導入釣魚網站中並使其留下個資。因此，若使用者在下載並安裝行動應用 APP 後，突然收到關於贏得獎品，或帳號、訂閱服務將被停止等訊息，都極有可能遭到網路釣魚 APP 的駭侵。

3. 殭屍網路(Bots)：此種惡意 APP 可以在行動裝置後台運作，和殭屍控制主機

(botmaster)聯繫並執行命令，使用者不易察覺。曾有一款名為 Hidden Administrator 的惡意 APP，以 Android 系統為目標，在進入受害者行動裝置之後便隱藏起來。此應用程式會將自己的權限提升至管理員等級，並且控制該受害行動裝置，使變成殭屍網路或挖礦的工具。因此，若使用者在下載並安裝 APP 後，其行動裝置容易產生連線中斷、網路無法連接，或是在未經使用者授權的情況下，行動裝置自動安裝或移除任何 APP，則該行動裝置極有可能已下載到殭屍惡意 APP。

4. 間諜軟體(Spyware)：會監控和記錄使用者的裝置狀態或行為資訊，例如簡訊、電子郵件、電話紀錄、聯絡人、地理位置等訊息，並分享給遠端的伺服器。趨勢科技發現六款於 Google Play 商店上架之間諜軟體 APP。這六款惡意 APP，都是由被稱為「MobSTSPY」的間諜軟體偽裝而成，當使用者啟動後，間諜軟體會檢查行動裝置的網路狀態，搜集裝置型號等設備資訊，以及簡訊、電話簿等使用者資訊，再將竊取的資訊回傳給中繼站伺服器。因此，使用者在下載並安裝行動應用 APP 後，若發現行動裝置有奇怪的行為，除了應將可疑的 APP 移除外，也必須檢查內部是否有被安裝或放置可疑的檔案及程式，並將其移除和卸載。

5. 下載器(Downloader)：此種程式自身並非惡意程式，但會隱身於 APP 中，負責下載其他的惡意程式到使用者行動裝置中。以色列資安公司 Check Point，在 Google Play 商店中發現一款新的惡意 APP。該惡意 APP 具有開啟特定網址的功能，並進行網路釣魚行為，也能替受害行動裝置安裝新的惡意程式。因此，當使用者下載並安裝 APP 後，若出現未經使用者授權下載之 APP、檔案，或突增電池耗用、網路流量，以及額外費用等，都可能是行動裝置遭惡

意下載器感染所致。

三、行動應用防護

(一)行動應用 APP 防護機制

惡意 APP 難以完全防範，使用者在下載行動應用 APP 之前，必須注意下述幾點：

1. 定期更新行動裝置作業系統或應用程式之版本，配合廠商進行漏洞修補，提升防護能量。
2. 僅從信用良好的應用程式商店下載行動應用 APP。
3. 許多惡意 APP 會偽冒知名品牌或企業的標章，下載前須檢查並識別該 APP 是否確為該品牌或企業所屬。
4. 在下載並安裝 APP 前，仔細閱讀其授權聲明，避免提供非該 APP 所必需的授權，以免洩漏行動裝置中的機敏資料。
5. 使用者可以安裝行動安全應用程式，協助辨識惡意 APP，以隔絕並保護行動裝置中的機敏資料。
6. 為了減少行動裝置或資料因惡意 APP 遭到破壞，建議使用者定期備份手機中的機敏或重要資訊。

美國的 Web 應用安全非營利組織 OWASP，提出了開發行動應用 APP，必須注意並避免的 10 個安全項目 Mobile Top 10：

1. 平臺使用不妥當(Improper Platform Usage)：主要為開發者未確實使用平臺權限、TouchID 等安全控管機制。為了防止平臺使用不當，在行動應用 APP 開發時，必須在伺服器端實踐安全編碼(Secure Coding)及安全相關設置。

2. 不安全的數據存取(Insecure Data Storage)：當開發者未針對文件或機敏資訊的存取進行管控時，就容易出現存取漏洞。因此，開發者必須避免使用較差的加密資料庫，並應設定須透過特殊的工具方能進行數據存取。

3. 不安全的通訊(Insecure Communication)：在行動應用 APP 數據傳輸的過程中，駭客可以透過系統或設備的漏洞竊取傳輸中的機敏資料。因此，開發者必須注意資訊傳輸的安全設定，或使用可信的憑證中心所提供的簽章，防止因通訊不安全造成的損失。

4. 不安全的身分驗證(Insecure Authentication)：由於行動裝置經常只要求使用者輸入短密碼，導致易於被破解入侵。因此，開發者必須避免較弱的身分驗證模式，確保相關程序都在通過嚴謹身分驗證後方可使用。

5. 不足夠的加密法(Insufficient Cryptography)：若開發者未使用足夠且有效的加密法，則駭客容易入侵竊取資料，甚至還原加密數據。因此，開發者應使用經過驗證且經得起考驗的加密標準，替相關資訊加密。

6. 不安全的授權(Insecure Authorization)：若開發者使用較為脆弱的授權方式，則駭客可能會以合法使用者的身分登入 APP 中，取得其不應取得的權限。因此，建議開發者應使用後端伺服器中的訊息進行驗證，避免使用來自於行動裝置的權限資訊進行授權驗證。

7. 較差的程式碼品質(Poor Code Quality)：此種類型的問題，本身並不一定是安全問題，但容易引發安全的漏洞。因此，開發者必須確保在開發團隊中，都維持一致的編碼方式。

8. 程式碼竄改(Code Tampering)：由於 APP 及大部分數據都置於行動裝置中，駭客可能入侵後竄改 APP 中的程式碼，或是更動記憶體中資訊等。因此，開

發者必須提供驗證機制，檢測該行動應用 APP 是否曾經遭到他人竄改，並執行適當處置行為。

9. 逆向工程(Reverse Engineering)：駭客可能透過某些工具針對 APP 進行反組譯解析，或是從中得到該 APP 的相關資訊、機敏資料等，甚至藉以對後端系統進行攻擊。因此，為了防範逆向工程，開發者必須使用混淆工具，將其程式碼、字符表等資料進行混淆處理，避免輕易遭到逆向工程的威脅。

10. 額外功能(Extraneous Functionality)：許多開發者為了方便進行程式的修改或安全控管，會在 APP 的程式碼中留下額外功能，雖不具惡意，但卻可能被駭客利用來入侵並竊取相關資訊。因此，為了防範此資安問題的發生，通常須由資安專家對該行動應用 APP 進行程式碼檢查，方能確保沒有任何隱藏功能。

數位發展部也邀集國內資安領域專家，參考國內外檢測標準，提出行動應用 APP 基本資安規範，分別從「行動應用程式發布安全」、「安全敏感性資料保護」、「交易資源控管安全」、「行動應用程式使用者身分鑑別及授權與連線管理安全」、「行動應用程式碼安全」及「伺服器端安全檢測」等六個層面提出資訊安全技術要求，供業界開發行動應用程式時依循參考，以提高行動應用 APP 的安全品質。

另為提供第三方機構針對行動應用程式，進行資訊安全檢測及評估其安全水準之依據，進而發布「行動應用 App 基本資安檢測基準」，以行動應用程式之功能分類，訂定各類別之安全要求範圍，分為三級：

L1：無須使用者身分鑑別之行動應用程式。

L2：須使用者身分鑑別之行動應用程式。

L3：含有交易行為之行動應用程式。

欲進行檢驗之行動應用 APP，若同時符合兩個以上之類型特徵，則以符合類型中檢測項目較多者做為檢驗依據。

(二)行動應用 APP 安全檢測概況

根據行動應用資安聯盟的數據，在總體通過驗證之 APP 中，通過的行業類別佔比分別為：金融業 57.2%、其他類別(如工具類)34.4%、醫療 4.7%、行動支付類 2.1%、通訊類 1.6%。

再針對三個檢測基準進行統計，在總體通過驗證之 APP 中，通過 L1 級佔比 8%、L2 級佔比 36.6%、L3 級佔 55.4%。

四、分析與建議

1. 行動應用 APP 隨著行動裝置的普及正快速成長，將是未來軟體發展的一大重點。
2. 隨著行動應用 APP 的普及，其相關之惡意程式也逐漸增多，且因為企業允許個人自備裝置(BYOD)數量的增加，以致惡意行動應用程式對企業的威脅也逐漸上升。
3. 行動裝置中勒索惡意 APP 的數量有上升趨勢，代表駭客將許多勒索軟體從電腦轉而以行動裝置做為目標。
4. 台灣因惡意 APP 受害的比例略高於全球平均，因此使用者仍須注意行動應用 APP 的使用，避免遭受惡意 APP 的攻擊。
5. 為減少惡意 APP 之威脅，使用者宜定期更新行動裝置作業系統、相關軟體及應用程式，盡量從信用良好之應用程式商店下載 APP，並識別商標、檢驗其功能權限。也應定期備份裝置中的重要資料或機敏資訊，以降低損害風險。

6. 美國的 Web 應用安全非營利組織 OWASP，提出了開發行動應用 APP 最可能發生的 10 個弱點，希望開發者能在進行 APP 開發製作時加以注意，以減少資安漏洞，達到較佳的 APP 資安防護。

7. 我國政府也針對行動應用程式的開發，發布「行動應用 APP 基本資安規範」，以及「行動應用 App 基本資安檢測基準」，提供 L1、L2、L3 三個等級對應需檢測驗證的項目，以提高 APP 的資訊安全。

8. 由於行動應用 APP 隨著行動裝置的蓬勃發展，其數量逐年快速增加，許多病毒或駭侵手法也從電腦轉往行動裝置。除了使用者需注意並維持行動裝置的安全外，開發者更應針對所開發之行動應用 APP 進行全面檢測，建議可尋求相關資安檢測實驗室協助驗證，以提高其安全性，並讓使用者放心使用。

- 資料來源：

1. The State Of Mobile 2019
2. Malicious Mobile Apps: The New Threat To Small Businesses
3. Internet Security Threat Report Volume 24
4. Internet Security Threat Report Volume 23
5. Operation Sheep: Pilfer-Analytics SDK in Action
6. Mobile malware evolution 2018
7. Types of Mobile Malware
8. Mobile malware evolution 2018
9. 【手機病毒】想要拍出好氣色,當心 29 款美肌相機應用程式會發送色情內容,還會偷個資盜用照片
10. Hidden Android Administrator Apps
11. Spyware Disguises as Android Applications on Google Play

12. SimBad: A Rogue Adware Campaign On Google Play
13. Mobile Top 10 2016-Top 10
14. 行動應用 APP 基本資安規範
15. 行動應用資安聯盟 110 年 APP 推動成果
16. Malicious Mobile Applications (6 Ways to Avoid Grayware & MalApps)

第 4 章、 資安活動紀事

企業資安實務研討會-台南場

活動時間：111.11.22(二) 13:25~16:30

活動議程：

時間	活動議程	講師
13:00~13:25	報到	
13:25~13:30	開場致詞	國立中山大學資訊安全研究中心 范俊逸 中心主任
13:30~14:00	TWCERT/CC服務 範疇及案例分享	TWCERT/CC 講師
14:00~14:10	中場休息	
14:10~15:10	IoT物聯網檢測介紹 與實務案例分享	中華資安國際股份有限公司 劉叡 經理
15:10~15:20	中場休息	
15:20~16:20	IoT物聯網安全 實務分享	安華聯網科技股份有限公司 洪光鈞 總經理
16:20~16:30	Q&A	TWCERT/CC 講師 資安講師

由 TWNIC、TWCERT/CC 主辦的企業資安實務研討會，11 月 22 日於台南沙崙國科會資安暨智慧科技研發大樓 1 樓 A122 第一會議室舉辦。

為增進南部企業之物聯網安全防護能力，研討會議題規劃以 IoT 物聯網為主題，特別邀請兩大企業分別為中華資安國際股份有限公司及安華聯網科技股份有限公司進行實務經驗分享。

首先，第一場由 TWCERT/CC 以「TWCERT/CC 服務範疇及案例分享」為開場主題，協助南部企業運用 TWCERT/CC 資源，處理資安危機。第二場由中華資安國際股份有限公司劉叡經理以「IoT 物聯網檢測介紹與實務案例分享」為主題進行探討。第三場活動主題「IoT 物聯網安全實務分享」，則由安華聯網科技股份有限公司洪光鈞總經理進行介紹與分享。藉由以上議題的討論和分享，提升南部企業物聯網資安意識及強化防禦措施。

本場研討會為實體與線上同步舉辦共 88 人與會，經由 TWCERT/CC 及兩位專業資安講師的案例探討與分享，使與會者進一步了解 TWCERT/CC 服務項目以及 IoT 相關資安防護措施，與會者對於本場研討會整體皆為滿意。

第 5 章、 國內外重要資安事件

5.1、資安趨勢

5.1.1、資安廠商發表研究報告，指出製造業營運科技系統主要資安問題與解決方案

資安廠商 Sectrio 日前發表研究報告，指出用於工業與製造業的營運科技系統（Operational Technology，OT）現今面臨的十大資安問題與解決方案。

Sectrio 日前公布的 2022 IoT 與 OT 資安長問卷調查（The IoT and OT CISO Peer Survey 2022）中發現，有 90% 的企業資安長表示，在過去 12 個月中其公司至少發生過一起重要駭侵攻擊事件；多數企業的製造與營運因而停止運作達到 4 天，造成平均 250 萬美元損失。

Sectrio 根據此問卷，分析出現今全球企業面臨的主要 OT 系統資安風險如下：

- 多數製造業的 OT 系統設備與作業系統版本過於老舊，且未曾或很少進行更新；
- OT 系統的管理與權責不明：多數公司的 IT 單位與系統擁有較明確的管理權責畫分，但製造業的 OT 系統普遍都有管理權責不明的問題，甚至只有

五分之一的製造業者設有資安長，負責 OT 系統的資安維運；

- OT 資產重要性未獲重視：超過 95% 公司承認未將 OT 系統資安維護視為公司重要例行工作；
- 日益提高的 IoT 僵屍網路與 DDoS 攻擊風險：許多駭侵者選擇製造業的 OT 系統當做布署僵屍網路的節點，或對企業發動 DDoS 攻擊。
- 許多 OT 系統直接曝露於公眾 Internet 上，與外網之間沒有強固的防火牆與其他資安設備隔開，等於對駭侵者大開方便之門。
- 使用可卸除式記憶媒體：許多製造業 OT 系統未對如 USB 隨身碟、記憶卡之類的可卸除式記憶裝置加強管制，大大提高遭到惡意軟體植入的機會。

近期製造業 OT 系統遭各式駭侵攻擊的案例愈來愈多，損失極為驚人；各製造業者應思考資安防護策略，提撥足夠人力與預算，加強 OT 系統的防護與人員訓練。

- 資料來源：
  1. The CISO Peer Survey 2022 Report
  2. OT Security Challenges and Solutions

5.1.2、72% 組織電腦系統仍含有 Log4Shell 漏洞

資安廠商 Tenable 近期發表研究報告指出，該公司掃瞄全球網路主機後發現，全球仍有高達 72% 的各型組織，其電腦系統仍含有約一年前發現的嚴重資安漏洞 Log4Shell（CVE-2021-44228）。

Tanable 指出，這次研究共在網路上進行 5 億次掃瞄測試，發現即使在去年發現 Log4j、Log4Shell 漏洞，全球各單位花費無數人力物力，針對該漏洞進行修補；甚至根據美國某聯邦資安單指出，該單位的資安團隊，花費高達 33,000 小時處理該漏洞，但截至 2022 年 10 月的掃瞄結果，仍有高達 72% 單位的主機並未修復該漏洞。

Tenable 表示，在這 72% 中，甚至還包括有 29% 過去曾經修復此漏洞的公司，但在這次掃瞄中再次遭到檢出，對於 Log4j、Log4Shell 漏洞不具防護力。

某些產業對此漏洞的應對處理整體狀況較佳，例如工程界（45%）、法律服務（38%）、金融服務（35%）、非營利組織（33%）、政府單位（30%）；但即使表現最好的工程界，也有一半以上的公司仍含有 Log4j、Log4Shell 漏洞。

在地域方面，各大洲的表現也有待加強。對 Log4j、Log4Shell 防護狀況最好的是北美洲，但完全防護率也僅有 28%，其次為歐洲、中東與非洲（27%）、亞洲 25%、拉丁美洲 21%。

在能夠部分防護 Log4j、Log4Shell 的企業比例方面，北美仍為最高（90%）、歐洲、中東與非洲為 85%、亞太地區亦為 85%、拉丁美洲為 81%。

有鑑於 Log4j、Log4Shell 的高危險性，以及廣為許多駭侵團體用於攻擊的現狀，建議各公私單位一定要加強對此漏洞的修補防護。

- 資料來源：
  1. Tenable: 72% of organizations remain vulnerable to Log4Shell
  2. 72% of organisations remain vulnerable to Log4j vulnerability

5.1.3、高達 75% 工業控制裝置未進行資安修補，暴露於高度駭侵風險中

Microsoft 近日指出，近 75% 製造業使用的物聯網系統（Internet of Things, IoT）、資訊科技（Information Technology，IT）系統與營運科技 (Operational Technology，OT）系統，沒有進行必須的資安漏洞修補，因此暴露在高度資安風險中。

Microsoft 在最新一期的「The Cyber Signal」資安專刊中指出，自其收集的每日 43 兆個資安相關信號資料，由全球 8500 位資安專家分析，得到以下必須注意的警訊數字：

- 製造業採用的知名大廠各種工控產品，含有已知高危險漏洞的數量，自 2020 年到 2022 年間增加了 78%；
- 在 Microsoft 客戶的 OT 網路中，有高達 75% 的常見工控設備未經修補，含有高危險漏洞。
- 超過 100 萬台連線 IoT 裝置仍在執行停止支援已久的 Boa 軟體。

報告中也指出，根據 IDC 的統計數字，至 2025 年時全球會有多達 416 億台 IoT 連網裝置，但這些裝置的資安漏洞能獲得更新的比例極低；近年來因為 IoT 與 OT 設備漏洞而造成的實體世界攻擊活動，包括 2021 年發生在美國的 Colonial 輸油管線遭勒贖攻擊、佛羅里達州供水設施遭攻擊投毒事件，以及今（2022）發生在烏克蘭的 Industroyer 斷電事件等。

此外，Microsoft 這份報告也統計了各種 IoT 惡意軟體的來源國排名（僅代表攻擊封包來源，不表示攻擊活動為該國政府支援或發動），前五名依序為中國（38%）、美國（19%）、印度（10%）、南韓（7%）、台灣（5%）。

建議各製造業者應強化自身的資安防護架構，包括將敏感或重要相關系統與外部網路隔開、加強可存取人員控管，並提高從業人員資安素養等。

- 資料來源：
  1. The Convergence of IT and Operational Technology: Cyber Risks to Critical Infrastructure on the Rise
  2. Severe vulnerabilities found in most industrial controllers

5.2、新興應用資安

5.2.1、Hyundai App 的錯誤，可導致駭侵者遠端開啟車門並發動車輛

資安廠商 Yuga Labs 旗下的研究人員，近期發現現代汽車（Hyundai）官方 App 中的漏洞，可導致駭侵者遠端開啟車門並發動車輛；此外，多家車廠使用的車輛管理系統 SiriusXM 也含有類似漏洞。

在 Hyundai 官方 App 漏洞方面，研究人員攔截 Hyundai 與 Hyundai 擁有的高級車品牌 Genesis 其官方 App MyHundai 與 MyGenesis 的網路封包內容後，可以找出其 API 呼叫方式；研究人員發現該 API 呼叫係以包括在 JSON 與 POST request 中的用呼 Email 地址來進行，而註冊使用 MyHyundai 與 MyGenesis，並不需要經過 Email 帳號驗證，因此研究人員可使用受害者的 email 位址，在後方加一個控制字元，即可註冊使用 myHyundai 來傳送指令，開啟並發動受害者的車輛。

在 SiriusXM 漏洞方面，SiriusXM 是個廣受各國大型車廠採用的車輛遙控管理平台，包括 Acura、BMW、Honda、Hyundai、Infinity、Jaguar、Land Rover、Lexus、Nissan、Subaru、Toyota 等車廠在內。

Yuga Labs 在分析 Nissan App 的流量後，發現可以透過特製的 HTTP 連線要求，加上車輛的唯一代碼 VIN (Vehicle Identification Number) 來遠端控制車輛，甚至從 SiriusXM 網站取得車主各項個資，包括姓名、電話、地址、帳單資訊等。

由於車輛的 VIN 往往就印在前擋風玻璃內側，自車外可輕易見到，在各大二手車銷售網站也可取得，因此造成車主與車輛極大的風險。

若用戶的車輛可經由 App 控制，且 VIN 碼可自擋風玻璃外部識別，建議先設法遮蔽 VIN 碼，或要求車廠提供車輛 App 更新，以解決此問題。

- 資料來源：
  1. Sam Curry @samwcyo
  2. Sam Curry @samwcyo More car hacking!
  3. Hyundai app bugs allowed hackers to remotely unlock, start cars
  4. Researchers find bugs allowing access, remote control of cars

5.2.2、微軟發現駭侵者透過 Telegram 攻擊加密貨幣投資業者

Microsoft 近日發表資安通報，指出該公司的資安研究團隊，近來發現多家加密貨幣投資業者，遭到某駭侵團體鎖定，透過這些業者用以和 VIP 投資人互動用的 Telegram 聊天群組發動攻擊。

Microsoft 指出，一個代號為 DEV-0139 的駭侵團體，加入多家加密貨幣投資業者設立的 Telegram 聊天群組，在其中鎖定駭侵攻擊的對象，假扮為其他加密貨幣投資機構的代表，宣稱提供更好的投資機會，以及更優惠的交易手續費；並在獲得目標對象的信任後，邀請其加入另一個 Telegram 聊天室，並且傳送一份內含惡意程式碼的兩大交易所 OKX 與 Huobi Global 手續費比較試算表給受害者。

在這份試算表中暗藏的惡意程式碼，會載入一個後門，讓駭侵者得以遠端存取用戶的電腦系統，並試圖竊取受害者的加密資產。

值得注意的是，Microsoft 指出在 Telegram 聊天室中的駭侵者，具備非常豐富的加密貨幣相關專業知識，因此能輕易取信於受害者。

雖然 Microsoft 沒有指名 DEV-0139 駭侵團體的身分，但另一家資安廠商 Volexity 對同一案例進行的分析，指出這個駭侵團體可能是 APT 團體 Lazarus。

Veloxity 指出，Lazarus 長期以來利用各種手法，針對加密貨幣產業與投資者進行駭侵攻擊，以竊取其數位資產；這次的攻擊也不例外。

鑑於透過社群工具進行的加密貨幣社交工程或釣魚攻擊愈來愈頻繁，加密貨幣投資者在這類管道與其他人互動時，應特別提高警覺，勿任意點按不明連結，也絕不能提供錢包相關密碼或復原短語，以免資金被竊。

- 資料來源：
  1. DEV-0139 launches targeted attacks against the cryptocurrency industry
  2. Microsoft: Hackers target cryptocurrency firms over Telegram

5.2.3、加密貨幣交易所 Gemini 570 萬用戶遭大規模釣魚攻擊，意圖騙取加密資產

加密貨幣交易所 Gemini 日前發布資安通報，指出該交易所用戶目前正遭到大規模釣魚攻擊，名單可能來自駭侵者自第三方取得的該交易所約有 570 萬名客戶的聯絡資訊。

Gemini 是在多個駭侵相關論壇中出現多篇試圖兜售號稱來自該交易所的客戶名單貼文後，對外發表該資安通報。在這些論壇貼文中試圖販售的用戶個資，包括 Gemini 用戶的電話號碼與 Email 地址等聯絡資訊。

據資安媒體 BleepingComputer 指出，早在 2022 年 9 月起，就有人在駭侵相關論壇上出售竊取自 Gemini 交易所的用戶資訊；當時的貼文者開價 30 枚比特幣，以目前的比特幣價格，約合 520,000 美元。

而在 10 月與 11 月時，陸續又有不同 ID 的貼文，試圖出售來自 Gemini 與其他加密貨幣交易所的用戶個資；不過也有貼文承認所販售的個資，在電話部分並不包括中間三碼在內。

資安專家表示，駭侵者針對加密貨幣交易所的用戶發動釣魚攻擊，其目的明顯就是要竊取用戶存在數位錢包中的資金；典型的攻擊方式就是以各種理由，如以巨額獎勵誘惑，或以停權威脅用戶，誘使用戶開啟信件中帶有惡

意軟體的夾檔或連結，在用戶的電腦中植入惡意軟體，接著再竊取用戶數位錢包內的加密貨幣等資產。

鑑於加密貨幣交易所屢傳各類資安事件，建議用戶除了應啟用二階段登入驗證，保護自己在交易所的帳號安全外，也應將數位資產存在離線冷錢包內；勿輕率點按 Email 中的各種不明連結與夾檔，以防數位資產遭到竊取，蒙受財務損失。

- 資料來源：
  1. Protecting Our Customers From Phishing Campaigns
  2. Hackers leak personal info allegedly stolen from 5.7M Gemini users

5.3、國際政府組織資安資訊

5.3.1、全新 CryWiper 資料刪除惡意軟體，針對俄羅斯公務機關發動攻擊

資安廠商 Kaspersky 旗下的研究人員，近來發現一個過去未曾記錄的全新資料刪除惡意軟體 CryWiper，正在針對俄羅斯境內各地區的市長辦公室和法院發動攻擊。

Kaspersky 指出，該公司是在今（2022）年秋天發現 CryWiper 布署的未知木馬惡意軟體，針對俄羅斯境內的公家單位發動攻擊；而據俄羅斯當地媒體指出，受到惡意軟體攻擊的公務單位，以司法單位與各地市長辦公室為主。

Kaspersky 分析指出，CryWiper 會假扮為勒贖軟體，實際上其惡意程式碼會刪除受害主機中的資料。其程式碼是 64 位元 Windows 可執行檔，名為「browserupdate.exe，執行後會在受害主機中設立排程，每 5 分鐘就自我執行一次，並在每次執行時與控制伺服器連線，收取執行或不執行的命令。

一旦收到執行的命令，CryWiper 會停止 MySQL、MS SQL 資料庫伺服器、MS Exchange email 伺服器、MS Active Directory 網頁伺服器等重要系統的執行，解除資料鎖定狀態，然後開始刪除受害主機上的資料。

CryWiper 不僅會刪除受害主機上的主要資料，也會刪除 shadow copy，以防止資料被輕鬆復原；另外 CryWiper 也會竄改 Windows 登錄檔，以防止 RDP 連線，阻止 IT 人員透過遠端遙控方式恢復資料。

最後，CryWiper 會將所有副檔名為 .exe、.dll、.lnk、.sys、.msi 與自身的 .cry 都加以破壞，但是不破壞系統、Windows 與啟動資料夾，讓電腦仍能啟動，看起來未被完全破壞。

建議各公私單位應強化人員資安培訓，勿點按不明連接並開啟不明檔案；重要系統也應做好異地備援措施，以在遭到攻擊時能迅速復原系統與資料。

- 資料來源：
  1. New CryWiper data wiper targets Russian courts, mayor’s offices
  2. Новый троянец CryWiper прикидывается шифровальщиком

5.3.2、駭侵者透過全新 MirrorStealer 惡意軟體，鎖定日本政治人物發動攻擊

資安廠商 ESET 發現一個名為「MirrorFace」的駭侵團體，自 2022 年 7 月起，利用一個過去未曾發現的惡意軟體「MirrorStealer」，針對特定日本政治人物進行駭侵攻擊。

ESET 的研究人員指出，這場駭侵攻擊活動始於 2022 年 7 月，正好是日本舉行國會大選的數周之前；涉嫌發動攻擊的駭侵團體疑似是 MirrorFace。

ESET 在報告中指出，MirrorFace 針對特定日本政治實體與人物，首先以夾帶有惡意軟體的釣魚信件，發送給特定目標，要求他們開啟信件中的 RAR 檔案，將解壓縮後得到的影片檔，分享到自己所有的社群媒體頻道中；而在 RAR 檔案解壓縮後，就會出現含有 MirrorStealer 惡意軟體的 .exe 檔。

遭到攻擊的對象一旦開啟該 .exe 檔，就會被安裝一個名為 LODEINFO 的後門惡意軟體；LODEINFO 可用於偷偷擷取螢幕畫面、記錄鍵盤輸入、停止某些程序運作、匯出檔案、執行各種指令與檔案等。

而在這波攻擊行動中，LODEINFO 實際竊取的是受害日本政治實體與人物所有電腦中，瀏覽器與 Email 應用程式內儲存的各種登入資訊以及 cookie；取得這些資訊後，即會將這些資訊傳送到駭侵者設立的控制伺服器。

駭侵者目前大多仍透過內含惡意夾檔的釣魚郵件來進行駭侵攻擊，因此各關鍵公私單位人員，應避免任意開啟郵件夾檔；儘可能利用 Web Mail 在遠端預覽夾檔內容，如有可疑檔案，應即通報資安單位調查。

- 資料來源：
  1. Unmasking MirrorFace: Operation LiberalFace targeting Japanese political entities
  2. Hackers target Japanese politicians with new MirrorStealer malware

5.3.3、駭侵者利用植入木馬的 Windows 10 安裝程式，駭入烏克蘭政府所屬網路

資安廠商 Mandiant 日前發表研究報告，指出該公司發現有駭侵團體透過植入惡意軟體的 Windows 10 安裝 ISO 檔，攻擊烏克蘭政府所屬單位，入侵其內部網路系統。

據 Mandiant 的報告指出，這波攻擊係透過 P2P 檔案分享網路 BitTorrent 的網站進行；駭侵者將木馬惡意軟體植入 Windows 10 安裝光碟映像檔，藉以發動供應鏈攻擊。

Mandiant 將這波攻擊行動代號命名為「UNC4166」。該公司在分析烏克蘭政府受到攻擊的部分單位內網時，發現被植入的木馬主要以竊取機密資訊為主，傳送到駭侵者控制伺服器的負訊，並未含有可用以竊取財物的資訊，也不含任何勒贖工具或加密貨幣挖礦程式。

Mandiant 說，駭侵者在初步入侵受害系統後，隨即進一步布署多種惡意後門 Stowaway、Beacon、Sparepart 等，以便讓駭侵者控制受駭系統、執行指令與程式碼、傳送檔案、竊取資訊如登入帳密和鍵盤輸入等。

Mandiant 也發現一些在 2022 年 7 月預先排程好的工作，以便透過 PowerShell 取得駭侵者下達的進一步攻擊指令。

Mandiant 在報告中指出，這次烏克蘭政府受到攻擊的單位，過去也曾遭到 APT 駭侵團體 APT28 的攻擊。

建議擁有機敏資訊的各公私單位或個人，在安裝軟體時務必循正規管道，使用經驗證安全性可靠的正版軟體，切勿透過 P2P 或社群平台連結安裝來路不明的盜版軟體或所謂破解工具、註冊機，以免遭到植入惡意軟體。

- 資料來源：
  1. Trojanized Windows 10 Operating System Installers Targeted Ukrainian Government
  2. Ukrainian govt networks breached via trojanized Windows 10 installers

5.4、社群媒體資安近況

5.4.1、Android 惡意軟體感染 30 萬台設備並竊取用戶 Facebook 帳號

資安廠商 Zimperium 近日發表研究報告，指出該公司發現一個已感染 30 萬台 Android 裝置的惡意軟體，自 2018 年就開始竊取受害用戶的 Facebook 帳號登入資訊。

根據 Zimperium 的觀察，這個名為「Schoolyard Bully」的木馬惡意軟體，藏身在多個上架到 Google Play Store 的閱讀與教育類應用程式中，受害者分布達全球 71 國，但主要的攻擊對象是越南境內的 Android 用戶。

用戶一旦安裝了含有 Schoolyard Bully 的惡意 Addroid 軟體，其 Facebook 登入資訊（Email 地址與密碼）、帳號 ID、用戶名稱、裝置 RAM、裝置 API 等資訊就會遭竊。該木馬會以 WebView 開啟一個真正的 Facebook 登入頁面，但在其中植入惡意 JavaScript 程式碼以攔截用戶輸入的資訊。

Zimperium 也說，由於 Schoolyard Bully 使用的是系統內建程式庫來進行資料竊取，因此較不易遭到手機上安裝的防毒防駭軟體發現。

Zimperium 指出，該公司一共發現有 37 個 Android App 內含 Schoolyard Bully 木馬；雖然在通報後，相關 App 都已經自 Google Play Store 中下架，但 Zimperium 警告這些 App 仍大量出現在許多第三方 Android App Store 中，因

此仍可能繼續傳布，造成更多人受害。

建議 Android 用戶除了避免在第三方或不明來源處安裝任何 App 外，即使在官方的 Google Play Store 下載軟體，也應提高警覺，仔細閱讀評價與用戶意見反應。

- 資料來源：
  1. Schoolyard Bully Trojan Facebook Credential Stealer
  2. Android malware infected 300,000 devices to steal Facebook accounts

5.4.2、Elon Musk 的 Twitter 追蹤者遭鎖定進行加密貨幣贈送詐騙攻擊

資安媒體 BleepingComuter 日前發現 Twitter 上有惡意帳號，假冒科技界名人 Elon Musk 之名，針對 Elon Musk 的新 Twitter 追蹤者發動加密貨幣詐騙攻擊。

該詐騙活動的手法，是利用一個使用 Twitter 圖示當做頭像的帳號，先將新近開始追蹤 Elon Musk Twitter 帳號的用戶，加入一個名為「Deal of the Year」的 List 中，該 List 在該文撰稿時，內有 155 個 Twitter 用戶。

在該 List 的頁面上，放了一張偽造的圖片，圖片中盜用 Elon Musk 的頭像與 Twitter 帳號發表假推文，內容詐稱 Elon Musk 將選擇 1000 名追蹤者參加「史上規模最大的加密貨幣贈送活動」，並放置一個名為「freedomgiveaway.net」，看起來似乎是正常網站的網址。

點入該網址便會進入駭侵者設立的詐騙網站，網站內有 Elon Musk 的照片，然後會要求用戶回答一些關於 Elon Musk 旗下企業如 Tesla、SpaceX、StarLink 與 Elon Musk 本人相關的一些問題。不論答對答錯，用戶都會被導向到一處顯示一個比特幣錢包位址的畫面；用戶如果想獲得 5000 枚比特幣的大獎，就必須先存入 0.02 到 1 枚比特幣到畫面上的網址；存入比特幣後，用戶將可獲得 5 倍到 10 倍的比特幣獎金。

當然，類似的詐騙活動，結果都是存入資金的受害者，永遠拿不到所謂的高額獎金。

根據加密貨幣資安廠商 Group-IB 指出，這類加密貨幣詐騙使用的網域名稱數量，今年比去年暴增三倍之多。

BleepingComputer 指出，在該刊發現此一詐騙活動並撰文報導當時，詐騙者提供的比特幣錢包位址，尚無任何比特幣轉入記錄；但該刊認為仍有必要揭露這類詐騙活動。

建議加密貨幣投資者應對明顯不合理的高報酬活動提高警覺，勿任意匯款，也絕對不可透露自己的錢包密碼或復原短語，以免造成損失。

- 資料來源：
  1. Crypto giveaway scams continue to soar: the number of fake domains grows five-fold in H1 2022
  2. Elon Musk "Freedom Giveaway" crypto scam promoted via Twitter lists

5.5、行動裝置資安訊息

5.5.1、Android 2022 年 12 月資安更新，共修復 81 個資安漏洞

Google 近日釋出 2022 年 12 月的 Android 行動作業系統資安更新，修復多達 81 個資安漏洞；其中有一個嚴重漏洞 CVE-2022-20472，駭侵者可透過此漏洞，經由藍牙連線，無需任何權限即可遠端執行任意程式碼。

這次 Android 資安更新包更新的所有漏洞中，含有以下 4 個嚴重 (Critical) 等級漏洞：

- CVE-2022-20472：存於 Android Framework 的遠端執行任意程式碼漏洞，影響的 Android 版本為 Android 10 到 13；
- CVE-2022-20473：存於 Android Framework 的遠端執行任意程式碼漏洞，影響的 Android 版本為 Android 10 到 13；
- CVE-2022-20411：存於 Android System 的遠端執行任意程式碼漏洞，影響的 Android 版本為 Android 10 到 13；
- CVE-2022-20498：存於 Android System 的資訊外洩漏洞，影響的

Android 版本為 Android 10 到 13。

其他獲得修復的 Android 資安漏洞類型，包括執行權限提升、遠端執行任意程式碼、資訊洩漏，以及分散式阻斷服務（Denial of Service, DoS）。

資安專家指出，在 Android 系統上的嚴重執行權限提升漏洞，可讓惡意軟體先以較低權限入侵裝置，然後再伺機利用該漏洞提升執行權限，接著載入更具危險性的惡意程式碼酬載，不可不防。

由於 Android 更新通常必須經由裝置原廠提供，無法直接套用 Google 推出的資安更新，因此用戶需注意原廠更新訊息；原廠可能不再支援過於老舊的裝置，應考慮更換為新機種。

- 資料來源：
  1. Android 安全公告 - 2022 年 12 月
  2. Android December 2022 security updates fix 81 vulnerabilities

5.5.2、多家企業所屬的 Android 軟體憑證遭駭侵者用於簽署惡意 App

Google 資安研究團隊發現，有多個由 Android OEM 設備廠商使用，用來進行 Android 軟體數位簽章的憑證平台，遭到駭侵者利用於簽署內含惡意程式碼的 Android App。

OEM Android 設備廠商使用平台憑證來簽署位於裝置核心 ROM 映像檔中的 Android 作業系統程式碼與相關 App，並給予這些體較高的執行權限，例如撥打、轉接或掛斷電話、安裝或移除程式套件、收集裝置資訊等較敏感的操作。

Google Android 資安團隊的一位資安專家指出，一旦有任何內含惡意軟體的程式碼使用該平台憑證來進行簽署，即可取得相同的高執行權限；目前觀察到有不少惡意軟體程式套件都使用了來自 Samsung、LG、MediaTek 三家 Android OEM 廠商憑證平台來簽署，因此內含來自這些平台的 SHA 256 雜湊和數位簽章。

濫用這些憑證簽署平台的惡意軟體，包括背景廣告木馬、資訊竊取工具、進階惡意軟體酬載布署工具等。

目前無法得知這些平台的憑證簽署平台，為何會外洩而讓駭侵者得以濫

用，目前仍不得而知；雖然 Google 已經通知這些簽署平台遭到濫用的廠商，要求廠商進行應對，並且調查遭濫用的原因，但據資安專業媒體 BleepingComputer 報導指出，Samsung 的軟體憑證簽署平台，仍可繼續用於核發憑證。

Google 表示將在 Android 系統與 Google Play Store 中加強對這類濫用簽署機制的惡意軟體，用戶也應使用最新版本的 Android 系統，以獲得相關防護能力。

- 資料來源：
  1. Issue 100: Platform certificates used to sign malware
  2. Samsung, LG, Mediatek certificates compromised to sign Android malware

5.5.3、全新 Zombinder 平台可將惡意程式碼植入正版 Android 應用程式中

資安廠商 ThreatFabric 日前發表資安研究報告，指出該公司發現一個暗網上的平台 Zombinder，可讓駭侵者將惡意程式碼植入正版的 Android 應用程式中，再誘騙用戶安裝，以散布惡意軟體。

該公司是在追蹤近期一些散布惡意 Windows 與 Android 惡意軟體的攻擊活動中，發現了這個位在暗網內的惡意軟體平台。

ThreatFabric 發現的 Zombinder，是個可以將惡意程式碼包裝成 APK 檔，附加在原始正版的各種 Android 應用軟體內。該平台在 2022 年 3 月開始活動，近來愈來愈受駭侵社群界的歡迎，使用率愈來愈高。

ThreatFabric 指出，目前觀察到遭到植入的 Android 正版軟體，包括一個足球比賽實況串流 App、以及遭到竄改的 Instagram App。

ThreatFabric 說，這些遭到植入惡意程式碼的 App，由於真正的程式碼並未遭到刪改，因此運作起來就和正版 App 一樣正常，但由 Zombinder 植入了惡意程式碼的載入器；這段載入器程式碼會設法逃過防毒防駭軟體偵測，並在開啟後顯示個要求使用者同意載入外掛程式的畫面；用戶一旦不察而同意，即會載入惡意程式碼並於背景執行。

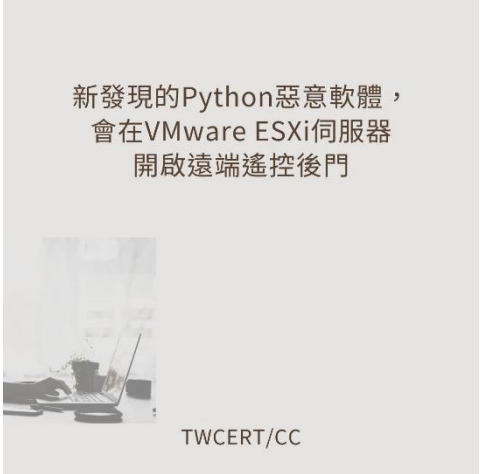
ThreatFabric 指出，目前發現的案例，都是植入 Ermac 惡意軟體，用於竊取用戶鍵盤輸入、發動覆疊畫面攻擊、竊取 Gmail 中的郵件、攔截二階段驗證代碼、竊取用戶加密貨幣錢包的復原短語等。

建議 Android 裝置用戶應避免下載安裝任何非來自官方 Google Play Store 的應用程式，特別是以檔案型式下載安裝的 APK 最為危險。

- 資料來源：
  1. Zombinder: new obfuscation service used by Ermac, now distributed next to desktop stealers
  2. New 'Zombinder' platform binds Android malware with legitimate apps

5.6、軟體系統資安議題

5.6.1、新發現的 Python 惡意軟體，會在 VMware ESXi 伺服器開啟遠端遙控後門



網通大廠 Juniper Networks 旗下的資安研究人員，日前發現一個過去未曾發現的 Python 後門，專門攻擊 VMware ESXi 伺服器，駭侵者能藉以在遭駭侵系統上遠端執行。

VMware ESXi 是一種廣受企業使用的虛擬化平台，可以高效率地運用主機的 CPU 與記憶體資源，同時執行多個伺服器。

Juniper Networks 發現的新後門，很可能是利用兩個十分老舊，存於 VMware ESXi OpenSLP 的漏洞 CVE-2019-5544 與 CVE-2020-3992 來發動攻擊；駭侵者在 /etc/ec.local.d/local.sh 這個指令檔中加上 7 行 Python 指令，啟動一個 web server，以接受來自駭侵者的密碼保護 POST 要求；這些要求可以攜帶以 base-64 編碼的惡意軟體酬載，或是在主機上啟用一個 reverse shell 連上駭侵者的控制伺服器。這種手法可以避免防火牆的阻擋。

Juniper 的資安研究人員，在實際攻擊案例中觀察到駭侵者利用此方式，更改 ESXi 的反向 http proxy 設定，使其可以遠端控制該主機，並發動進一步的駭侵攻擊。

Juniper 提供的暫時處理方案指出，VWware ESXi 伺服器的管理者，應立即檢查伺服器的 /etc/ec.local.d/local.sh 檔案中，是否多出報告中列出的 7 行惡意 Python 程式碼，如發現異常，應徹底檢查主機是否有可疑的設定變更。此外，也應設定 ESXi 主機僅能透過可信賴的主機進行連線。

- 資料來源：
  1. A Custom Python Backdoor for VMWare ESXi Servers
  2. New Python malware backdoors VMware ESXi servers for remote access

5.6.2、完全斷網的電腦內部資料，可能經由電源供應器放射的電磁波外洩

以色列 Ben-Gurion University 大學的資安研究人員發現一種稱為「COVID-BIT」的全新資料竊取方式；即使電腦完全未連接任何網路，其電源供應器對外放射的電磁波，也可能在近距離內遭到讀取而取得其內部資料。

研究人員指出，這類完全沒有連結網路連線的電腦，多半因為擔負重要任務，例如武器控制系統或重要關鍵基礎設施，或儲存高度機敏資訊，因而必須與內外網路隔絕。

由於無法直接透過網路入侵，傳統上要攻擊這類電腦，都必須經由可出入管制場所的人來實體接觸電腦；然而透過 COVID-BIT 即可遠端接收該電腦的內部資訊。

研究人員開發出一種惡意軟體，可控制受害電腦的 CPU 負載，並利用交換式電源供應應的運作原理，讓該電腦的電源供應器發出 0 - 48KHz 的低頻電磁波。

研究人員在報告中指出，運用 COVID-BIT，攻擊者可以在距離該電腦 2 公尺左右處，以行動裝置或其他設備加裝可隱藏在有線耳機中的微型天線，

收集受害電腦經由其電源供應器釋放的電磁波脈衝訊號，加以分析後解出資料。

報告也指出，運用這種方式，受害電腦將可以約 1000 bps 的傳輸速度對外傳送資料，傳送一個 10KB 大小的檔案，約需 80 秒；而一個 4096 位元組的 RSA 加密金鑰檔案，傳送時間最快僅需 4 秒；甚至可以透過這種方式遠端接收即時鍵盤輸入字元。

建議這類隔空透過電磁波接收資訊的攻擊方式，可以透過監控 CPU 不正常的頻率變化來防杜，此外也應加強電腦所在場所的電磁波屏蔽能力；由於這種攻擊方式仍需有人將惡意軟體植入隔離電腦中，因此加強人員進出管制監控亦屬必要。

- 資料來源：
  1. COVID-bit: Keep a Distance of (at least) 2m From My Air-Gap Computer!
  2. Air-gapped PCs vulnerable to data theft via power supply radiation

5.6.3、新型惡意軟體 Zerobot 利用多家連網裝置漏洞布署僵屍網路

網通設備大廠 Fortinet 旗下的資安研究團隊，最近發現一個名為 Zerobot 的全新惡意軟體，利用多家廠商的防火牆設備、路由器，以及網路攝影機等各型連網裝置合計 21 個漏洞進行攻擊，植入僵屍網路以發動分散式服務阻斷攻擊（Distributed Denial of Service, DDoS）。

Fortinet 在報告中指出，Zerobot 可「支援」的系統架構十分多樣化，從 i386、AMD64、ARM、ARM64 到 MIPS64、MIPSle、PPC64、PPC64le、RISC64、S390x 等不同架構與裝置，都可能受其攻擊。

Fortinet 的報告也說，Zerobot 利用上述聯網設備合計 21 個漏洞來攻擊上述裝置，並植入惡意軟體以組成龐大的僵屍網路。這 21 個漏洞中，有 8 個是在 2022 年發現的，其餘 13 個漏洞的發現期間在 2014 年到 2021 年之間。

在成功植入設備執行後，會與駭侵者設立的控制伺服器連線，上傳遭駭裝置的一些基本資料，同時等候命令發動 DDoS 攻擊。

據 Fortinet 指出，該公司的資安專家發現 Zerobot 後，也觀察到在 11 月的新版中，加入了許多額外組件與利用新發現漏洞的程式碼，顯示該惡意軟體的開發活動十分積極。

建議各型連網裝置的使用者或管理者，應隨時注意裝置是否提供資安更新或韌體升級，如有新版或更新應立即升級。過於老舊的產品可能已未列在原廠支援之列，若長期缺乏升級服務，應考慮設備汰舊換新。

- 資料來源：
  1. Zerobot – New Go-Based Botnet Campaign Targets Multiple Vulnerabilities
  2. New Zerobot malware has 21 exploits for BIG-IP, Zyxel, D-Link devices

5.6.4、哥倫比亞最大公共能源公司 EPM 遭 BlackCat 勒贖攻擊，部分營運與系統受阻

哥倫比亞最大的能源公司 Empresas Públicas de Medellín (EPM)，日前遭到一個名為 BlackCat/ALPHV 勒贖軟體的攻擊，導致該公司部分營運活動受阻，部分網路系統也因而離線，無法提供服務。

EPM 是哥倫比亞最大的綜合公共能源公司，供應水、電、燃油、瓦斯等重要民生工業物資，服務範圍廣達 123 個城鎮或地區。該公司隸屬於哥倫比亞 Medellin 自治區，2022 年至今的營業額高達 220 億美元。

該公司疑似於 2022 年 12 月 12 日遭到 BlackCat 的攻擊，其內部 IT 系統無法運作，且公司官網也無法正常連線；該公司於 12 月 13 日公告，要求近 4,000 名員工在家上班。

EMP 隨即對當地媒體證實遭到勒贖攻擊，並且發布資安通報，證實有部分裝置內的資料遭到加密鎖定，資料亦可能遭到竊取；該公司也提供客戶多種替代繳費方式，但該公司沒有透露駭侵攻擊行動本身的內容，也沒有公布駭侵者相關資訊。

資安專業媒體 BleepingComputer 於相關報導中指出，該媒體發現一個稱為 BlackCat/ALPHV 的勒贖團體，宣稱發起這起攻擊事件，並且在攻擊行動中竊得 EMP 的內部資料。

不過資安專家發現，BlackCat/APLHV 將竊得的資料上傳到一個未經妥善保護的網路主機，因此知道網址的任何人都可以存取該批資料；資安專家分析這批資料後，認為可能竊取自 40 台 EPM 的內部電腦。

建議列為關鍵基礎設施的公私營業者，特別是水電燃氣之類攸關國計民生的重要物資供應商，都必須加強各種資安防護能力，以防遭駭侵團體發動勒贖或其他攻擊，因而影響公司運作與重要物資的供應。

- 資料來源：
  1. Hackers piden plata a EPM para devolverle información robada
  2. Germán Fernández @1ZRR4H
  3. Colombian energy supplier EPM hit by BlackCat ransomware attack

5.7、軟硬體漏洞資訊

5.7.1、NVIDIA 釋出新版 GPU 驅動程式，修復多達 29 個資安漏洞

PC 顯示晶片大廠 NVIDIA 日前釋出新版 Windows 與 Linux 驅動程式，一共修復多達 29 個資安漏洞；這些漏洞形態包括任意程式碼執行與權限提升等，用戶應立即更新。

NVIDIA 在這波驅動程式更新中，一共修復 25 個 Windows 版驅動程式的各式漏洞，Linux 版則修復 4 個漏洞；其中兩個最為危險的漏洞如下：

- CVE-2022-34669：存於 Windows GPU driver 中的本機用戶模式濫用漏洞；未經授權的用戶可以存取或修改應用程式的重要檔案，導致任意程式碼執行、權限提升、資訊洩漏、資料竄改、發動 DoS 攻擊等。
- CVE-2022-34671：存於 Windows GPU driver 中的遠端用戶模式濫用漏洞；未經授權的一般用戶可用以越界寫入資料，導致任意程式碼執行、權限提升、資訊洩漏、資料竄改、發動 DoS 攻擊等。

CVE-34669 的 CVSS 危險程度評分高達 8.8 分（滿分為 10 分），對於已透過其他駭侵攻擊取得本機使用權的駭侵者和惡意軟體來說，可利用此方法存取 Windows 裝置，並且試圖提升執行權限。

CVE-34671 的 CVSS 危險程度評分為 8.5 分；雖然該漏洞透過網路遠端攻擊，但由於方法較為複雜，較不易成功，因此分數較低。

資安專家指出，由於 NVIDIA 顯示卡的市場佔有率相當高，因此有意發動攻擊的駭侵者，很容易找到可資攻擊的受害對象；如果你的電腦系統也使用 NVIDIA 顯示產品，應特別提高警覺。

建議 NVIDIA 顯示產品用戶，應立即透過系統更新工具更新到最新版本的驅動程式，以修復已知漏洞，避免駭侵者利用已知漏洞大規模發動攻擊。

- CVE 編號：CVE-2022-34669、CVE-2022-34671 等
- 影響產品/版本：參考 NVIDIA 資安通報上揭露之資訊。
- 解決方案：升級至最新版本 NVIDIA 驅動程式。

- 資料來源：
  1. Security Bulletin: NVIDIA GPU Display Driver - November 2022
  2. NVIDIA releases GPU driver update to fix 29 security flaws

5.7.2、Microsoft 推出 2022 年 12 月資安更新包 Patch Tuesday，共修復 49 個漏洞

Microsoft 日前推出 2022 年 12 月例行資安更新修補包「Patch Tuesday」，共修復 49 個資安漏洞，其中有 6 個是屬於「嚴重」(Critical) 危險程度的漏洞，另有 2 個 0-day 漏洞也獲得修復，其中有 1 個已知遭用於攻擊活動。

以漏洞類型來區分，這次修復的資安漏洞與分類如下：

- 權限提升漏洞：19 個；
- 資安防護功能略過漏洞：2 個；
- 遠端執行任意程式碼漏洞：23 個；
- 資訊洩露漏洞：3 個；
- 服務阻斷（Denial of Service）漏洞：3 個；
- 假冒詐騙漏洞：1 個。

上述在這次 Patch Tuesday 中獲得修補的漏洞，並未包括 25 個於 12 月 5 日推出資安修補包的 Microsoft Edge 瀏覽器。

本月修復的 2 個 0-day 漏洞如下：

- CVE-2022-44698：Windows SmartScreen 資安防護功能略過漏洞；該漏洞證實已遭駭侵者利用假造簽署的特製 JavaScript 用於攻擊活動之中；
- CVE-2022-44710：Microsoft DirectX Kernel 執行權限提升漏洞；駭侵者可利用此漏洞，將己身的執行權限提升到系統等級。。

- CVE 編號：CVE-2022-44698、CVE-2022-44710
- 解決方案：鑑於 Microsoft 軟體產品眾多，建議所有用戶與系統管理者應立即套用這次的 Patch Tuesday 資安更新，以免遭駭侵者利用已知的未修補漏洞發動攻擊，造成不必要的損失。

- 資料來源：
  1. Security Update Guide
  2. Microsoft December 2022 Patch Tuesday fixes 2 zero-days, 49 flaws

5.7.3、Apple 修復會攻擊 iPhone 等產品的 WebKit 全新 0-day 漏洞

Apple 近日在最新發表的 iOS、iPadOS、tvOS、macOS 等多種作業系統中，修復了一個存於 WebKit 組件中的 0-day 漏洞；該漏洞可讓駭侵者利用特製的網頁，在受駭系統上執行任意程式碼。

該漏洞的 CVE 編號為 CVE-2022-42856，是一種存於 Apple WebKit 網頁瀏覽器引擎中的形別混淆錯誤（Type Confusion），由 Google 旗下的 Threat Analysis Group 的資安研究人員發現。

研究人員指出，駭侵者可利用特製的網頁程式碼來誘發此錯誤，並在裝置上執行任意程式碼，以在作業系統中執行惡意軟體，或是進一步下載後續的惡意程式或監控軟體酬載，以發動進一步的攻擊。

這次 Apple 推出的 0-day 漏洞更新，置於新推出的 iOS/iPadOS 15.7.2、Safari 16.2、tvOS 16.2 與 macOS Ventura 13.1。Apple 也在更新說明中表示，該漏洞可能已遭駭侵者大規模用於攻擊活動。

受此漏洞影響的 Apple 裝置，包括 iPhone 6s 所有機型、iPhone 7 所有機型、iPhone SE (第 1 代）、iPad Pro 所有機型、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第 7 代。

建議使用上述機種機型的用戶，應立即透過作業系統更新，修補所有已知的資安漏洞，以防駭侵者利用尚未修補的漏洞趁虛而入。

- CVE 編號：CVE-2022-42856
- 影響產品/版本：iPhone 6s 所有機型、iPhone 7 所有機型、iPhone SE(第 1 代)、iPad Pro 所有機型、iPad Air 2 與後續機種、iPad 第 5 代與後續機種、iPad mini 4 與後續機種、iPod Touch 第 7 代。
- 解決方案：升級至 iOS/iPadOS 15.7.2、Safari 16.2、tvOS 16.2 與 macOS Ventura 13.1 與後續版本作業系統。

- 資料來源：
  1. About the security content of iOS 15.7.2 and iPadOS 15.7.2
  2. Apple security update fixes new iOS zero-day used to hack iPhones

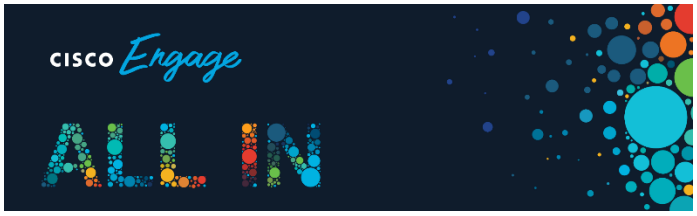
第 6 章、 資安研討會及活動

資安檢測工具實務	
活動時間	112 年 1/11，週三白天 9:30 ~16:30
活動地點	工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準
活動網站	https://college.itri.org.tw/Home/LessonData/4A4BFE93-06B1-4627-9E2C-82ACB794D51C
活動概要	 **主辦單位：工業技術研究院** 聯絡資訊：黃靖棻 02-23701111#304 上課地址/ 工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準!!!! 報名截止日：2023/01/09 課程介紹 數位經濟帶動產業朝跨世代、跨境、跨領域、 跨虛實等趨勢發展，根據世界經濟論壇(World Economic Forum， WEF)「109 年全球風險報告」，網路攻擊無論在影響(impact)風險或是可能性(likelihood)風險，已連續三年皆位於前 10 名之列，可見網路攻擊事件不但發生可能性高。本課程首先針對常見資安檢測方法進行說明，以現今企業資安健診常見的檢測與檢視作為主軸，介紹資安健診工作項目與如何搭配工具檢測是否存在已知安全漏洞或惡意程式，伺服器與使用者電腦的作業系統設定是否符合建議

	的組態基準，幫助網管人員可以自行在內部進行基礎的資安強化作業，針對缺失的地方進行改善。 課程特色/目標 本課程介紹常見用以偵測資安弱點、掃描惡意程式碼及分析電腦組態設定的資安檢測工具，學習如何安裝與使用的資安檢測工具，並學習設定後即時用於企業環境，講師以本身多年經驗分享可用於企業的實際做法。 課程對象：資訊人員、資安人員 課程注意事項：請學員自備筆電上課。

一鍵完成設備部署、資安、合規的實作秘笈 | In Taipei Apple Office	
活動時間	2023/01/12 (四) 2:00pm - 3:40pm
活動地點	Taipei Apple Office (松仁路 100 號 32F)
活動網站	https://jamf.kktix.cc/events/onetouch2023-1
活動概要	 **主辦單位：Jamf Software** 隨著蘋果設備的數量在企業環境內增加，如何有效管理設備，建立完善的資安環境對 IT 人員至關重要。這次活動將會分享一鍵完成設備部署、資安、合規的實作秘笈，誠摯的邀請您到 Apple 台北辦公室與我們共襄盛舉！ 主講人：Apple x Jamf 企業團隊 議程： 2:00pm - 2:40pm - 如何選擇最佳工作平台 - 跨國企業實戰經驗分享 2:40pm - 3:30pm - 快速與企業環境整合 目錄服務 單一登入 企業級網路

	VPN 設定 - 讓 Mac 設備變成公司的資安防護罩 企業行動裝置威脅防護 Threat Defense 網頁瀏覽過濾 Data Policy 擺脫 VPN，以 ZTNA 實現零信任網路訪問 3:30pm - 3:40pm Q&A

Cisco Engage Taipei 2023	
活動時間	2023 年 1 月 17 日，9:30~17:10 (8:30 開放報到)
活動地點	台北國際會議中心 (台北市信義區信義路五段 1 號)
活動網站	https://www.cisco.com/c/m/zh_tw/events/ciscoengage2023.html
活動概要	 **主辦單位：CISCO** 連結無盡未來 Vision for the Future Cisco Engage 以大型現場活動的形式為全球技術創新者提供新知與啟發，也是思科用戶與合作夥伴建立社群連結與知識交流的不二選擇。 本活動不僅是作為 IT 領域最優秀且最具智慧的人才互惠、學習的地，Cisco Engage 更能夠激發創造力，提供實用的專業知識來加速連結，以此為您的數位化未來賦能。

資訊安全工程師初級培訓班	
活動時間	112 年 2/7-2/8，週二三白天 9:30 ~12:30,13:30~16:30 ，共 2 天、計 12 小時
活動地點	工研院產業學院 產業人才訓練一部(台北)，實際地點依上課通知為準
活動網站	https://college.itri.org.tw/Home/LessonData/489FA646-8933-446D-BFA9-0F919B2BFCA4
活動概要	 **主辦單位：財團法人工業技術研究院 產業人才訓練一部(台北)** 課程介紹：配合我國產業升級需大量專業人才，為促進大學生能學以致用，特邀集企業共同規劃各項專業人才能力鑑定，並鼓勵在校學生報考，以培養企業所需人才。資訊安全領域涉獵範圍極廣，一般學校課程通常偏重管理或技術領域。而 iPAS 資訊安全工程師初級希望能培育對資訊安全有通才了解之學員，因此特別設立此課程對有意願考試之學員介紹資訊安全領域所應注意事項。 課程目標：瞭解 iPAS 能力鑑定中的資訊安全工程師初級考試內容，包含資訊安全管理與安全技術的相關基礎知識，上完課程後具備從事資安相關工作的入門水準。 合適對象：大三~大四學生、有意願或從事資安相關人員、想要考取 iPAS 能力鑑定資訊安全工程師初級者。

	報名方式： 線上報名：到工研院產業學院官網報名 課程洽詢：02-2370-1111 分機 609 或 306 黃小姐 報名截止日：2023/02/03

第 7 章、 TVN 漏洞公告

育碁數位科技 a+HRD - Server-Side Request Forgery (SSRF)	
TVN / CVE ID	TVN-202210019 / CVE-2022-39039
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD v6.8 & v7.0
問題描述	aEnrich a+HRD 特定 URL 參數未作恰當的過濾，遠端攻擊者不須權限，透過該漏洞任意發送 HTTP(s)請求，進行 Server-Side Request Forgery (SSRF)攻擊。
解決方法	聯繫育碁數位科技進行版本更新
公開日期	2022-12-14
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6792-c4a62-3.html

育碁數位科技 a+HRD - SQL Injection	
TVN / CVE ID	TVN-202210021 / CVE-2022-39041
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD v6.8 & v7.0
問題描述	aEnrich a+HRD 特定 API 參數未對使用者輸入進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法。
解決方法	聯繫育碁數位科技進行版本更新
公開日期	2022-12-14
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6794-35928-3.html

育碁數位科技 a+HRD - Improper Authentication	
TVN / CVE ID	TVN-202210022 / CVE-2022-39042
CVSS	9.8 (Critical)
影響產品	育碁數位科技 a+HRD v6.8 & v7.0
問題描述	aEnrich a+HRD 登入功能含有 Improper Authentication 漏洞，遠端攻擊者不須登入，即可透過此漏洞繞過登入驗證存取 API 功能。
解決方法	聯繫育碁數位科技進行版本更新
公開日期	2022-12-14
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6795-f7fe6-3.html

利凌企業 AH55B04 & AH55B08 DVR - Hard-coded Credentials	
TVN / CVE ID	TVN-202212007 / CVE-2022-47618
CVSS	9.8 (Critical)
影響產品	Merit LILIN AH55B04 DVR firmware ver 20220106 <= SVN# 7570 Merit LILIN AH55B08 DVR firmware ver 20220106 <= SVN# 7570
問題描述	利凌企業 AH55B04 & AH55B08 DVR firmware 使用 hard-coded 的管理者帳密，未經身份驗證的遠端攻擊者可以利用這組帳密登入管理頁面，並對系統進行任意操作或中斷服務。
解決方法	更新 Merit LILIN AH55B04 & AH55B08 DVR 至 SVN#8044(含)以上版本
公開日期	2022-12-29
相關連結	https://www.twcert.org.tw/newepaper/cp-151-6825-6691e-3.html

全球系統整合 GATEKEEPER 運維管理平台(GKP) - SQL Injection	
TVN / CVE ID	TVN-202211006 / CVE-2022-48229
CVSS	9.8 (Critical)
影響產品	聯繫全球系統整合詢問 GKP 受影響版本
問題描述	全球系統整合 GATEKEEPER 運維管理平台(GKP) 存有 SQL Injection 漏洞，特定功能參數未對使用者輸入進行驗證，遠端攻擊者不須權限，即可注入任意 SQL 語法讀取、修改及刪除資料庫。
解決方法	Update version to GKP-1.3.8，並已公告於全球系統整合官方網站之會員專區，亦可登入下載最新版本。
公開日期	2022-12-30
相關連結	**https://www.twcert.org.tw/newepaper/cp-151-6858-d5c35-3.html**

第 8 章、 2022 年 12 月份資安情資分享概況

本中心每日透過官方網站、電郵、電話等方式接收資安情資，以下為各項統計數據，分別為對外資安情資分享地區統計圖及資安情資分享類型統計圖。

分享地區統計圖為本中心所接獲之資安情資分享中，針對資安情資所屬地區之分享比率，如圖 1 所示；分享類型統計圖則為本中心所接獲的資安情資分享中，各項攻擊類型之比率，如圖 2 所示。

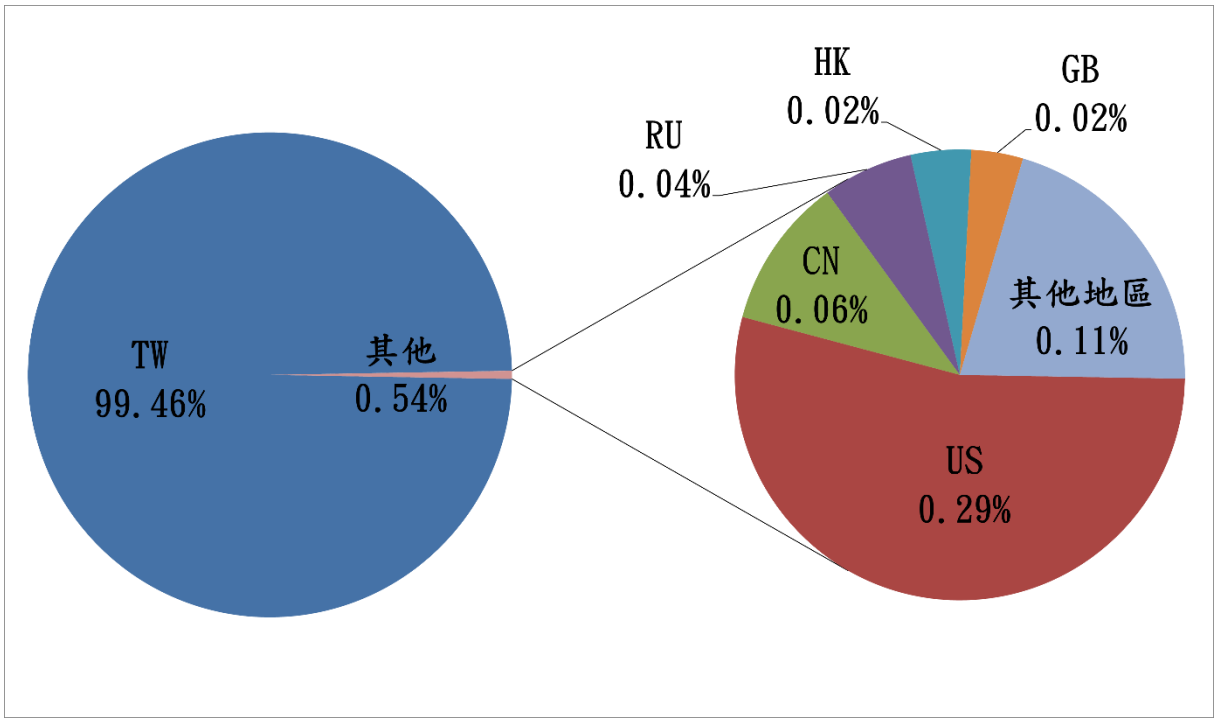


圖 1、分享地區統計圖

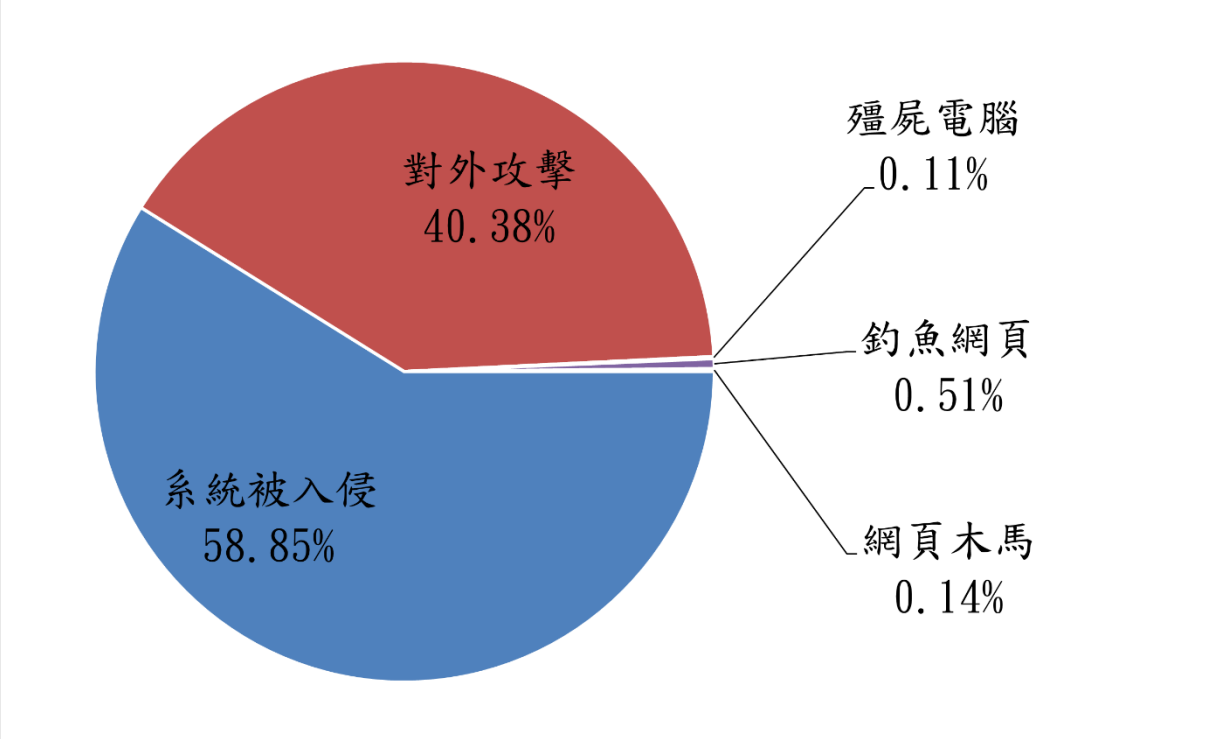


圖 2、分享類型統計圖

發行單位：**台灣電腦網路危機處理暨協調中心**
(Taiwan Computer Emergency Response Team / Coordination Center)

出刊日期：**2023 年 1 月 10 日**

編輯：**TWCERT/CC 團隊**

電子郵件：**twcert@cert.org.tw**

官網：**https://twcert.org.tw**

痞客邦：**https://twcert.pixnet.net/blog**

Facebook 粉絲專頁：**https://www.facebook.com/twcertcc**

Instagram：**https://www.instagram.com/twcertcc**

Twitter：**@TWCERTCC**