TLP:GREEN

國家資通安全研究院

威脅分析中心

電話: 02-2739-1000 傳真: 02-2733-1655

地址: 100057 臺北市中正區延平南路 143 號

電子郵件: ai2@nics.nat.gov.tw

# 資安聯防監控月報

# 114 年 12 月

**NICS-SOC2-2025-12**

TLP:GREEN

# 修訂紀錄

| 項次 | 版次 | 修訂日期 | 說明 |
|---|---|---|---|
| 1 | V1.0 | 115/1/19 | 新編 |
| 2 | | | |
| 3 | | | |

關於國家資通安全研究院(以下簡稱資安院)資安聯防監控月報：

資安院為協助政府機關提升資安聯防能力，彙整與綜合分析政府資安資訊與相關內外部情資，進行整體資安威脅趨勢與來源分析，分析結果提供政府機關與資安監控服務廠商做為資安環境布建防禦之參考。目前收容之資安聯防情資包含各公務機關資安監控中心(Security Operation Center, SOC)委外服務廠商所回傳之「資安監控單」與「情資分析單」等，本月報內容分為 3 部分：

1. 聯防監控綜覽：說明政府機關整體資安威脅趨勢與來源。
2. 威脅種類分析：藉由業務類別、資安責任等級及威脅種類之交叉分析，說明本月各類型機關主要威脅種類。
3. 聯防監控回饋建議：分析資安聯防情資觸發資安院中繼站黑名單威脅狀況、跨機關資安聯防情資來源 IP 及惡意威脅連線 IP 等，以不同面向提供多元資安情資，包含近期資安院資安研究、惡意電子郵件檢測分析、殭屍網路攻擊威脅、網路潛在資安風險及威脅指標檢測分析之資安情資，供政府機關與資安監控服務廠商參考。

依國際資安事件緊急應變小組(Forum of Incident Response and Security Teams, FIRST)所定義資訊分級協議(Traffic Light Protocol, TLP)[1]，本月報內容資訊屬 TLP:GREEN 資訊，機關僅可提供予協助執行聯防監控之所屬機關與資安監控服務廠商。

請參考國家資通安全通報應變網站，了解最新訊息，若需轉載、引用或對本月報資料有更多需求，請洽詢 ai2@nics.nat.gov.tw。

# 目　次

# 圖 目 次

# 表 目 次

# 1. 聯防監控綜覽

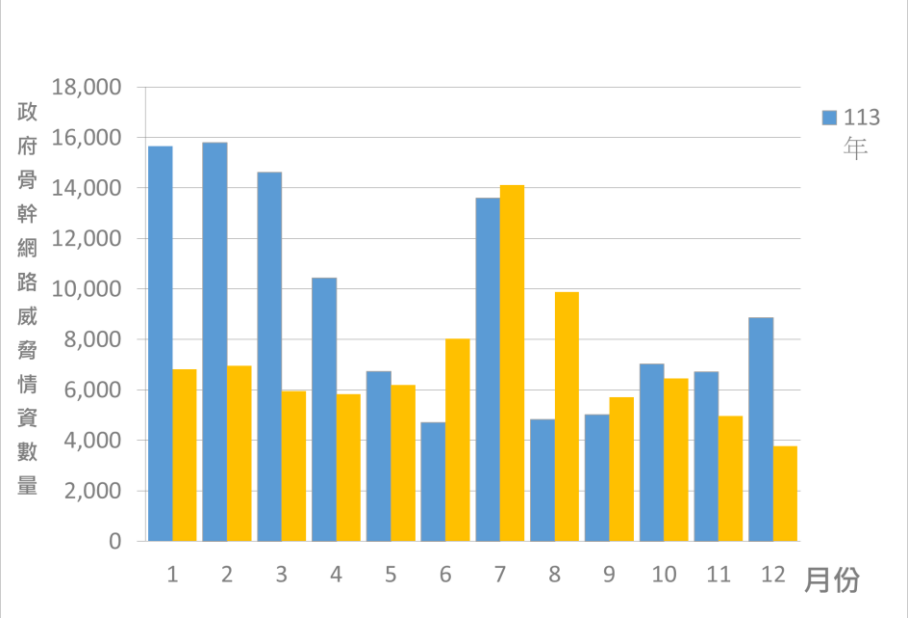
針對資安院聯防監控收集之資安聯防情資，進行整體資安威脅趨勢與來源分析。資安聯防情資係資安院之政府領域聯防監控作業規範所定義之「資安監控單」與「情資分析單」。本章針對 114 年 12 月(以下簡稱本月)資安聯防情資，進行整體威脅趨勢與國內外威脅來源分析。

## 1.1 整體威脅趨勢

本月蒐整政府機關之資安聯防情資共 61,580 件，統計近一年情資數量分布詳見圖 1。經分析上述資安聯防情資，可明確辨識之威脅種類，第 1 名為資訊蒐集類(45%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(21%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(18%)，大多為系統遭未經授權存取或取得系統/使用者權限。

依政府機關業務類別區分，本月事件單前 3 名分為綜合行政類之資訊蒐集類事件 11,510 件、綜合行政類之入侵攻擊類事件 8,273 件及教育科學文化類之資訊蒐集類事件 5,309 件。

依政府機關資安責任等級區分，本月事件單前 3 名分別為 B 級機關之資訊蒐集類事件 15,040 件、A 級機關之資訊蒐集類事件 12,705 件及 B 級機關之入侵攻擊類事件 8,403 件。



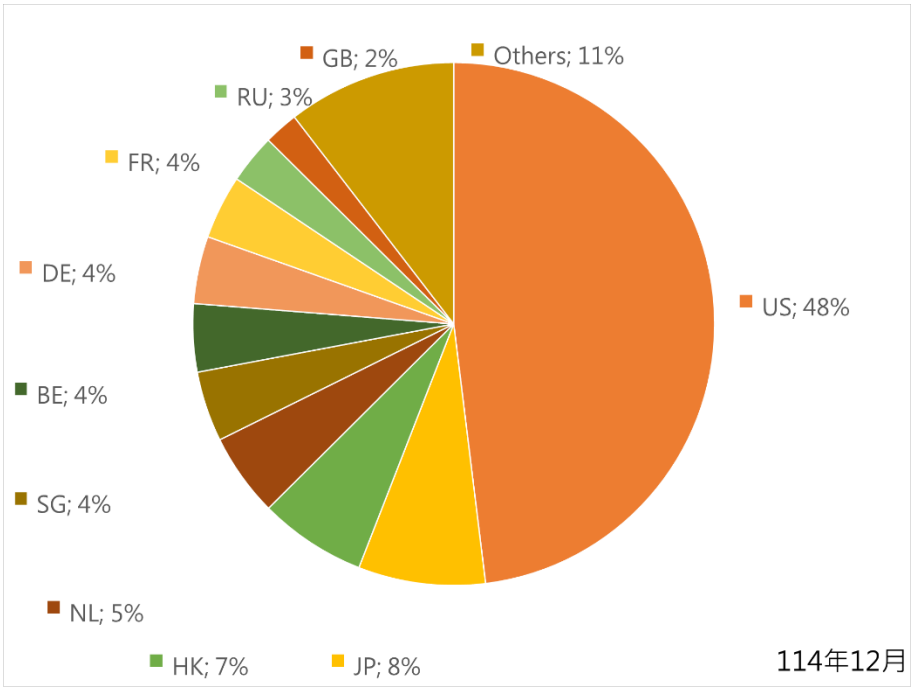

資料來源： 資安院整理

圖1 113 年 1 月至 114 年 12 月資安聯防情資分布趨勢

## 1.2 威脅來源分析

觀察整體資安聯防情資來源 IP，本月國外攻擊跳板來源前 3 名分別為美國(48%)、日本(8%)及香港(7%)，詳見圖 2。本月國外攻擊跳板來源國家觸發資安聯防情資前 3 名分別為「外部主機執行掃描探測攻擊」、「外對內防火牆大量阻擋案件」及「內部主機執行掃描探測攻擊」。

另外，與香港相關資安聯防情資還包含「疑似持續性攻擊行為」、「單一來源 IP 觸發大量 WAF 事件」及「外部主機執行弱點掃描攻擊」，比較過往情資，近期香港竄升為前 3 大主要攻擊跳板來源國家，建議協同資安監控服務廠商加強監控攻擊跳板來源。



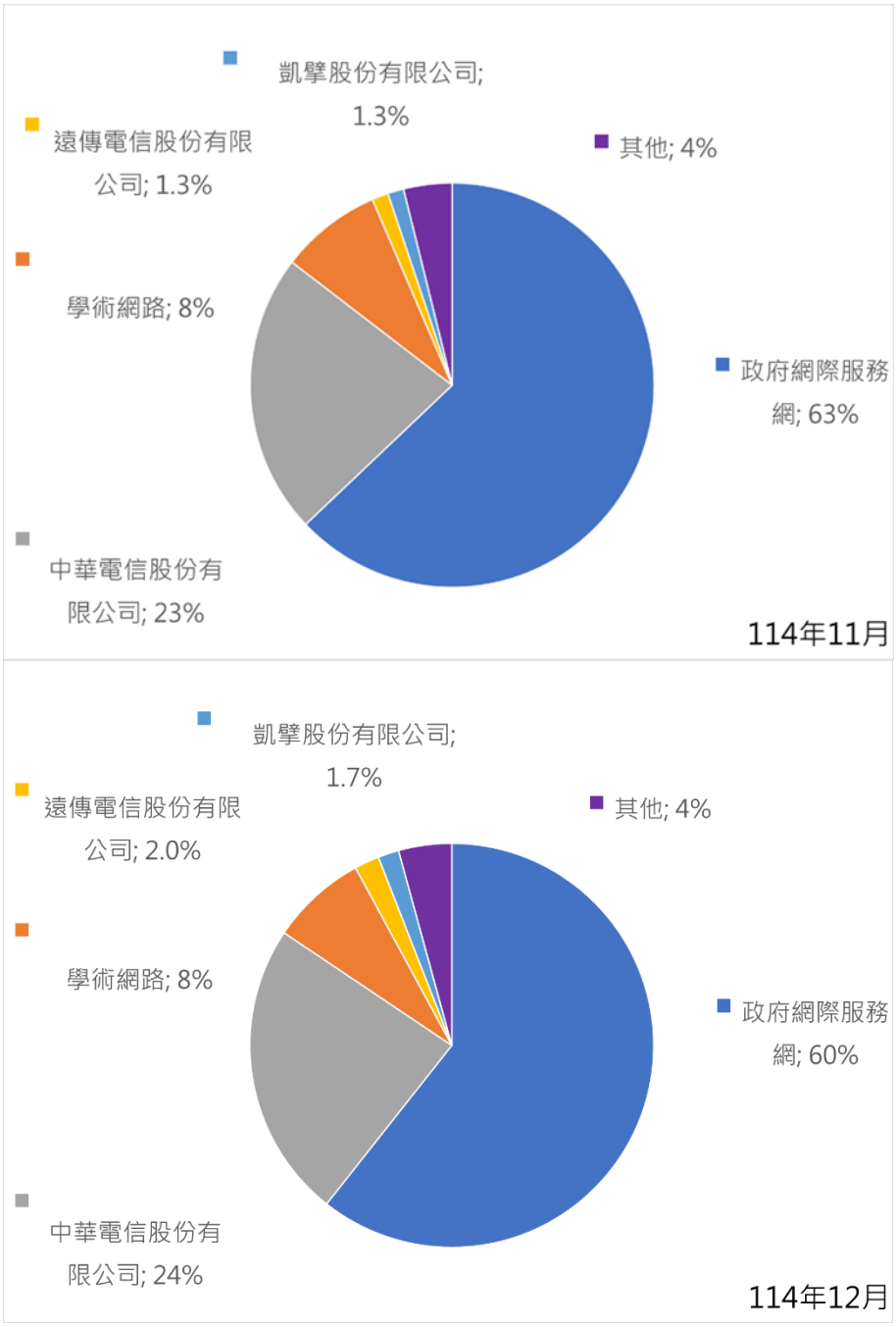

資料來源：資安院整理

圖2　資安聯防情資來源 IP 所屬國家分布

資安聯防情資來源 IP 屬於國內部分，來源大部分均為政府網際服務網(GSN)占 60%，其次為中華電信股份有限公司占 24%，以及學術網路占 8%，詳見圖 3。

來源為政府網際服務網(GSN)之資安聯防情資類別前 3 名分別為資訊蒐集類之「內部主機執行掃描探測攻擊」、資訊蒐集類之「內部主機違反防火牆政策」及惡意程式類之「內對內防火牆大量阻擋」。

來源為非政府網際服務網(GSN)之資安聯防情資類別前 3 名分別為資訊蒐集類之「外對內防火牆大量阻擋案件」、入侵攻擊類之「伺服器主機異常網域查詢行為」及資訊蒐集類之「外部主機執行掃描探測攻擊」。




資料來源：資安院整理

圖3　資安聯防情資國內來源 IP 所屬 ISP 分布[1]

[1] 部分學術網路 IP 依據使用單位之屬性，分別歸類至政府機關與學術單位。

## 1.3 資安訊息情報彙整

「資安訊息情報」係指最新之資安漏洞、攻擊活動及資安公告等重要訊息，根據近期內外部情資彙整資安訊息情報，做為各機關加強聯防監控使用，詳見表 1 至表 8。

表1　Fortinet FortiWeb 存在高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000641 |
| 情報摘要 | Fortinet FortiWeb 存在高風險安全漏洞，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現 Fortinet FortiWeb 存在作業系統指令注入(OS Command Injection)漏洞(CVE-2025-58034)。已取得管理權限之遠端攻擊者可注入任意作業系統指令並於伺服器上執行。該漏洞已遭駭客利用，請儘速確認並進行修補。 |
| 影響平台 | FortiWeb 8.0.0 至 8.0.1 版本<br>FortiWeb 7.6.0 至 7.6.5 版本<br>FortiWeb 7.4.0 至 7.4.10 版本<br>FortiWeb 7.2.0 至 7.2.11 版本<br>FortiWeb 7.0.0 至 7.0.11 版本 |
| 建議措施 | 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：<br>https://fortiguard.fortinet.com/psirt/FG-IR-25-513 |

資料來源：　資安院整理

表2　WordPress 擴充程式與網頁主題存在 6 個安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000651 |
| 情報摘要 | WordPress 擴充程式與網頁主題存在 6 個安全漏洞，請儘速確認並進行修補 |

| | |
|---|---|
| 內容說明 | 研究人員發現 WordPress 擴充程式與網頁主題存在 6 個高風險安全漏洞，請儘速確認並進行修補。1. Blubrry PowerPress 擴充程式存在任意檔案上傳(Arbitrary File Upload)漏洞，取得一般權限之遠端攻擊者可於受影響網頁伺服器上傳並執行網頁後門程式，進而達成遠端執行任意程式碼。2. FindAll Listing 與 Tiare Membership 擴充程式及 Tiger 網頁主題存在權限提升(Privilege Escalation)漏洞，未經身分鑑別之遠端攻擊可於註冊時指定管理者角色，進而利用漏洞取得網站管理員權限。3. FindAll Membership 擴充程式存在身分鑑別繞過(Authentication Bypass)漏洞，未經身分鑑別之遠端攻擊者於取得一般使用者帳號且能存取管理員電子郵件之情況下，以管理員身分登入系統。4. StreamTube Core 擴充程式存在任意使用者密碼變更(Arbitrary User Password Change)漏洞，未經身分鑑別之遠端攻擊者可任意變更網站使用者密碼，進而接管管理員帳號。WordPress 為常見網站架設系統，由於其擴充程式與網頁布景主題數量眾多，因此偶有出現嚴重漏洞情況，如本次警訊所列之幾項漏洞。建議若有使用 WordPress 系統時，除留意 WordPres 本身核心程式之更新資訊外，針對擴充程式網頁布景主題亦須關注，適時更新修補，此外亦建議評估所用之擴充程式網頁布景主題之必要性，如無需求，建議移除。 |
| 影響平台 | 詳見實際警訊內容 |
| 建議措施 | 詳見實際警訊內容 |

資料來源： 資安院整理

表3 研華科技 WISE-DeviceOn Server 存在高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000672 |
| 情報摘要 | 研華科技 WISE-DeviceOn Server 存在高風險安全漏洞，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現研華科技 WISE-DeviceOn Server 存在使用硬刻之加密金鑰(Use of Hard-coded Cryptographic Key)漏洞，未經身分鑑別之遠 |

| | |
|---|---|
| | 端攻擊者可自行製作 token 以偽冒任意 DeviceOn 帳號，進而取得完整控制權，請儘速確認並進行修補。 |
| 影響平台 | WISE-DeviceOn Server 5.3.12 版本 |
| 建議措施 | 請更新 WISE-DeviceOn Server 至 5.4(含)以後版本 |

資料來源： 資安院整理

表4 Fortinet 多項產品存在高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000673 |
| 情報摘要 | Fortinet 多項產品存在高風險安全漏洞(CVE-2025-59718 與 CVE-2025-59719)，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現 Fortinet 多項產品存在身分鑑別繞過(Authentication Bypass)漏洞，未經身分鑑別之遠端攻擊者可利用特製 SAML response message 繞過 FortiCloud SSO 登入之身分鑑別，請儘速確認並進行修補。 |
| 影響平台 | 詳見實際警訊內容 |
| 建議措施 | 官方已針對漏洞釋出修復更新，請參考官方說明進行更新，網址如下：<br>https://fortiguard.fortinet.com/psirt/FG-IR-25-647 |

資料來源： 資安院整理

表5 以 Chromium 為基礎之瀏覽器存在 5 個高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000674 |
| 情報摘要 | 以 Chromium 為基礎之瀏覽器存在 5 個高風險安全漏洞，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現 Google Chrome、Microsoft Edge、Vivaldi 及 Brave 等以 Chromium 為基礎之瀏覽器存在 5 個高風險安全漏洞，類型包含 |

| | |
|---|---|
| | 類型混淆(Type Confusion)漏洞、權限提升(Privilege Escalation)漏洞、使用釋放後記憶體(Use After Free)漏洞及不正確之類型轉換(Incorrect Type Conversion or Cast)漏洞，最嚴重可使未經身分鑑別之遠端攻擊者於使用者端執行任意程式碼，請儘速確認並進行修補。 |
| 影響平台 | 詳見實際警訊內容 |
| 建議措施 | 詳見實際警訊內容 |

資料來源： 資安院整理

表6 WordPress 擴充程式與網頁主題存在 10 個高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000681 |
| 情報摘要 | WordPress 擴充程式與網頁主題存在 10 個高風險安全漏洞，請儘速確認並進行修補 |
| 內容說明 | 未經身分鑑別之遠端攻擊者可利用此漏洞，誘使伺服器端 PHP 程式載入本機非預期檔案，並於伺服器端執行任意程式碼，請儘速確認並進行修補。 |
| 影響平台 | 詳見實際警訊內容 |
| 建議措施 | 詳見實際警訊內容 |

資料來源： 資安院整理

表7 WatchGuard Fireware OS 存在高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000691 |
| 情報摘要 | WatchGuard Fireware OS 存在高風險安全漏洞(CVE-2025-14733)，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現 WatchGuard Fireware OS 存在越界寫入(Out-of-Bounds Write)漏洞。當 Mobile User VPN 使用 IKEv2 協定，或 Branch Office VPN(BOVPN)使用 IKEv2 協定且設定為動態閘道時，未經身分鑑別 |

| | |
|---|---|
| | 之遠端攻擊者可透過傳送特製封包觸發記憶體越界寫入，進而造成服務異常，嚴重情況下可執行任意程式碼。該漏洞目前已遭駭客利用，請儘速確認並進行修補。 |
| 影響平台 | 詳見實際警訊內容 |
| 建議措施 | 詳見實際警訊內容 |

資料來源： 資安院整理

表8 7-Zip 存在高風險安全漏洞

| | |
|---|---|
| 警訊編號 | NICS-ANA-2025-0000692 |
| 情報摘要 | 7-Zip 存在高風險安全漏洞，請儘速確認並進行修補 |
| 內容說明 | 研究人員發現 7-Zip 存在連結追蹤(Link Following)漏洞。未經身分鑑別之本機端攻擊者可利用此漏洞寫入任意檔案。該漏洞目前已遭駭客利用，請儘速確認並進行修補。 |
| 影響平台 | 7-Zip 25.01(不含)以下版本 |
| 建議措施 | 更新 7-Zip 至 25.01(含)以上版本 |

資料來源： 資安院整理

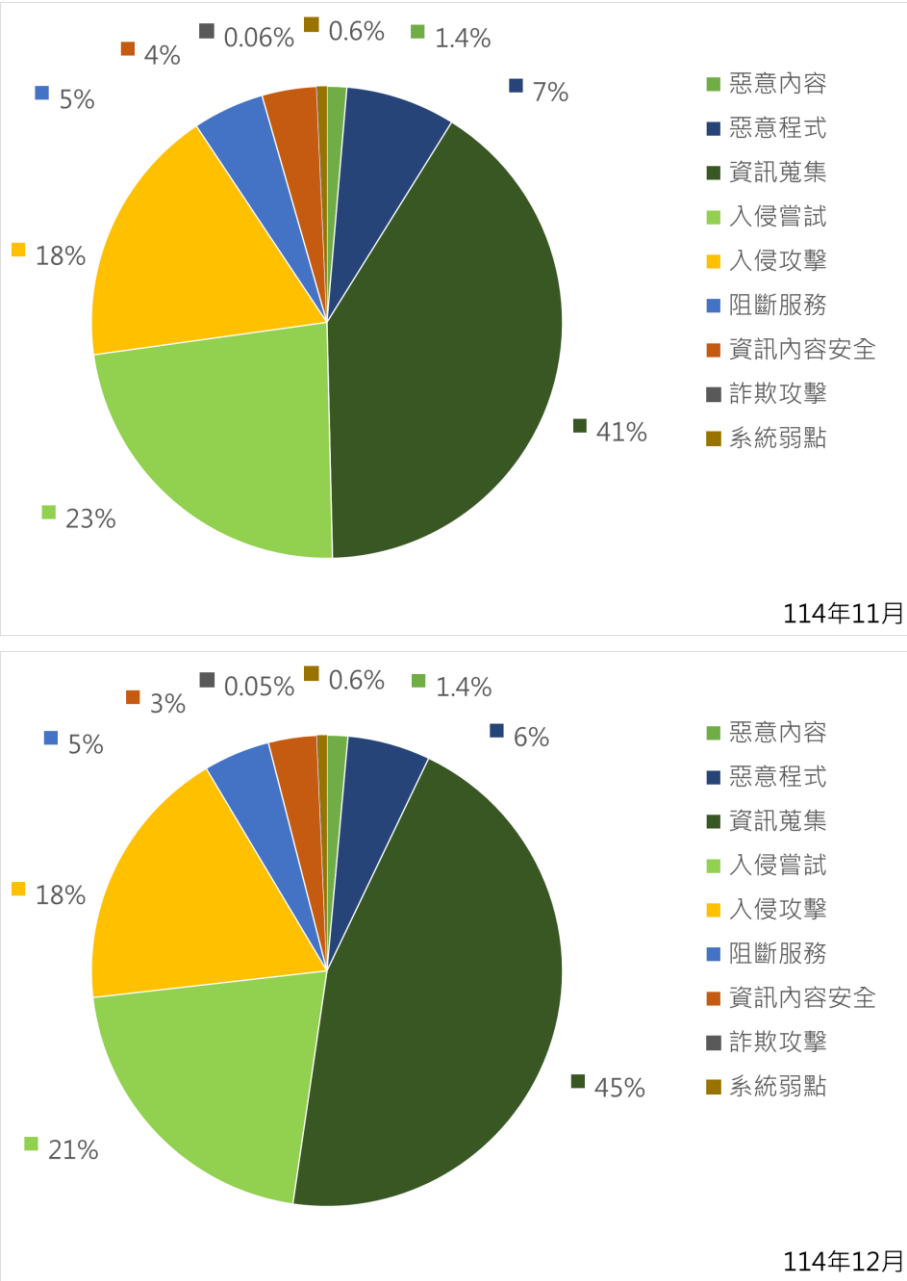
## 2. 威脅種類分析

根據本月資安聯防情資整體威脅種類進行各類別內容分析，並以業務類別、資安責任等級及威脅種類進行交叉分析，比較近 2 個月資安聯防情資變化量，分析各業務類別與資安責任等級現況。

### 2.1 整體威脅種類分析

本月整體資安聯防情資依照資安情資類別[2]統計可明確辨識之威脅種類，其中，第 1 名為資訊蒐集類(45%)，主要是透過掃描、探測及社交工程等攻擊手法取得資訊；其次為入侵嘗試類(21%)，主要係嘗試入侵未經授權的主機；以及入侵攻擊類(18%)，大多為系統遭未經授權存取或取得系統/使用者權限；各威脅種類比例詳見圖 4。以下彙整各資安聯防情資類別，主要影響機關業務類別與主要觸發威脅資訊詳見表 9。

[2]詳見附件 2：資安情資類別說明。




資料來源：資安院整理

圖4　資安聯防情資各類攻擊分布趨勢

表9　資安聯防情資類別、主要影響機關業務類別及觸發資訊彙整

| 編號 | 資安威脅類別 | 主要機關業務類別 | 主要觸發資訊 |
|---|---|---|---|
| 1 | 惡意內容 | 教育科學文化 | SPAM 設備發現有威脅郵件 |
| 2 | 惡意程式 | 教育科學文化 | 偵測到惡意程式活動 |
| 3 | 資訊蒐集 | 綜合行政 | 來源 IP 觸發多種未阻擋 IDS 事件 |
| 4 | 入侵嘗試 | 綜合行政 | 外部主機疑似對網站應用程式攻擊 |
| 5 | 入侵攻擊 | 綜合行政 | 已知中繼站 IP 連線 |
| 6 | 服務阻斷 | 經濟能源農業 | 網頁 HTTP 監控異常 |
| 7 | 資訊內容安全 | 綜合行政 | 非上班時間異動帳號及群組設定 |
| 8 | 詐欺攻擊 | 財政主計金融 | 電子郵件過濾 |
| 9 | 系統弱點 | ▪綜合行政<br>▪內政衛福勞動 | 漏洞攻擊行為偵測 |

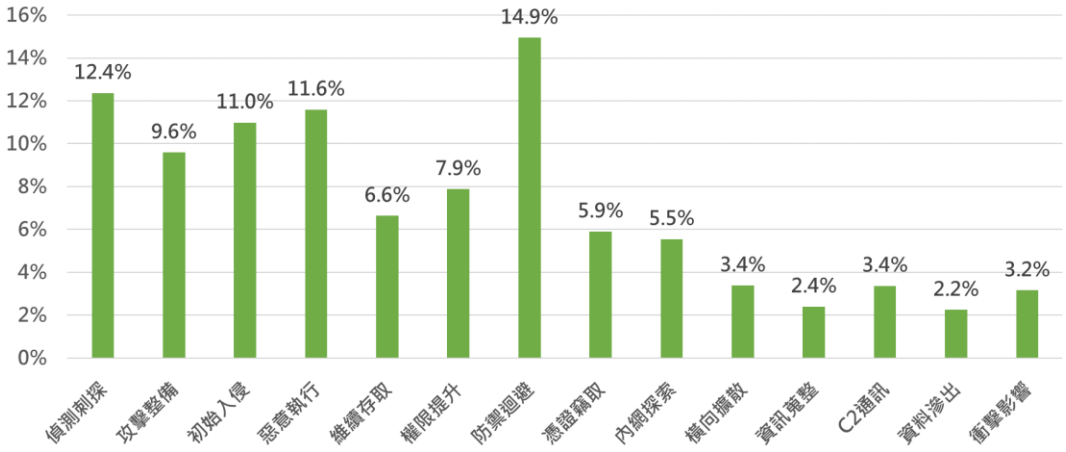
資料來源：資安院整理

## 2.2 整體 MITRE ATT&CK 威脅分析

Mitre ATT&CK 是一套針對真實攻擊行為所建構的對手戰術與技術知識庫，可用來分析攻擊者如何入侵與橫向移動。結合聯防監控所蒐集之情資，對應至 ATT&CK 框架，能系統性掌握政府機關常見的攻擊手法與風險熱點，做為資安強化策略之依據。

本月整體統計 MITRE ATT&CK 框架之戰術，其中，第 1 名為防禦迴避(14.9%)，大多為躲避安全機制，如禁用防毒軟體或混淆惡意程式碼；其次為偵測刺探(12.4%)，主要是收集目標資訊，如網域名稱、員工名單；以及惡意執行 (11.6%)，主要是在受駭系統上執行惡意程式或指令等；各戰術比例詳見圖 4，針對上述戰術彙整相關攻擊技術(Technique)前三名，詳見表 9，攻擊技術細節可參考 MITRE ATT&CK 官網[6]。

本月以防禦迴避為最常見戰術，攻擊者常透過關閉或清除指令紀錄，並以系統合法工具間接執行惡意命令，以規避監控，建議導入端點防護，強化指令紀錄稽核、限制高風險工具濫用，並落實特權帳號管理，以防範攻擊者規避偵測並抹除行為痕跡。




資料來源：資安院整理

圖5　資安聯防情資 MITRE ATT&CK 框架分布

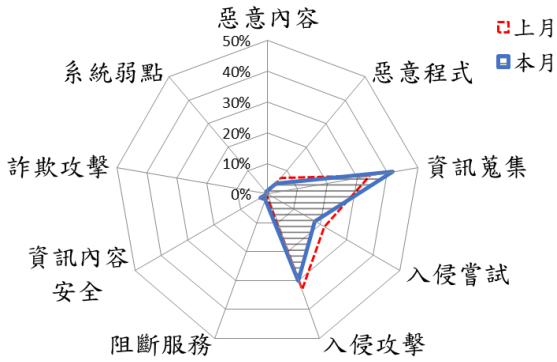
| 編號 | 資安威脅<br>類別 | 主要觸發攻擊技術 |
|---|---|---|
| 1 | 防禦迴避 | ▪ Impair Command History Logging<br>▪ Indirect Command Execution<br>▪ Clear Command History |
| 2 | 偵測刺探 | ▪ Scanning IP Blocks<br>▪ Active Scanning<br>▪ Vulnerability Scanning |
| 3 | 惡意執行 | ▪ Visual Basic<br>▪ PowerShell<br>▪ Python |

資料來源：　資安院整理

## 2.3 業務類別[3]與威脅種類交叉分析

針對政府機關業務類別與威脅種類進行交叉分析，以雷達圖呈現各威脅種類分布比，藉此了解各業務機關遭遇資安威脅種類分布情形，相關內容詳見表 10 至表 17。同時，將各威脅種類資安聯防情資經各業務類別機關數量平減為平均每 1 機關之數量，並與上月資訊進行比較，了解各業務類別機關遭遇資安威脅之增減情形，相關內容詳見表 18。

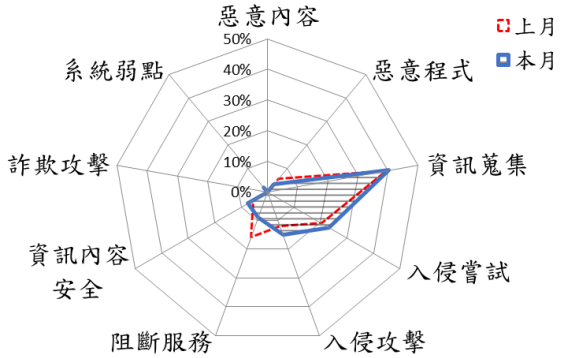
表10 綜合行政類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="3"> 
</td></tr>
<tr><td colspan="3">綜合行政類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td></tr>
<tr><td>本月</td><td>4.3</td><td rowspan="2">↗</td></tr>
<tr><td>上月</td><td>3.7</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">資訊蒐集</td><td>來源 IP 觸發多種未阻擋 IDS 事件</td></tr>
<tr><td>2</td><td colspan="2">入侵攻擊</td><td>偵測可疑 IP</td></tr>
</table>

資料來源：資安院整理

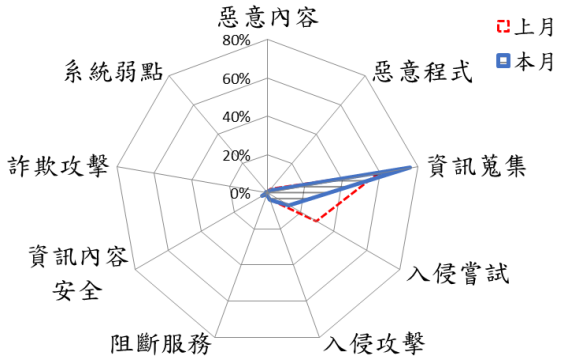
[3] 詳見附件 1：公務機關業務類別與資安責任等級說明。

表11 內政衛福勞動類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">內政衛福勞動類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>45.6</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>50.8</td></tr>
<tr><td>編號</td><td>主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td>資訊蒐集</td><td>內部主機對外進行遠端維運工具連線</td></tr>
<tr><td>2</td><td>入侵嘗試</td><td>核心系統非上班時間登入</td></tr>
</table>

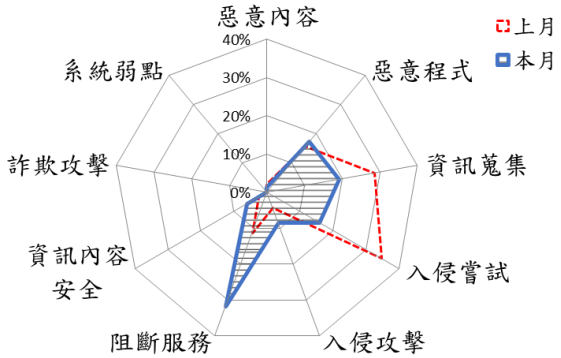
資料來源：資安院整理

表12 外交國防法務類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">外交國防法務類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>26.8</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>24.3</td></tr>
<tr><td>編號</td><td>主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td>資訊蒐集</td><td>來源 IP 觸發多種未阻擋 IDS 事件</td></tr>
</table>

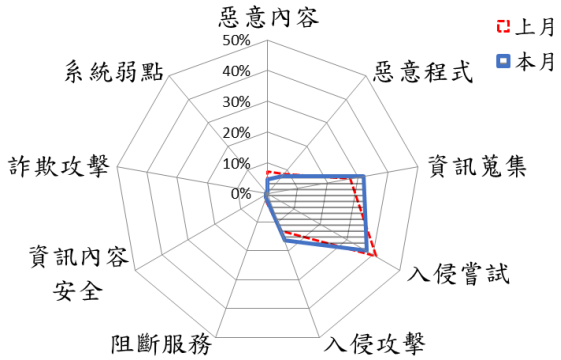
資料來源：資安院整理

表13 交通環境資源類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">交通環境資源類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>18.5</td><td rowspan="2">  </td></tr>
<tr><td>上月</td><td>27.1</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">服務阻斷</td><td>網頁 HTTP 監控異常</td></tr>
</table>

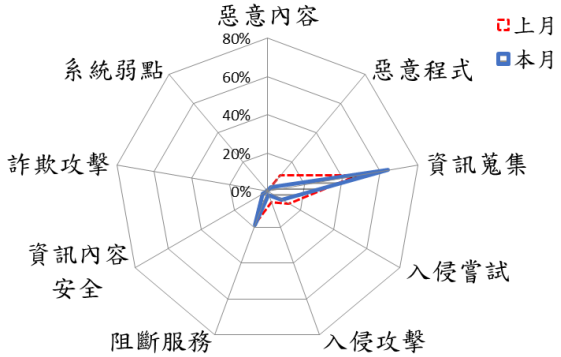
資料來源：資安院整理

表14 財政主計金融類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">財政主計金融類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>63.9</td><td rowspan="2">  </td></tr>
<tr><td>上月</td><td>52.0</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">入侵嘗試</td><td>使用者登入 SSLVPN 失敗通知</td></tr>
</table>

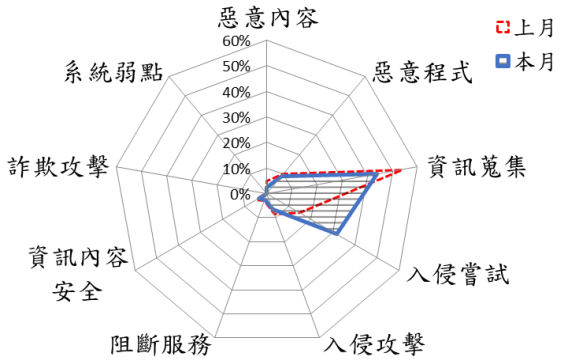
資料來源：資安院整理

表15 經濟能源農業類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">經濟能源農業類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>38.4</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>58.9</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">資訊蒐集</td><td>來源 IP 觸發多種已阻擋 IDS 事件</td></tr>
</table>

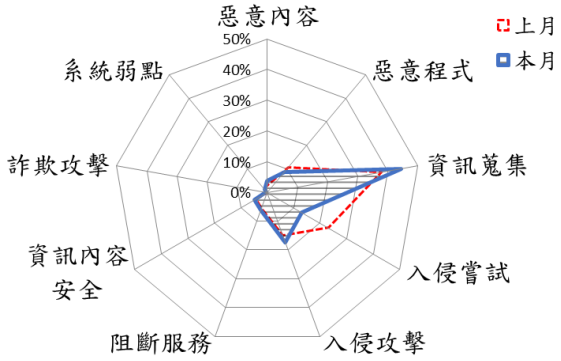
資料來源：資安院整理

表16 教育科學文化類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">教育科學文化類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>43.4</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>24.3</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">資訊蒐集</td><td>WAF 偵測外對內高風險事件</td></tr>
<tr><td>2</td><td colspan="2">入侵嘗試</td><td>遠端管理連線告警事件</td></tr>
</table>

資料來源：資安院整理

表17 非行政院所屬類資安威脅分析

<table>
<tr><td colspan="3">機關業務類別</td><td rowspan="2"> 
</td></tr>
<tr><td colspan="3">非行政院所屬類</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td><td rowspan="3"></td></tr>
<tr><td>本月</td><td>33.5</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>33.0</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">資訊蒐集</td><td>來源 IP 觸發多種未阻擋 IDS 事件</td></tr>
</table>

資料來源：資安院整理

表18 各業務類別與威脅種類交叉分析[4]

| 類別 / 業務 | 惡意內容 | 惡意程式 | 資訊蒐集 | 入侵嘗試 | 入侵攻擊 | 服務阻斷 | 資訊安全 | 詐欺攻擊 | 系統弱點 | 合計 |
|---|---|---|---|---|---|---|---|---|---|---|
| 綜合行政 | 0.0 | 0.2 | 1.8 | 0.8 | 1.3 | 0.1 | 0.1 | 0.0 | 0.0 | 4.3 |
| | 0.0 | 0.3 | 1.3 | 0.8 | 1.2 | 0.0 | 0.1 | 0.0 | 0.0 | 3.7 |
| 內政衛福勞動 | 0.0 | 1.5 | 18.4 | 10.6 | 6.8 | 4.0 | 3.3 | 0.0 | 0.9 | 45.6 |
| | 0.0 | 2.9 | 20.1 | 10.4 | 6.1 | 7.9 | 2.8 | 0.0 | 0.7 | 50.8 |
| 外交國防法務 | 0.1 | 0.5 | 20.4 | 3.5 | 1.0 | 0.1 | 0.9 | 0.0 | 0.2 | 26.8 |
| | 0.2 | 0.7 | 14.4 | 7.2 | 0.8 | 0.2 | 0.6 | 0.1 | 0.2 | 24.3 |
| 交通環境資源 | 0.2 | 3.2 | 3.5 | 3.0 | 1.6 | 5.9 | 1.1 | 0.0 | 0.0 | 18.5 |
| | 0.6 | 4.3 | 7.7 | 9.4 | 1.2 | 3.1 | 0.7 | 0.1 | 0.1 | 27.1 |
| 財政主計金融 | 2.9 | 4.6 | 20.3 | 23.9 | 10.4 | 0.9 | 0.4 | 0.3 | 0.0 | 63.9 |
| | 3.7 | 4.3 | 14.3 | 21.3 | 6.8 | 1.1 | 0.4 | 0.2 | 0.0 | 52.0 |
| 經濟能源農業 | 0.0 | 1.1 | 24.7 | 3.3 | 0.8 | 7.3 | 1.0 | 0.0 | 0.3 | 38.4 |
| | 0.1 | 6.3 | 28.3 | 7.8 | 3.5 | 10.9 | 1.8 | 0.0 | 0.2 | 58.9 |
| 教育科學文化 | 1.1 | 3.9 | 19.1 | 13.8 | 2.8 | 1.1 | 1.6 | 0.0 | 0.0 | 43.4 |
| | 1.2 | 2.4 | 13.1 | 3.6 | 2.1 | 0.7 | 1.2 | 0.0 | 0.1 | 24.3 |
| 非行政院所屬 | 1.3 | 2.9 | 14.9 | 4.4 | 5.8 | 2.0 | 1.7 | 0.2 | 0.4 | 33.5 |
| | 0.7 | 3.5 | 12.5 | 7.6 | 4.9 | 1.9 | 1.4 | 0.0 | 0.4 | 33.0 |
| 合計 | 5.7 | 17.9 | 123.2 | 63.3 | 30.5 | 21.5 | 10.2 | 0.5 | 1.8 | 274.5 |
| | 6.6 | 24.5 | 111.7 | 68.0 | 26.5 | 25.8 | 8.8 | 0.3 | 1.7 | 274.1 |

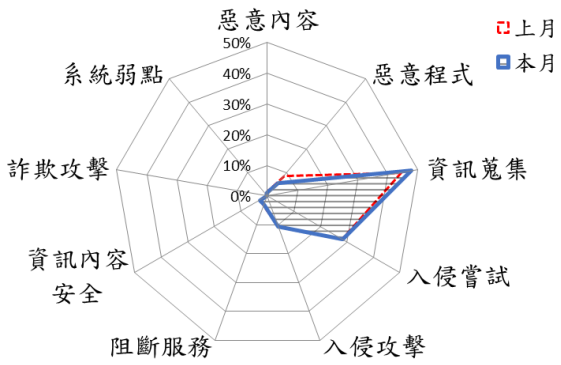
資料來源：資安院整理

[4]表內藍色粗體數字為本月各類平均資安聯防情資數量，紅色數字為上月各類平均資安監控情資數量，兩者均經各業務類別機關數量平減為平均每 1 機關之數量，數量上升者以黃底表示。

## 2.4 資安責任等級[5]與威脅種類交叉分析

針對政府機關資安責任等級與威脅種類進行交叉分析，以雷達圖呈現各威脅種類分布比例，藉此了解各業務機關遭遇資安威脅種類分布情形，相關內容詳見表 19 至表 21。同時，將各種威脅種類資安聯防情資數量經各資安責任等級機關數量平減為平均每 1 機關之數量，並與上月資訊進行比較，了解各資安責任等級機關遭遇資安威脅之增減情形，以利對各資安責任等級機關提出改善建議，相關內容詳見表 22。

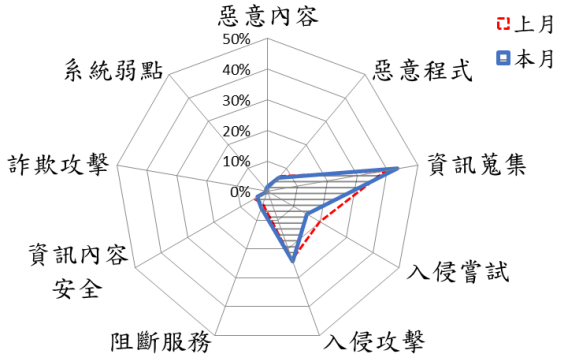
表19 A 級機關資安威脅分析

<table>
<tr><td colspan="3">機關資安責任等級</td><td rowspan="3"> 
</td></tr>
<tr><td colspan="3">A</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td></tr>
<tr><td>本月</td><td>542.0</td><td rowspan="2">  </td></tr>
<tr><td>上月</td><td>482.7</td></tr>
<tr><td>編號</td><td colspan="2">主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td colspan="2">資訊蒐集</td><td>WAF 偵測外對內高風險</td></tr>
<tr><td>2</td><td colspan="2">入侵嘗試</td><td>遠端管理連線告警事件</td></tr>
</table>

資料來源：資安院整理

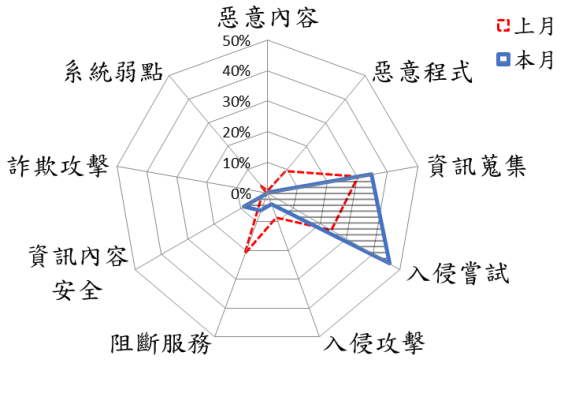
[5]詳見附件 1：公務機關業務類別與資安責任等級說明。

表20 B 級機關資安威脅分析

<table>
<tr><td colspan="3">機關資安責任等級</td><td rowspan="3"> 
</td></tr>
<tr><td colspan="3">B</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td></tr>
<tr><td>本月</td><td>157.0</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>161.1</td></tr>
<tr><td>編號</td><td>主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td>資訊蒐集</td><td>來源 IP 觸發多種未阻擋 IDS 事件</td></tr>
<tr><td>2</td><td>入侵攻擊</td><td>偵測可疑 IP</td></tr>
</table>

資料來源：資安院整理

表21 C 級機關資安威脅分析

<table>
<tr><td colspan="3">機關資安責任等級</td><td rowspan="3"> 
</td></tr>
<tr><td colspan="3">C</td></tr>
<tr><td colspan="3">平均資安聯防情資數量</td></tr>
<tr><td>本月</td><td>0.3</td><td rowspan="2"></td></tr>
<tr><td>上月</td><td>3.9</td></tr>
<tr><td>編號</td><td>主要資安威脅</td><td>資安威脅主要觸發資訊</td></tr>
<tr><td>1</td><td>入侵嘗試</td><td>特權帳號異常登入</td></tr>
<tr><td>2</td><td>資訊蒐集</td><td>外部主機對內進行遠端維運工具連線</td></tr>
</table>

資料來源：資安院整理

因本月無收容相關 D 級或 E 級機關資安聯防情資，故未呈現該責任等級機關威脅分析資訊。

表22 各資安責任等級與威脅種類交叉分析[6]

| 類別 / 業務 | 惡意內容 | 惡意程式 | 資訊蒐集 | 入侵嘗試 | 入侵攻擊 | 服務阻斷 | 資訊安全 | 詐欺攻擊 | 系統弱點 | 合計 |
|---|---|---|---|---|---|---|---|---|---|---|
| A 級機關 | 6.0 | 30.3 | 259.3 | 153.7 | 56.8 | 16.2 | 15.8 | 0.7 | 3.3 | 542.0 |
| | 6.8 | 42.0 | 214.0 | 136.2 | 50.5 | 16.9 | 12.5 | 0.5 | 3.2 | 482.7 |
| B 級機關 | 2.6 | 9.1 | 68.1 | 23.5 | 38.0 | 9.0 | 5.7 | 0.0 | 1.0 | 157.0 |
| | 2.2 | 10.5 | 63.5 | 31.8 | 38.1 | 6.8 | 7.6 | 0.0 | 0.6 | 161.1 |
| C 級機關 | 0.0 | 0.0 | 0.1 | 0.1 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.3 |
| | 0.0 | 0.4 | 1.2 | 1.0 | 0.3 | 0.8 | 0.1 | 0.0 | 0.1 | 3.9 |
| 合計 | 8.6 | 39.5 | 327.4 | 177.3 | 94.8 | 25.2 | 21.4 | 0.7 | 4.3 | 699.3 |
| | 9.1 | 52.9 | 278.7 | 168.9 | 89.0 | 24.6 | 20.2 | 0.5 | 3.9 | 647.7 |

資料來源：資安院整理

[6]表內藍色粗體數字為本月各類平均資安聯防情資數量，紅色數字為上月各類平均資安聯防情資數量，兩者均經各資安責任等級機關數量平減為平均每 1 機關之數量，數量上升者以黃底表示。

# 3. 聯防監控回饋建議

本章針對資安院聯防監控所收集之資安聯防情資，進行整體資安威脅趨勢與來源分析，分析結果提供政府機關與資安監控服務廠商做為資安環境布建防禦之參考。

## 3.1 聯防監控高風險情資分析

資安院分析資安聯防情資，並持續追蹤近期資安事件之後續發展，提供相關高風險威脅指標供聯防監控防護之參考。

### 3.1.1 資安院中繼站黑名單觸發情形

根據資安監控服務廠商回傳之資安聯防情資，彙整中繼站黑名單情資於各級政府機關之實際連線活躍情形，做為各機關加強監控使用。本月中繼站黑名單情資共 200 不重複 IP 紀錄與 134 不重複域名紀錄，統計本月資安威脅情資屬於中繼站黑名單情形詳見表 23 所示，並標示是否曾被資安網站列為黑名單，參考之資安網站包含 RiskIQ PassiveTotal[2]、VirusTotal[3]及 Google Safe Browsing[4]，建議機關與資安監控服務廠商特別關注。

表23 資安院中繼站黑名單觸發情形

| 編號 | 中繼站黑名單 | 國別 | 資安聯防情資數量 | 資安聯防情資內容 |
|---|---|---|---|---|
| 1 | 161.248.87.195 | MY | 1 | 已知中繼站連線 |
| 2 | 103.159.132.91 | MY | 1 | 已知中繼站連線 |
| 3 | 203.91.74.8 | HK | 1 | 已知中繼站連線 |

資料來源： 資安院整理

### 3.1.2 跨機關且跨 SOC 威脅來源分析

本月資安聯防情資中，跨機關(4 個以上)且跨 SOC(2 個以上)之威脅來源 IP，前 10 名詳見表 24。此情資為現有資安院黑名單情資，建議針對觸發之重點威脅指標持續觀察。

表24 跨機關且跨 SOC 威脅來源 IP

| 編號 | 資安聯防情資來源 IP | 國別 | 自治系統名稱 (ASNAME) | 機關數量 | SOC 數量 | 攻擊手法 |
|---|---|---|---|---|---|---|
| 1 | 104.194.155.33 | SG | ROUTERHOSTING, US | 50 | 8 | Exploit Public-Facing Application |
| 2 | 121.127.232.63 | HK | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK | 28 | 8 | Exploit Public-Facing Application |
| 3 | 107.173.135.116 | US | AS-COLOCROSSING, US | 28 | 7 | Exploit Public-Facing Application |
| 4 | 173.199.71.13 | FR | AS-VULTR, US | 23 | 7 | Exploit Public-Facing Application |
| 5 | 192.159.99.95 | NL | SERVICES-1337-GMBH 1337-SERVICES-GMBH-NETWORK, DE | 21 | 7 | Vulnerability Scanning |
| 6 | 202.61.130.161 | SG | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK | 21 | 7 | Exploit Public-Facing Application |
| 7 | 85.93.9.247 | DE | PFWEBSOLUTIONS, DK | 20 | 7 | Exploit Public-Facing Application |

| 編號 | 資安聯防情資來源 IP | 國別 | 自治系統名稱 (ASNAME) | 機關數量 | SOC 數量 | 攻擊手法 |
|---|---|---|---|---|---|---|
| 8 | 194.50.16.73 | NL | AS49870-BV, NL | 18 | 6 | Botnet |
| 9 | 85.114.132.32 | DE | MYLOC-AS IP Backbone of WIIT AG formerly myLoc managed IT AG, DE | 16 | 6 | Exploit Public-Facing Application |
| 10 | 179.43.173.12 | CH | PLI-AS, PA | 15 | 5 | Exploit Public-Facing Application |

資料來源： 資安院整理

## 3.2 近期資安研究資訊

資安院根據近期內外部情資彙整資訊進行研析，並提供回饋情資供機關防護參考，做為各機關聯防監控使用。

### 3.2.1 政府領域 MongoDB 資料庫管理系統漏洞研析

MongoDB 為一款 NoSQL 資料庫管理系統，專為應用程式提供高擴展性與高效能的資料儲存解決方案。與傳統關聯式資料庫不同，MongoDB 採用「文件導向」儲存資料，開發者無需預先定義資料表結構(Schema)，可隨需求動態調整，賦予資料模型靈活性。其核心技術優勢包括開放原始碼、透過分片技術(Sharding)實現水平擴展，以及利用副本集技術(Replica Set)確保高可用性與自動容錯轉移；此外，具備強大的資料庫查詢語言，可有效於巨量資料中進行搜尋與處理。這些優勢使 MongoDB 廣泛應用於內容管理、即時分析及物聯網部署等應用情境中，成為發展應用程式使用資料庫的選擇之一。

MongoDB 官方 2025 年 12 月公告其資料庫管理系統存在高風險漏洞[8][9]，可使未經身分驗證之遠端攻擊者惡意利用漏洞觸發記憶體堆疊問題，導致

MongoDB 記憶體洩漏敏感資訊之疑慮，漏洞資訊詳見表 25。

表25 CVE-2025-14847 漏洞資訊

| 漏洞編號 | CVE-2025-14847 |
|---|---|
| 漏洞分數(CVSS 4.0) | 8.7(HIGH) |
| 漏洞類別 | 參數處置不當 (Improper Handling of Length Parameter Inconsistency) |
| 受影響版本 | MongoDB 8.2.0 至 8.2.2 版(含)<br>MongoDB 8.0.0 至 8.0.16 版(含)<br>MongoDB 7.0.0 至 7.0.26 版(含)<br>MongoDB 6.0.0 至 6.0.26 版(含)<br>MongoDB 5.0.0 至 5.0.31 版(含)<br>MongoDB 4.4.0 至 4.4.29 版(含)<br>所有 MongoDB 4.2 版<br>所有 MongoDB 4.0 版<br>所有 MongoDB 3.6 版 |

資料來源： 資安院整理

根據情資顯示該漏洞已遭駭客惡意利用，相關概念性驗證程式已於公開平台釋出，預期將引發新一波漏洞自動化掃描與利用攻擊，美國網路安全和基礎設施安全局(CISA)亦已將該漏洞加入已知成功利用漏洞目錄(KEV)[10]。漏洞公告之初，資安院已偵測到多筆 MongoDB 服務探測紀錄，彙整相關威脅指標資訊詳見表 26。

表26 MongoDB 資料庫管理系統服務探測攻擊指標列表

| 項次 | 攻擊指標 | 國別 | 自治系統名稱(ASN) |
|---|---|---|---|
| 1 | 139.0.166.57 | ID | FASTNET-AS-ID Linknet-Fastnet ASN, ID |
| 2 | 139.195.99.59 | ID | FASTNET-AS-ID Linknet-Fastnet ASN, ID |
| 3 | 149.113.248.183 | ID | FASTNET-AS-ID Linknet-Fastnet ASN, ID |
| 4 | 134.209.111.71 | SG | DIGITALOCEAN-ASN, US |
| 5 | 38.58.182.203 | US | FIBERSTATE, US |
| 6 | 139.0.140.99 | ID | FASTNET-AS-ID Linknet-Fastnet ASN, ID |
| 7 | 149.113.208.158 | ID | FASTNET-AS-ID Linknet-Fastnet ASN, ID |
| 8 | 62.60.135.174 | IR | FPS12, RO |
| 9 | 65.108.216.47 | FI | HETZNER-AS, DE |
| 10 | 196.251.100.160 | SC | OPTIBOUNCE, US |

資料來源： 資安院整理

經資安院研析發現，政府領域存在 5 個機關 IP 使用受漏洞影響版本，其中以綜合行政類機關為主，其資安責任等級與業務類別分布詳見表 27，資安院已發布警訊通知機關進行處置。此外，亦發現國內通訊傳播領域、民間組織與企業、醫療領域及高科技園區領域存在受漏洞影響設備，以已通知相關單位，建議使用漏洞修補版本進行緩解措施以確保安全性。

表27 政府領域受漏洞影響之機關 IP 分布

| 編號 | 資安責任等級 / 機關業務類別 | A | B | C | D | 總計 |
|---|---|---|---|---|---|---|
| 1 | 教育科學文化 | 1 | 0 | 0 | 0 | 1 |
| 2 | 非行政院所屬 | 0 | 1 | 0 | 0 | 1 |
| 3 | 綜合行政 | 0 | 2 | 0 | 1 | 3 |
| 總計 | | 1 | 3 | 0 | 1 | 5 |

資料來源： 資安院整理

針對政府領域 MongoDB 資料庫管理系統漏洞風險，提供相關建議供機關防護參考：

1. 確認機關內部是否部署使用 MongoDB 資料庫管理系統，官方已釋出安全性更新，建議評估執行更新或其他風險緩解措施。
2. MongoDB 4.2 以前之版本，官方已不提供安全性更新，建議進行版本升級。
3. 建議評估 MongoDB 公開於網際網路之必要性，必要時僅允許內網或設置白名單進行存取。
4. 參考表 26 威脅指標資訊，檢視近期機關設備是否遭相關威脅指標連線，並進行適當處置。
5. 建議設備納入資安監控範圍，並定期分析是否有網路異常行為。

### 3.2.2 利用行政訴訟名義之社交工程電子郵件攻擊案例

近期資安院接獲外部情資，發現駭客以「行政訴訟」為誘因，針對政府機關發動社交工程電子郵件攻擊。駭客於寄件人顯示名稱中標示為「行政訴訟起訴狀」，以營造具法律效力與急迫性假象，藉此提高收件者開啟郵件之意願；同時，駭客於郵件主旨中刻意使用收件者所屬機關名稱，並將郵件內容偽裝為「法院通知書」，包含案件編號、案件名稱等看似正式之資訊，以提升郵

件可信度，進而引導收件者點擊郵件內所附連結，查閱所謂「相關資料」，進而下載並植入惡意後門程式(ValleyRAT)以達竊取電腦機敏資料目的，相關社交工程電子郵件內容範例詳見圖 6，惡意壓縮檔內容詳見圖 7。


資料來源： 資安院整理

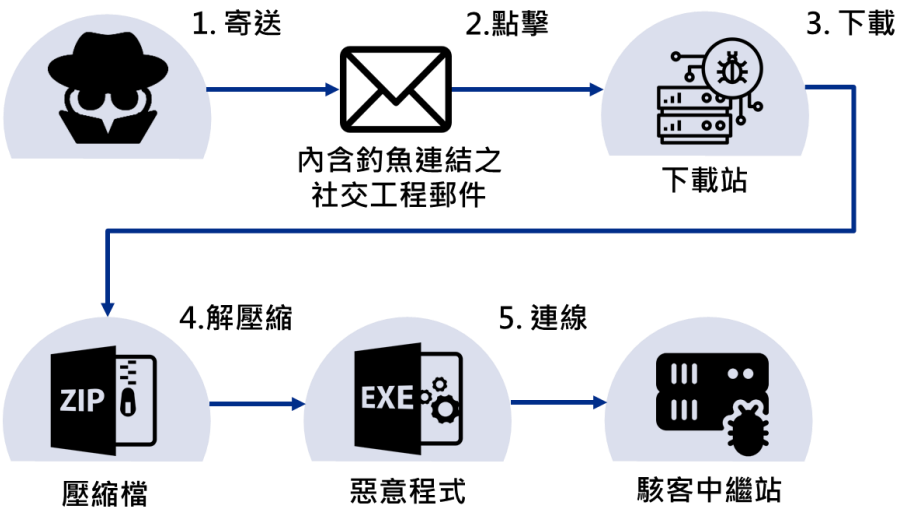
圖6 社交工程郵件內容範例


資料來源： 資安院整理

圖7 惡意壓縮檔內容

經檢視分析該釣魚連結，駭客濫用合法雲端服務平台（騰訊雲）作為惡意檔案下載站。此手法除可降低惡意基礎設施之建置與維運成本外，亦可利用合法雲端服務之可信度，降低資安防護設備對惡意連線與檔案下載行為之偵測與阻擋機率，進而提升攻擊成功率。

當收件者點擊釣魚連結，將下載一內含惡意執行檔之壓縮檔；待收件者解壓縮並點擊執行該檔案後，將於其電腦中植入惡意後門程式(ValleyRAT)，最終連線至惡意中繼站，使駭客得以遠端存取目標收件者系統，進一步執行竊取電腦內部機敏資料、蒐集系統資訊，或接收並執行其他駭客指令等後續攻擊行為，整體攻擊流程詳見圖 8。




資料來源： 資安院整理

圖8 整體攻擊流程

彙整本月社交工程惡意電子郵件案例中，所取得之 IoC 詳見表 28。

表28 社交工程惡意電子郵件受駭偵測指標

| 編號 | IoC | 說明 |
|---|---|---|
| 1 | 770e64e02d2cf2cac30d6074c201d44279996cbc | 惡意檔案雜湊值(SHA1) |
| 2 | e69b347f9608abaf31cab02f0a34b3dfa1d7c872 | 惡意檔案雜湊值(SHA1) |
| 3 | 202[.]79[.]168[.]155 | 惡意中繼站 IP |
| 4 | giugh9ygiuhljbgh-1328314126[.]cos[.]ap-tokyo[.]myqcloud[.]com | 惡意下載站 DN |

資料來源：資安院整理

此次駭客利用行政訴訟名義寄送社交工程電子郵件，誘騙收件者點擊連結並下載惡意檔案，進而達成竊取機敏資訊之目的，針對此威脅攻擊手法，提供相關建議供資安防護參考

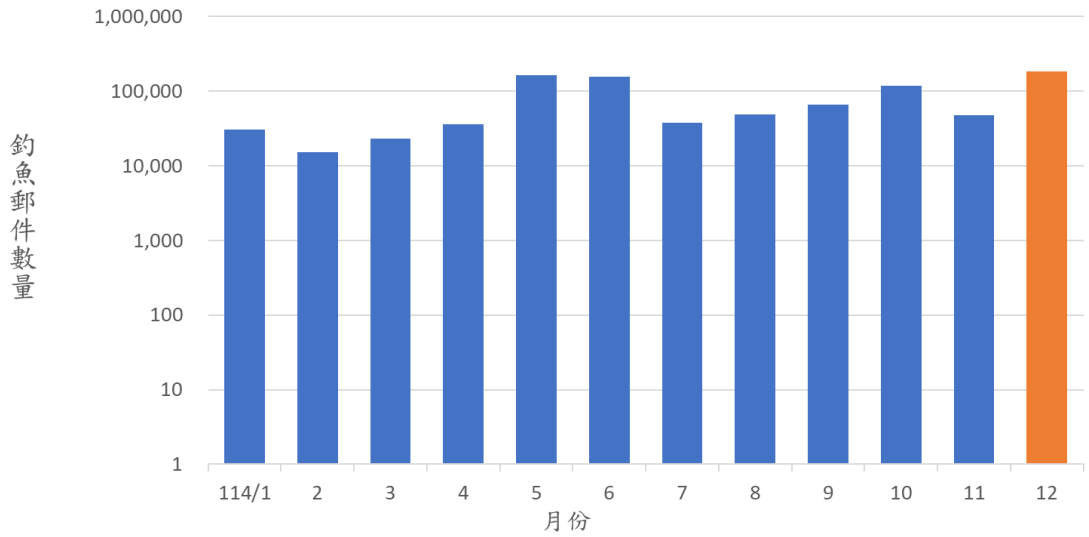
1. 建議承辦人員留意業務相關主旨之可疑電子郵件，注意郵件來源正確性，勿開啟不明來源之郵件與相關附檔及連結。
2. 請注意個別系統之安全修補與病毒碼更新，包含作業系統、程式套件及防毒軟體等。
3. 加強內部宣導，提升人員資安意識，以防範駭客利用電子郵件進行社交工程攻擊。
4. 網路管理人員請清查中繼站相關連線紀錄，並確實定期更新防火牆。

## 3.3 惡意電子郵件檢測分析

本章節分享惡意電子郵件檢測分析情資，並提供近期惡意電子郵件分析，供機關資安聯防參考。

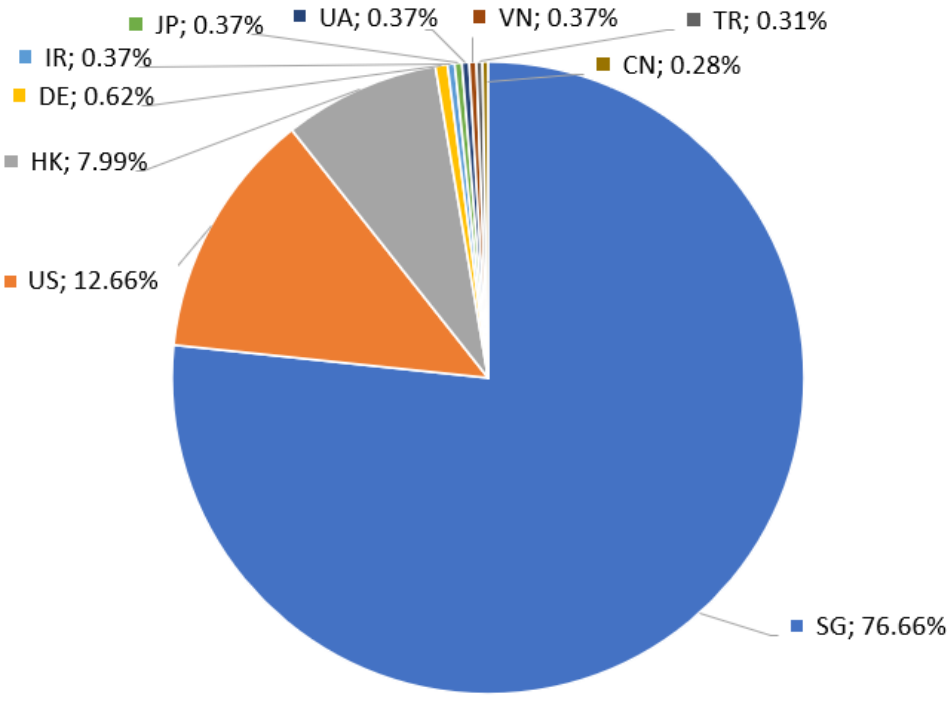
### 3.3.1 社交工程釣魚郵件威脅統計分析

本月透過惡意電子郵件檢測機制蒐集 185,868 封有釣魚網址攻擊手法之社交工程郵件，每月偵測數量分布詳見圖 9。經分析檢測社交工程釣魚郵件，其中前 10 大釣魚郵件攻擊來源 IP 所屬國家詳見圖 10，前 10 大釣魚郵件主旨詳見表 29。




資料來源：資安院整理

圖9　釣魚郵件每月偵測分布趨勢




資料來源：資安院整理

圖10 前 10 大釣魚郵件攻擊來源 IP 所屬國家分布

表29 前 10 大釣魚郵件主旨

| 編號 | 寄件來源<br>IP 位址 | 國別 | 釣魚郵件主旨 | 數量 |
|---|---|---|---|---|
| 1 | ▪43.165.185.250<br>▪43.164.128.92<br>▪43.165.131.99<br>▪43.165.128.150<br>▪43.164.131.159 | SG | ヨドバシドットコム：「お客様情報」変更依頼受付のご連絡 | 121 |
| 2 | 192.227.128.148 | US | RE: December Holiday Schedule & Christmas Bonus Information | 96 |
| 3 | ▪43.164.3.204<br>▪43.164.133.171<br>▪43.164.1.143<br>▪43.165.180.30<br>▪43.164.3.61 | SG | 【重要】自動継続購入の停止とお手続き方法のご案内（Nintendo Switch Online） | 78 |
| 4 | ▪43.164.3.204<br>▪43.164.134.76<br>▪43.164.1.143<br>▪43.164.134.118<br>▪43.164.132.32 | SG | 【アクションが必要です】継続課金の解除について | 57 |
| 5 | ▪43.243.165.255<br>▪103.95.56.255<br>▪103.71.228.2<br>▪43.243.165.194<br>▪43.243.165.196 | HK | MRNA–mAb Custom High-Difficulty GPCR Target Antibody: One-stop all-inclusive delivery, only $8,999 | 42 |
| 6 | ▪43.164.130.196<br>▪43.165.194.128 | SG | 【至急】ご利用を継続いただくためのお願い | 34 |

| 編號 | 寄件來源<br>IP 位址 | 國別 | 釣魚郵件主旨 | 數量 |
|---|---|---|---|---|
| | ▪ 43.164.129.252<br>▪ 43.165.184.43<br>▪ 43.164.133.246 | | | |
| 7 | ▪ 43.160.244.219<br>▪ 43.164.1.106<br>▪ 43.160.249.236<br>▪ 43.160.242.52<br>▪ 43.164.3.37 | SG | 会員専用ネットサービスからのお知らせ | 33 |
| 8 | ▪ 43.243.165.194<br>▪ 103.95.56.255<br>▪ 43.243.165.255<br>▪ 103.71.228.2<br>▪ 43.243.165.196 | HK | AI + Multi-Platform Integration for Low Immunogenicity Antibody R&D: ISPRI/IEDB/BioPhi and Engineering Strategies | 32 |
| 9 | ▪ 138.204.117.44<br>▪ 177.185.42.125<br>▪ 170.246.99.42<br>▪ 191.156.49.171<br>▪ 191.156.60.99 | BR<br><br><br>CO | 您的帐户已被黑。数据被盗。了解如何重新获得访问权限。 | 30 |
| 10 | ▪ 43.160.249.188<br>▪ 43.165.187.213<br>▪ 43.164.0.78<br>▪ 43.164.134.135<br>▪ 43.164.128.77 | SG | ポケットカード利用制限：認証手続きのお願い | 28 |

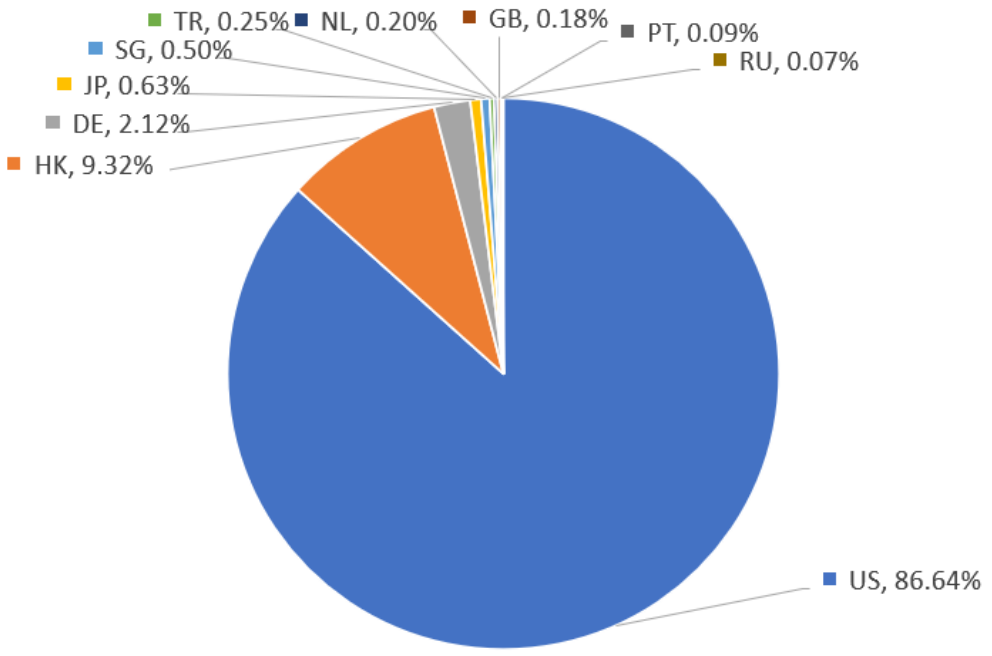
資料來源：資安院整理

本月檢測釣魚郵件共解析出 15,129 個釣魚網址，經分析前 10 大釣魚網址使用之域名詳見表 30，前 10 大釣魚網址對應之 IP 位址所屬國家分布詳見圖 11 所示。

表30 前 10 大釣魚網址域名

| 編號 | 域名 | 編號 | 域名 |
|---|---|---|---|
| 1 | tgr.jp | 6 | www.moringax.best |
| 2 | ai-tradlngview.com | 7 | imlines-update.appwrite.network |
| 3 | geandf.top | 8 | fdcvdz.top |
| 4 | games33.top | 9 | safe.cgnrbwhwqcjnb.cc |
| 5 | games22.top | 10 | spemail5.online |

資料來源：資安院整理




資料來源：資安院整理

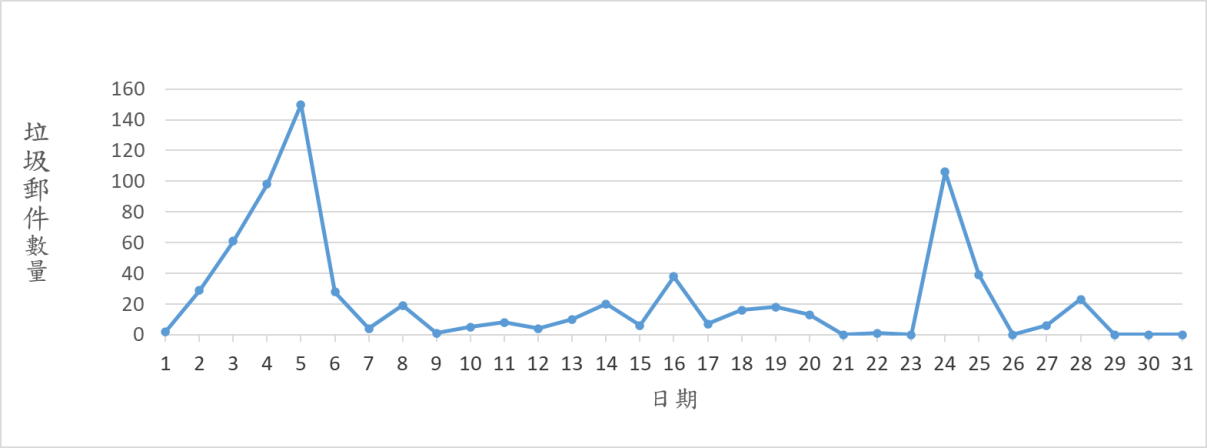
圖11 前 10 大釣魚網址對應 IP 所屬國家分布

針對社交工程釣魚郵件攻擊，以下提供相關建議供政府機關防護參考。

1. 請使用者留意相關電子郵件，注意郵件來源正確性，不要開啟不明來源郵件之連結。
2. 切勿於網頁隨意提供機密資訊，如公務用電子郵件帳號、通行碼及信用卡號碼等，以防個人資料與公務機敏資訊外洩。

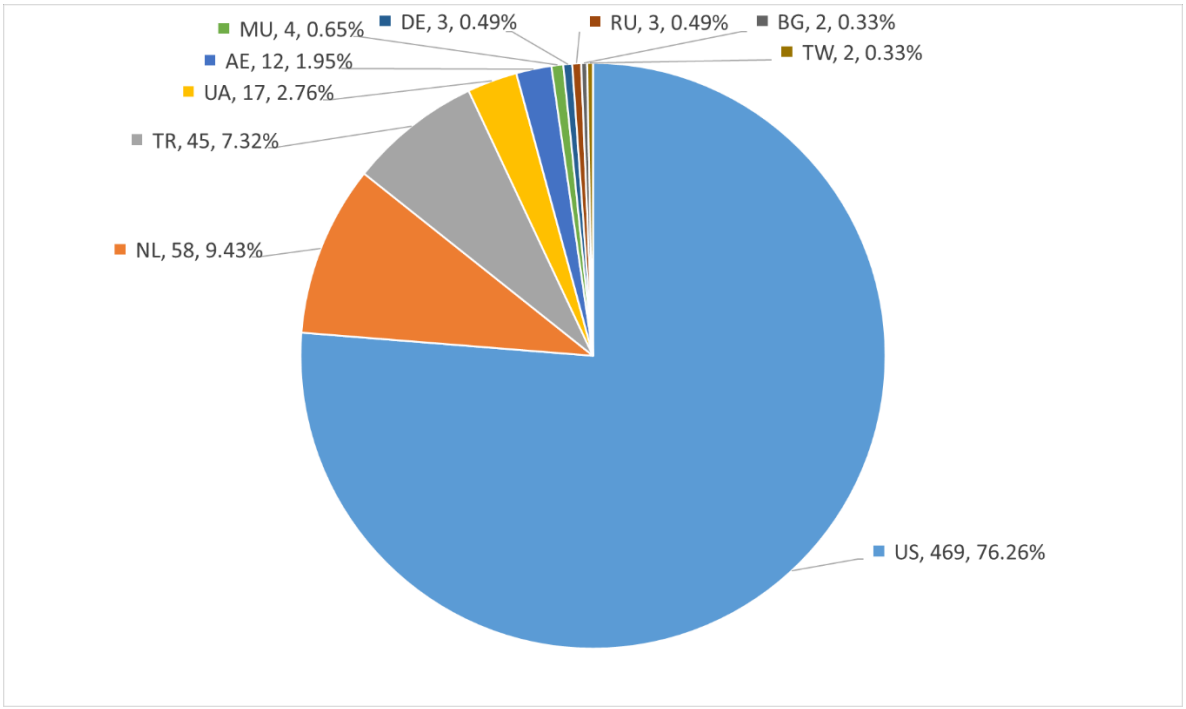
### 3.3.2 惡意程式垃圾郵件威脅統計分析

本月透過惡意電子郵件檢測機制，蒐集 712 封夾帶惡意程式附檔之電子郵件，每日偵測數量分布詳見圖 12。經分析檢測惡意程式垃圾郵件，其中前 10 大惡意程式垃圾郵件攻擊跳板來源 IP 所屬國家詳見圖 13，惡意郵件附檔以 AgentTesla 遠端木馬占整體 55.2%為最多，其次為 Remcos 遠端木馬與 CVE201711882 漏洞，整體分布詳見圖 14。



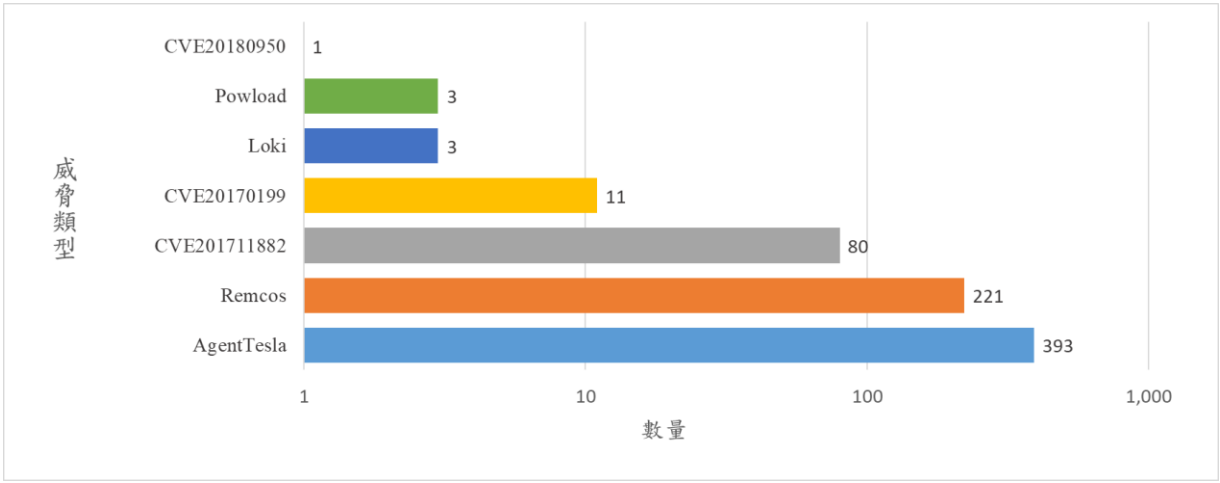

資料來源：資安院整理

圖12 惡意程式垃圾郵件每日偵測分布圖




資料來源：資安院整理

圖13 前 10 大惡意程式垃圾郵件攻擊跳板來源 IP 所屬國家分布




資料來源：資安院整理

圖14 主要惡意郵件附檔威脅類型排名

本月檢測惡意程式垃圾郵件共解析出 720 個惡意附檔，經分析前 10 大惡

意附檔詳見表 31，相關中繼站 IoC 詳見表 32。

表31 前 10 大惡意附檔

| 編號 | 郵件主旨 | 檔案名稱 | 檔案雜湊值 (SHA-1) | 數量 |
|---|---|---|---|---|
| 1 | RFQ-Vendor 012433 PO 00013491049 | ▪ Vendor%20012433%20PO%2000013491049.7z<br>▪ Vendor 012433 PO 00013491049.7z | B8F041588115C11562150869C187A59DFE309B59 | 66 |
| 2 | RFQ P02-06-5119 ( BCD 02-DEC-2025 ) | ▪ RFQ%20P02-06-5119%20%28%20BCD%2002-DEC-2025%20%29.Tar<br>▪ RFQ P02-06-5119 ( BCD 02-DEC-2025 ).Tar | 7C71624F989B800B7270C6480543B4EA78FEF581 | 47 |
| 3 | RE: Copia_Documentación | ▪ ccf_4573%20Documento.uue<br>▪ ccf_4573 Documento.uue | 05245003E33E0953130AE9DC3BBC5E2BC6371A4A | 41 |
| 4 | MI4416 Request for Quotation - Top Urgent | ▪ MI4416%20Request%20for%20Quotation.Tar<br>▪ MI4416 Request for Quotation.Tar | AB7FC062307B62F3DB224318371EB4E3095C88A4 | 40 |
| 5 | ▪ M/T ATLANTIC PRINCESS (IMO No. 9899363) - MRPL cp | ▪ ATLANTIC%20PRINCESS%20PARTICULARS.xlam | 05983D88CB7D463D237450FB6FE94E91E1EB3D11 | 30 |

| 編號 | 郵件主旨 | 檔案名稱 | 檔案雜湊值 (SHA-1) | 數量 |
|---|---|---|---|---|
| | 05.12.2025 - Call for Loading<br>▪ Spring Fortune V2508 - Transiting thru Suez (South bound)<br>▪ VSL: GSL-SOFIA, QUOTATION: C155-CS255013A - URGENT RFQ<br>▪ MV Lindsaylou - Loading Port Agency Appointment | ▪ ATLANTIC PRINCESS PARTICULARS.xlam<br>▪ 1.%20Q88%20V6%20-%20SPRING%20FORTUNE.xlam<br>▪ 1. Q88 V6 - SPRING FORTUNE.xlam<br>▪ QUOT_C155-CS255013A_S1311_3.pdf%2CE_QUOT_XLS_C155-CS255013A_S1311_3.xlam<br>▪ "QUOT_C155-CS255013A_S1311_3.pdf, E_QUOT_XLS_C155-CS255013A_S1311_3.xlam"<br>▪ UPDATE LINDSAYLOU_BALTIC QNNAIRE.xlam | | |
| 6 | Quotation Request For WSO# 23 | ▪ Quotation%20Request%20For%20WSO%23%2023.Tar<br>▪ Quotation Request For WSO# 23.Tar | D08B960F36D27E4EEFC16CA92A9C6583120FA4B7 | 29 |

| 編號 | 郵件主旨 | 檔案名稱 | 檔案雜湊值 (SHA-1) | 數量 |
|---|---|---|---|---|
| 7 | Quotation Request For WSO# 23 | ▪ Quotation%20Request%20For%20WSO%23%2023.GZ<br>▪ Quotation Request For WSO# 23.GZ | D7A554F91B0788D0ECAA5F0469D7D5E9E6936D9C | 29 |
| 8 | ENQ DB9002M ORDER M24093 2025 | ▪ ENQ%20DB9002M%20ORDER%20M24093%202025.zip<br>▪ ENQ DB9002M ORDER M24093 2025.zip | 922B21084E81BFB7F500882EFF0E728A5DE5ADCC | 28 |
| 9 | RE: Enquiry / QUOTATION REF NO: AH0409231 | ▪ Enquiry%20%20QUOTATION%20REF%20NO%20AH0409231.Tar<br>▪ Enquiry QUOTATION REF NO AH0409231.Tar | 1339FB7D981319540DDF4253E08570126DA49612 | 26 |
| 10 | RFQ for Materials - Q2590008 SD55KDB MATERIALS | ▪ Q2590008%20SD55KDB%20MATERIALS.GZ<br>▪ Q2590008 SD55KDB MATERIALS.GZ | F40C763E8E26091D2D957B25D3F41DD7A90B9D99 | 24 |

資料來源：資安院整理

表32 惡意程式垃圾郵件偵測指標列表

| 編號 | 中繼站/<br>下載站 | 檔案名稱 | 檔案雜湊值<br>(SHA-1) | 攻擊手法/<br>威脅類型 |
|---|---|---|---|---|
| 1 | ftp://ftp.gizemetiket.com.tr/PW_Administrator-Win-James_2025_12_17_09_27_56.html | ▪ D:/xampp/htdocs/JATGPUO1ZONGV8R16DKYZ6Z/ferritic<br>▪ ccf_4573%20Documento.uue | ▪ 5C78A84436AA40B293ABA827214479F09AAFE530<br>▪ 05245003E33E0953130AE9DC3BBC5E2BC6371A4A | AgentTesla |
| 2 | mail.allportcargoservice.com | ▪ D:/xampp/htdocs/W10NJR3ZQBMQL035S/Thebit<br>▪ D:/xampp/htdocs/IASZFU4PK1/forniciform | ▪ 9867E1FD642D01873A9CCDCC2361D5B658FDA450<br>▪ 9867E1FD642D01873A9CCDCC2361D5B658FDA450 | AgentTesla |
| 3 | mail.real-honesty.com | ▪ URGENT !! RE RE LCL FOB Shanghai-Nhava shevaTWVD82.exe | ▪ 1A42D1AEFC5557B805E4305AEB8D210D7A2735C9<br>▪ 01D332D39ED2D284 | AgentTesla |

| 編號 | 中繼站/<br>下載站 | 檔案名稱 | 檔案雜湊值<br>(SHA-1) | 攻擊手法/<br>威脅類型 |
|---|---|---|---|---|
| | | ▪ URGENT%20%21%21%20RE%20RE%20LCL%20FOB%20Shanghai-%20Nhava%20shevaTWVD82.7z.001 | 40CFDFE0620397C34D82EC66 | |
| 4 | zo.cm | AnfrageIP250009-AF2506595.docx | 7750FD92044A99E6B151EE94D01492D02EE5F135 | ▪ CVE20180199<br>▪ CVE20170950 |

資料來源：資安院整理

針對惡意程式垃圾郵件攻擊，以下提供相關建議供政府機關防護參考。

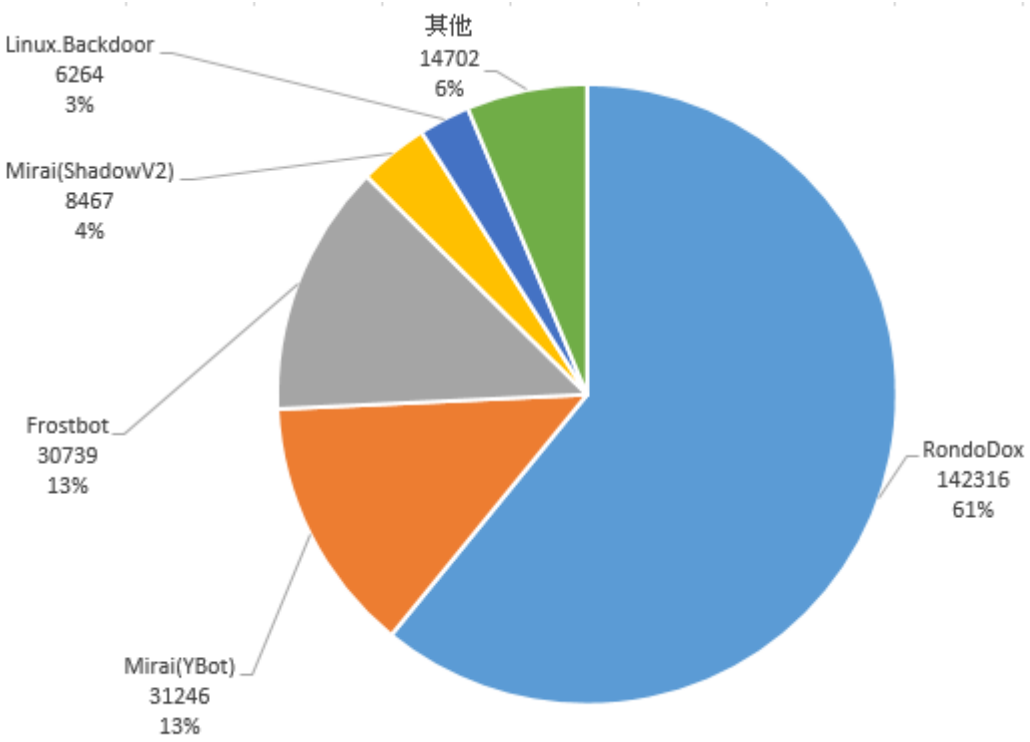
1. 請使用者留意相關電子郵件，注意郵件來源正確性，不要開啟不明來源郵件之附檔，以防被植入惡意程式。
2. 建議針對網路服務之存取行為建立控管機制，並定期檢視網路可疑連線，避免造成資安漏洞。

## 3.4 殭屍網路攻擊威脅情資

資安院長期監控全球殭屍網路攻擊動向與發展趨勢，透過分析自行蒐集之殭屍網路樣本取得進階攻擊樣態，製作殭屍網路攻擊指標(Indicator of Attack, IoA)偵測規則，並結合資安院自有網路攻擊威脅誘捕系統，偵測來自世界各地之殭屍網路攻擊情勢，除能鎖定攻擊來源 IP，亦能藉由長期追蹤攻擊來源，辨識殭屍網路之新型態攻擊變化，以下提供近期物聯網殭屍網路之威脅情資，供機關進行資安聯防參考。

### 3.4.1 物聯網殭屍網路攻擊情資

現今殭屍網路族群主要攻擊家用路由器與網路監控器等物聯網設備，資安院本月偵測之殭屍網路攻擊次數高達 233,734 次，其中包含 38 類殭屍網路與其變種病毒，大量殭屍網路病毒仍持續變形與散布，感染各種 IoT 設備，攻擊次數前 5 大殭屍網路占全體攻擊比例約 93%，詳見圖 15。




資料來源： 資安院整理

圖15 攻擊次數前 5 大變種類型比例圖

物聯網殭屍網路會針對特定型號物聯網設備之弱點進行攻擊，攻擊成功後將控制受駭設備連線至惡意下載站下載並植入惡意程式，感染受駭設備為殭屍網路成員。各殭屍網路之來源分布、攻擊次數及變種資訊詳見表 33，受駭偵測指標詳見表 34。

表33 各殭屍網路 IoA 排名列表

| 編號 | 攻擊跳板來源 IP | 國家 | 攻擊次數 | 變種類型 |
|---|---|---|---|---|
| 1 | 74.194.191.52 | US | 142316 | RondoDox |
| 2 | 158.94.210.88 | GB | 31246 | Mirai(YBot) |
| 3 | 87.121.84.181 | US | 30739 | Frostbot |
| 4 | 91.200.220.143 | UA | 8467 | Mirai(ShadowV2) |

| 編號 | 攻擊跳板來源 IP | 國家 | 攻擊次數 | 變種類型 |
|---|---|---|---|---|
| 5 | 130.12.180.127 | CA | 6264 | Linux.Backdoor |
| 6 | 23.132.228.234 | IT | 4709 | vtuber |
| 7 | 103.77.246.136 | VN | 2196 | Mirai(Katana) |
| 8 | 23.177.185.39 | US | 1644 | Hailbot |
| 9 | 103.245.236.146 | VN | 897 | Mirai(ShadowV2) |
| 10 | 130.12.180.20 | GB | 867 | Linux.Persistence |

資料來源： 資安院整理

表34 殭屍網路 IoC 影響概況

| 編號 | 殭屍網路類型 | 惡意 C&C | 惡意下載網站 URL |
|---|---|---|---|
| 1 | RondoDox | 104.26.12.205 | http://74.194.191.52/rondo.ebj.sh |
| 2 | Mirai(YBot) | 158.94.210.88 | 158.94.210.88/jaws |
| 3 | Frostbot | 87.121.84.181 | http://87.121.84.181/ipcam.zavio.sh<br>http://87.121.84.181/nas.dlink2.sh+<br>http://87.121.84.181/router.totolink2.sh |
| 4 | Mirai(Shadow V2) | 91.200.220.143 | http:/\\/91.200.220.143/bins/shadow.arm7<br>http:/91.200.220.143/shadow.sh |

| 編號 | 殭屍網路類型 | 惡意 C&C | 惡意下載網站 URL |
|---|---|---|---|
| 5 | Linux.Backdoor | 130.12.180.127 | http:/\\/130.12.180.127/ntx86 |

資料來源： 資安院整理

針對上述惡意程式與攻擊情資，建議採取以下防護措施。

1. 建議修改設備之預設帳號通行碼，並符合通行碼複雜性原則，避免遭駭客利用字典檔進行暴力破解攻擊。
2. 建議勿將設備放置於公開網路中，以免增加惡意程式透過網路入侵之機率。
3. 建議定期更新廠商推出之最新版本韌體，確保設備免遭惡意程式利用已知漏洞進行攻擊。
4. 建議考量該殭屍網路對機關可能造成之影響，評估是否將上述來源 IP 納入資安設備黑名單進行偵測阻擋。
5. 建議檢視相關設備連線紀錄，觀察是否存在上述情資之來源 IP 連線，並進行必要應變處置。

## 3.5 網路潛在資安風險情資

資安院長期關注政府機關網路潛在資通安全風險並進行研究分析，以下列出近期關注之資安風險類別，分別為遠端控制類、已知漏洞類及資料庫與檔案類，並針對各資安風險類別分享前 10 大可疑外部 IP，供機關進行資安聯防參考。

### 3.5.1 已知漏洞類風險

已知漏洞類風險為駭客透過已知資安漏洞，嘗試對機關進行入侵行為，並針對相關威脅來源 IP 進行分析，進階找出下載站或 C&C 中繼站，其中威脅來源 IP 視為 IoA，下載站或 C&C 中繼站則為 IoC。表 35 彙整近期已知漏洞資訊[7]，並依漏洞類型提供前 10 大 IoA，供機關做為聯防監控參考，詳見表 35 至表 41。

表35 已知漏洞資訊

| 編號 | 已知漏洞類型 | 漏洞編號 | CVSSv3 漏洞評鑑分數 |
|---|---|---|---|
| 1 | Next.js Web 應用程式框架 | CVE-2025-55182 | 10.0 |
| 2 | PHP 伺服器端腳本語言 | CVE-2024-34340 | 9.1 |
| | | CVE-2024-36048 | 9.8 |
| | | CVE-2024-34502 | 9.8 |
| 3 | D-Link 網路儲存設備 | CVE-2024-3272 | 10.0 |
| | | CVE-2024-3273 | 9.8 |

7 Exploit Database: https://www.exploit-db.com/;
Common Vulnerabilities and Exposures: https://www.cve.org/

| 編號 | 已知漏洞類型 | 漏洞編號 | CVSSv3 漏洞評鑑分數 |
|---|---|---|---|
| 4 | GeoServer 地理位置資訊伺服器 | CVE-2025-58360 | 9.8 |
| | | CVE-2024-36401 | 9.8 |
| | | CVE-2023-35042 | 10.0 |
| 5 | Apache OFBiz 企業資源規劃系統 | CVE-2024-38856 | 9.8 |
| | | CVE-2024-45195 | 9.8 |
| 6 | Citrix NetScaler 設備 | CVE-2023-3519 | 9.8 |
| | | CVE-2023-4966 | 9.4 |
| | | CVE-2025-5777 | 9.3 |

資料來源： 資安院整理

表36 Next.js Web 應用程式框架漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 193.142.147.209 | DE | COLOCATEL-INC Colocatel Network - High Bandwidth Dedicated Servers, SC |
| 2 | 193.32.162.157 | RO | UNMANAGED-DEDICATED-SERVERS, GB |
| 3 | 95.214.52.170 | PL | MEVSPACE, PL |
| 4 | 185.16.39.52 | PL | MEVSPACE, PL |
| 5 | 5.187.35.21 | NL | AMARUTU-TECHNOLOGY, SC |
| 6 | 62.60.131.239 | IR | FPS12, RO |
| 7 | 87.121.84.154 | US | VPSVAULTHOST, GB |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 8 | 192.159.99.95 | NL | SERVICES-1337-GMBH 1337-SERVICES-GMBH-NETWORK, DE |
| 9 | 193.34.213.150 | PL | MEVSPACE, PL |
| 10 | 149.50.96.133 | PL | MEVSPACE, PL |

資料來源： 資安院整理

表37 PHP 伺服器端腳本語言漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 176.123.1.163 | MD | ALEXHOST, MD |
| 2 | 146.19.213.39 | MD | ALEXHOST, MD |
| 3 | 91.208.197.157 | MD | ALEXHOST, MD |
| 4 | 91.208.197.221 | MD | ALEXHOST, MD |
| 5 | 81.180.92.130 | RO | ALEXHOST, MD |
| 6 | 146.19.213.242 | MD | ALEXHOST, MD |
| 7 | 123.143.114.188 | KR | LGDACOM LG DACOM Corporation, KR |
| 8 | 91.208.184.223 | MD | ALEXHOST, MD |
| 9 | 216.118.251.162 | HK | NETSEC-HK Netsec Limited, HK |
| 10 | 121.127.232.63 | HK | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK |

資料來源： 資安院整理

表38 D-Link 網路儲存設備漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 192.159.99.95 | NL | SERVICES-1337-GMBH 1337-SERVICES-GMBH-NETWORK, DE |
| 2 | 104.194.155.33 | SG | ROUTERHOSTING, US |
| 3 | 204.76.203.27 | NL | PFCLOUD Pfcloud UG, DE |
| 4 | 87.121.84.181 | US | VPSVAULTHOST, GB |
| 5 | 155.94.154.218 | US | AS-COLOCROSSING, US |
| 6 | 87.121.84.44 | US | VPSVAULTHOST, GB |
| 7 | 87.121.84.52 | US | VPSVAULTHOST, GB |
| 8 | 121.127.232.63 | HK | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK |
| 9 | 107.172.75.229 | US | AS-COLOCROSSING, US |
| 10 | 176.65.148.246 | NL | PFCLOUD Pfcloud UG, DE |

資料來源： 資安院整理

表39 GeoServer 地理位置資訊伺服器漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 103.252.89.75 | DE | SYNLINQ synlinq.de, DE |
| 2 | 103.163.119.65 | VN | BKH-AS-VN BKHOST TECHNOLOGY VIETNAM JOINT STOCK COMPANY, VN |
| 3 | 103.130.215.154 | VN | BKHOST-AS-VN Vietnam Online Network Solution Joint Stock |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| | | | Compnay, VN |
| 4 | 113.186.100.110 | VN | VNPT-AS-VN VNPT Corp, VN |
| 5 | 193.142.147.209 | DE | COLOCATEL-INC Colocatel Network - High Bandwidth Dedicated Servers, SC |
| 6 | 152.53.132.183 | DE | NETCUP-AS netcup GmbH, DE |
| 7 | 149.129.237.250 | ID | ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN |
| 8 | 8.215.40.165 | ID | ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN |

資料來源： 資安院整理

表40 Apache OFBiz 企業資源規劃系統漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 121.127.232.63 | HK | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK |
| 2 | 103.148.245.119 | HK | COGNETCLOUD, US |
| 3 | 202.73.4.152 | BD | IDC-AS-AP Dromatics Systems Pte Ltd, SG |
| 4 | 149.88.89.30 | US | FD-298-8796, US |
| 5 | 202.73.4.57 | HK | IDC-AS-AP Dromatics Systems Pte Ltd, SG |
| 6 | 107.172.75.229 | US | AS-COLOCROSSING, US |
| 7 | 202.73.4.58 | HK | IDC-AS-AP Dromatics Systems Pte Ltd, SG |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 8 | 43.251.225.234 | HK | COGNETCLOUD, US |
| 9 | 47.243.51.220 | US | ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN |
| 10 | 202.155.141.37 | HK | IDC-AS-AP Dromatics Systems Pte Ltd, SG |

資料來源： 資安院整理

表41 Citrix NetScaler 設備漏洞探測前 10 大威脅資訊

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 107.173.135.116 | US | AS-COLOCROSSING, US |
| 2 | 43.153.5.160 | US | TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN |
| 3 | 198.12.111.122 | US | AS-COLOCROSSING, US |
| 4 | 107.172.75.229 | US | AS-COLOCROSSING, US |
| 5 | 170.106.81.52 | US | TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN |
| 6 | 170.106.176.235 | US | TENCENT-NET-AP-CN Tencent Building, Kejizhongyi Avenue, CN |
| 7 | 192.227.155.181 | US | AS-COLOCROSSING, US |
| 8 | 107.173.135.116 | US | AS-COLOCROSSING, US |

資料來源： 資安院整理

### 3.5.2 遠端控制類風險

遠端控制類風險係指使用者透過網路協定或應用服務，進行遠端操作系統設備行為，因此相關設備開放遠端操作服務常成為駭客攻擊目標，進而成為受駭設備遭惡意利用，機關設備若無相關管理需求，建議關閉遠端操作服務。以下彙整近期遠端控制類別前 10 大 IoA，供機關進行聯防參考，詳見表 42 至表 44。

表42 RDP 遠端桌面前 10 大 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 147.124.210.240 | US | MAJESTIC-HOSTING-01, US |
| 2 | 66.63.188.46 | CA | AS-COLOCROSSING, US |
| 3 | 122.252.227.229 | IN | RAILTEL-AS-IN RailTel Corporation of India Ltd, IN |
| 4 | 94.26.88.96 | BG | MEVSPACE, PL |
| 5 | 185.156.73.173 | UA | FDN3, UA |
| 6 | 92.63.197.9 | UA | FDN3, UA |
| 7 | 185.156.73.24 | UA | FDN3, UA |
| 8 | 185.156.73.62 | UA | FDN3, UA |
| 9 | 185.156.73.59 | UA | FDN3, UA |
| 10 | 185.156.73.69 | UA | FDN3, UA |

資料來源： 資安院整理

表43 Telnet 遠端控制前 10 大 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 194.50.16.36 | NL | AS49870-BV, NL |
| 2 | 91.243.177.78 | DE | DAINTERNATIONALGROUP, BG |
| 3 | 165.140.240.2 | US | WEBNX, US |
| 4 | 91.148.141.14 | BG | DAINTERNATIONALGROUP, BG |
| 5 | 185.243.5.189 | HK | RELIABLESITE, US |
| 6 | 37.49.226.210 | NL | PUSHPKT, EE |
| 7 | 104.152.48.26 | BG | DAINTERNATIONALGROUP, BG |
| 8 | 185.224.128.25 | NL | AS49870-BV, NL |
| 9 | 185.205.209.170 | BG | BELCLOUD Premium IP transit network, BG |
| 10 | 20.9.185.246 | US | MICROSOFT-CORP-MSN-AS-BLOCK, US |

資料來源： 資安院整理

表44 VNC 遠端控制前 10 大 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 140.235.18.105 | US | DYNU, US |
| 2 | 140.235.17.49 | US | DYNU, US |
| 3 | 140.235.17.46 | US | DYNU, US |
| 4 | 140.235.19.17 | US | DYNU, US |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 5 | 72.51.56.6 | US | DYNU, US |
| 6 | 207.174.3.224 | US | DYNU, US |
| 7 | 72.51.57.7 | US | DYNU, US |
| 8 | 140.235.17.65 | US | DYNU, US |
| 9 | 140.235.18.167 | US | DYNU, US |
| 10 | 207.174.2.241 | US | DYNU, US |

資料來源： 資安院整理

### 3.5.3 資料庫與檔案服務類風險

資料庫與檔案服務類風險係指駭客對資料庫與檔案伺服器進行通行碼暴力破解、SQL 資料隱碼攻擊或對資料庫已知弱點進行探測，進而對資料進行惡意利用、資訊洩漏或加密勒索等行為，以下彙整近期資料庫類前 10 大 IoA 供機關進行聯防參考，詳見表 45 至表 48。建議機關設置防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠，過濾異常連線。

表45 SQL 資料隱碼攻擊前 10 大 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 104.194.155.33 | SG | ROUTERHOSTING, US |
| 2 | 104.36.50.56 | US | HOSTROYALE, IN |
| 3 | 107.172.75.229 | US | AS-COLOCROSSING, US |
| 4 | 107.173.135.116 | US | AS-COLOCROSSING, US |
| 5 | 121.127.232.63 | HK | CTGSERVERLIMITED-AS-AP |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| | | | CTG Server Limited, HK |
| 6 | 128.14.230.229 | US | UCLOUD-HK-AS-AP UCLOUD INFORMATION TECHNOLOGY HK LIMITED, HK |
| 7 | 134.122.136.96 | JP | CTGSERVERLIMITED-AS-AP CTG Server Limited, HK |
| 8 | 149.129.237.250 | ID | ALIBABA-CN-NET Alibaba US Technology Co., Ltd., CN |
| 9 | 155.94.154.218 | US | AS-COLOCROSSING, US |
| 10 | 156.224.139.119 | HK | MYCLOUD-AS-AP LUOGELANG FRANCE LIMITED, HK |

資料來源： 資安院整理

表46 MSSQL 資料庫前 10 大大量嘗試登入 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 112.223.67.166 | KR | LGDACOM LG DACOM Corporation, KR |
| 2 | 149.202.79.152 | FR | OVH, FR |
| 3 | 151.241.154.124 | AE | VIRTUO, CA |
| 4 | 151.241.154.127 | AE | VIRTUO, CA |
| 5 | 154.194.250.173 | HK | ANSHENG-AS-AP Ansheng Network Technology Co., Limited, HK |
| 6 | 157.173.116.83 | FR | CONTABO, DE |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 7 | 158.220.124.148 | FR | CONTABO, DE |
| 8 | 160.119.253.169 | ZA | Host-Africa-AS, ZA |
| 9 | 180.149.32.107 | US | US-CLOUDNIUM-01, US |
| 10 | 195.154.176.27 | FR | Online SAS, FR |

資料來源： 資安院整理

表47 MySQL 資料庫前 10 大大量嘗試登入 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 103.118.150.170 | IN | KVBPL-AS-IN Kerala Vision Broad Band Private Limited, IN |
| 2 | 103.130.18.209 | ID | MYREPUBLIC-AS-ID PT. Eka Mas Republik, ID |
| 3 | 103.139.127.10 | ID | IDNIC-MITRACOM-ID PT. MITRACOM SOLUSI TEKNOLOGI, ID |
| 4 | 103.156.17.131 | ID | RSTNET-AS-ID RSTNET, ID |
| 5 | 103.215.25.250 | ID | ICONPLN-ID-AP-ISP PT INDONESIA COMNETS PLUS, ID |
| 6 | 121.137.139.49 | KR | KIXS-AS-KR Korea Telecom, KR |
| 7 | 173.197.14.231 | US | TWC-11427-TEXAS, US |
| 8 | 176.65.132.30 | NL | PFCLOUD Pfcloud UG, DE |
| 9 | 180.149.32.98 | US | US-CLOUDNIUM-01, US |

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 10 | 180.149.32.99 | US | US-CLOUDNIUM-01, US |

資料來源： 資安院整理

表48 PostgreSQL 資料庫前 10 大大量嘗試登入 IoA

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 103.219.207.42 | IN | KNETISP-AS K Net Solutions Pvt Ltd, IN |
| 2 | 103.43.71.160 | US | CYBERFORESTLLC-AS-AP CyberForest LLC., AP |
| 3 | 118.223.123.161 | KR | SKB-AS SK Broadband Co Ltd, KR |
| 4 | 124.40.255.210 | ID | LDP-AS-ID Lintas Data Prima, PT, ID |
| 5 | 131.72.168.61 | VE | SISTEMAS TELCORP, C.A., VE |
| 6 | 132.145.96.147 | CA | ORACLE-BMC-31898, US |
| 7 | 141.98.11.173 | LT | HOSTBALTIC, LT |
| 8 | 162.245.188.213 | US | IS-AS-1, US |
| 9 | 181.115.151.50 | BO | EMPRESA NACIONAL DE TELECOMUNICACIONES SOCIEDAD ANONIMA, BO |
| 10 | 185.143.243.146 | US | AS40676, US |

資料來源： 資安院整理

### 3.5.4 後門與木馬程式類風險

後門與木馬程式類風險係指駭客對受駭系統進行後門或木馬程式行為，包含後門程式散布、後門連線報到及後門連線管理行為，以下彙整近期前 10 大 IoA 供機關進行聯防參考，詳見表 49。建議機關定期盤點系統服務，設置防火牆規則，確認個別系統僅開放所需對外提供服務之通訊埠，過濾內外部異常網路連線，並定期進行監控，針對系統異常通訊埠與連線行為進行評估分析。

表49 蟻劍(AntSword)後門連線 IoA[8]

| 編號 | IoA | 國別 | 自治系統名稱(ASNAME) |
|---|---|---|---|
| 1 | 45.147.46.213 | TR | HOSTINGDUNYAM HOSTING DUNYAM, TR |

資料來源： 資安院整理

本月報提供之相關威脅指標包含 IP、DN 及 URL 型，分類彙整後發布於國家資通安全通報應變網站，供機關與資安監控服務廠商進行聯防監控部署參考。

[8] 蟻劍(AntSword)後門連線 IoA，經分析人員驗證後未達 10 項。

## 4. 聯防監控有效性驗證

資安院聯防監控有效性驗證對象為，具備通過政府領域聯防監控連通測試之資安監控服務廠商，其廠商名單請參考資安院官網聯防監控專區[6]。將資安監控服務廠商回傳之資安監控情資，進行監控有效性驗證，其驗證項目構面分 3 面向，分別為「回傳能力」、「偵測能力」及「情資品質」，各驗證構面細分驗證分析指標，以評估回傳之資安監控情資之有效性，每季於 3 月、6 月、9 月及 12 月之資安聯防監控月報呈現該季有效性驗證結果，供政府機關與資安監控服務廠商參考。

### 4.1 聯防監控驗證項目說明

以下依據有效性驗證之分析指標、計算方式及統計呈現方式進行說明，驗證分析指標說明有效性詳見表 50，驗證分析指標之計算說明詳見表 51，驗證分析指標統計呈現方式綜整詳見表 52。

表50 聯防監控有效性驗證項目說明

| 項目 | 分析指標 | 驗證標的 |
|---|---|---|
| 1.回傳能力 | 1.1 資安監控情資格式與回傳率 | 1.1.1 依據「政府領域聯防監控作業規範」規定之「資安監控單」、「情資分析單」及「監控設備狀況單」格式與回傳頻率進行正確性驗證 |
| | 1.2 資安防護項目回傳率 | 1.2.1 依據資安監控服務廠商回傳「監控設備狀況單」之資安防護項目資訊，評估其監控偵測之回傳情形 |
| 2.偵測能力 | 2.1 網路攻防演練驗證 | 2.1.1 以機關網路攻防演練狀況，評估資安監控服務廠商偵測能力 |
| | 2.2 資安院資安警訊驗證 | 2.2.1 以機關被通知之資安警訊，評估資安監控服務廠商偵測能力 |

| | | |
|---|---|---|
| | 2.3 機關通報資安事件驗證 | 2.3.1 以機關主動通報之資安事件，評估資安監控服務廠商偵測能力 |
| | 2.4 DDoS 攻擊偵測驗證 | 2.4.1 以外部情資通知之 DDoS 事件，評估 SOC 業者偵測能力 |
| 3.情資品質 | 3.1 資安監控情資品質分析 | 3.1.1 依據資安監控服務廠商回傳之資安監控情資評估內容正確性 |
| | | 3.1.2 依據資安監控服務廠商回傳之資安監控情資之有效情資回傳率 |
| | | 3.1.3 依據資安監控服務廠商回傳之情資分析單，評估是否有萃取分析之指標情資，包含 IoC 與 IoA |
| | 3.2 資安監控情資回饋能量 | 3.2.1 評估資安監控服務廠商回傳之資安監控情資有無額外回饋資訊，包含網際攻擊狙殺鍊分類資訊(Cyber Kill Chain, CKC)、MITRE ATT&CK、駭客工具、威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等 |
| | | 3.2.2 依據資安監控服務廠商回傳之資安監控情資之 ATT&CK 威脅樣態(Technique)資訊，評估其涵蓋率(ATT&CK 官網最新公告之威脅樣態資訊為準) |
| | | 3.2.3 依據資安監控服務廠商回傳之資安監控情資之情資調查率 |

資料來源：資安院整理

表51 聯防監控有效性驗證項目計算說明

| 項目 | 分析指標 | 計算說明 |
|---|---|---|
| 1.回傳能力 | 1.1 資安監控情資格式與回傳率 | ▪計算項目為「資安監控單正確率」與「情資分析單正確率」，檢視當季資安監控廠商回傳之「資安監控單」與「情資分析單」欄位格式正確數量，以百分比呈現正確情資占比<br>▪統計區間分為「完全正確(100%)」、「大部分正確(90%以上)」、「過半正確(60%以上)」、「少部分正確(少於 60%)」及「無正確(0%)」。計算結果為「未回傳」表示當季資安監控廠商未回傳相關資安監控情資 |
| | 1.2 資安防護項目回傳率 | ▪計算項目為「資安防護項目回傳率」，以資安監控廠商回傳之「監控設備狀況單」數據為基底，比較其回傳之「資安監控單」與「情資分析單」之監控設備涵蓋範圍，以百分比呈現監控設備涵蓋占比。此計算項目趨近於 100%表監控設備正常回傳監控情資，差距 100%越大，表示越多監控設備未回傳監控情資或未如實填報「監控設備狀況單」<br>▪統計區間分為「完全符合(100%)」、「大部分符合(100%±20%)」、「過半符合(100%±40%)」、「少部分符合(超出 100%±60%)」及「未符合(0%)」。計算結果為「未回傳」表示當季資安監控廠商未回傳「監控設備狀況單」 |
| 2.偵測能力 | 2.1 網路攻防演練驗證 | ▪計算項目為「網路攻防演練驗證開單率」，以當季政府機關接獲網路攻防演練入侵攻擊情報警訊，進行通報並結報之資訊，驗證資安監控廠商回傳之資安監控情資是否涵蓋相關入侵攻擊資訊。計算結果為「無結報資 |

| 項目 | 分析指標 | 計算說明 |
| --- | --- | --- |
| | | 訊」表示當季未有相關入侵攻擊情報警訊之政府機關結報資訊 |
| | 2.2 資安院資安警訊驗證 | ▪計算項目為「資安院資安警訊驗證開單率」，以當季政府機關接獲資安院入侵攻擊情報警訊，進行通報並結報之資訊(不含攻防演練警訊)，驗證資安監控廠商回傳之資安監控情資是否涵蓋相關入侵攻擊資訊。計算結果為「無結報資訊」表示當季未有相關入侵攻擊情報警訊之政府機關結報資訊 |
| | 2.3 機關通報資安事件驗證 | ▪計算項目為「機關資安事件通報驗證開單率」，以當季政府機關自主資安通報並結報之資訊，驗證資安監控廠商回傳之資安監控情資是否涵蓋相關自主資安通報資訊。計算結果為「無結報資訊」表示當季未有相關政府機關自主資安通報之結報資訊 |
| | 2.4 DDoS 攻擊偵測驗證 | ▪計算項目為「DDoS 攻擊偵測驗證開單率」，以當季外部情資通知之 DDoS 事件，驗證資安監控廠商回傳之資安監控情資是否涵蓋相關 DDoS 事件。計算結果為「無結報資訊」表示當季未有相關政府機關之 DDoS 事件 |
| 3.情資品質 | 3.1 資安監控情資品質分析 | ▪計算項目為「資安監控情資內容正確性」，檢視當季資安監控廠商回傳之格式正確資安監控情資，計算其內容錯誤之欄位數量<br>▪統計區間分為「完全正確」、「1 個欄位錯誤」、「2 個欄位錯誤」、「3 個以上欄位錯誤」及「未回傳」 |

| 項目 | 分析指標 | 計算說明 |
| --- | --- | --- |
| | | ▪計算項目為「有效情資回傳率」，檢視當季資安監控廠商回傳之「資安監控單」，其事件類別非「其他」之監控情資數量百分比<br>▪統計區間分為「多數有效(80%以上)」、「過半有效(60%以上)」、「半數有效(40%以上)」、「少數有效(少於 40%)」及「無效(0%)」。計算結果為「未回傳」表示當季資安監控廠商未回傳相關資安監控情資 |
| | | ▪計算項目為「萃取分析之指標情資」，檢視當季資安監控廠商回傳之「情資分析單」，評估是否涵蓋 50%以上「情資分析單」數量，能萃取分析並填報規定之指標情資，包含：具備 IoC、IoA 等<br>▪方框填滿表資安監控廠商回傳之「情資分析單」符合上述評估標準 |
| | 3.2 資安監控情資回饋能量 | ▪計算項目為「額外回饋情資」，檢視當季資安監控服務廠商回傳之「情資分析單」，評估是否涵蓋 80%以上「情資分析單」數量，能展現其監控服務能量之項目，可包含：網際攻擊狙殺鍊分類資訊(Cyber Kill Chain, CKC)分類資訊、MITRE ATT&CK、、駭客工具與威脅手法分析情資、跨機關關聯性事件情資或重大資安弱點資訊等<br>▪方框填滿表資安監控廠商回傳之「情資分析單」符合上述評估標準 |
| | | ▪計算項目為「威脅樣態涵蓋率」，檢視當季資安監控服務廠商回傳之「情資分析單」，評估其 ATT&CK 威脅樣態(Technique)資訊 |

| 項目 | 分析指標 | 計算說明 |
|---|---|---|
| | | 是否涵蓋 ATT&CK 官網公告之威脅樣態資訊 20%以上<br>▪ 方框填滿表資安監控廠商回傳之「情資分析單」符合上述評估標準 |
| | | ▪ 計算項目為「情資調查率」，檢視當季資安監控服務廠商回傳之資安監控情資，評估其「資安監控單」之「其他」情資，經監控人員調查分析後，進行正確分類並彙整為「情資分析單」之情資調查百分比<br>▪ 統計區間分為「完全調查(100%)」、「大部分調查(90%以上)」、「過半調查(60%以上)」、「少部分調查(少於 40%)」及「未調查(0%)」。計算結果為「未回傳」表示當季資安監控廠商未回傳相關資安監控情資 |

資料來源：資安院整理

表52 聯防監控有效性驗證項目統計呈現方式綜整

| 項目 | 分析指標 | 項目名稱 | 統計呈現方式 |
|---|---|---|---|
| 1.回傳能力 | 1.1 資安監控情資格式與回傳率 | 資安監控情資格式與回傳率 | ▪ 完全正確(100%)<br>▪ 大部分正確(90%以上)<br>▪ 過半正確(60%以上)<br>▪ 少部分正確(少於 60%)<br>▪ 無正確(0%)<br>▪ 未回傳(未回傳相關資安監控情資) |
| | 1.2 資安防護項目回傳率 | 資安防護項目回傳率 | ▪ 完全符合(100%)<br>▪ 大部分符合(100%±20%)<br>▪ 過半符合(100%±40%) |

| 項目 | 分析指標 | 項目名稱 | 統計呈現方式 |
|---|---|---|---|
| | | | ▪ 少部分符合(超出 100%±60%)<br>▪ 未符合(0%)<br>▪ 未回傳(未回傳相關資安監控情資) |
| 2.偵測能力 | 2.1 網路攻防演練驗證 | 網路攻防演練驗證開單率 | ▪ 以百分比呈現，統計母數屬該資安監控服務廠商監控範圍之網路攻防演練警訊數量<br>▪ 無結報資訊(表示無入侵攻擊情報警訊之政府機關結報資訊) |
| | 2.2 資安院資安警訊驗證 | 資安院資安警訊驗證開單率 | ▪ 以百分比呈現，統計母數屬該資安監控服務廠商監控範圍之入侵攻擊情報警訊數量<br>▪ 無結報資訊(表示無入侵攻擊情報警訊之政府機關結報資訊) |
| | 2.3 機關通報資安事件驗證 | 機關資安事件通報驗證開單率 | ▪ 以百分比呈現，統計母數屬該資安監控服務廠商監控範圍之自主資安通報數量<br>▪ 無結報資訊(表示無政府機關自主資安通報之結報資訊) |
| | 2.4 DDoS 攻擊偵測驗證 | DDoS 攻擊偵測驗證開單率 | ▪ 以百分比呈現，統計母數屬該資安監控服務廠商監控範圍之 DDOS 通知數量<br>▪ 無結報資訊(表示政府機關未回傳相關情資) |
| 3.情資品質 | 3.1 資安監控情資品質分析 | 資安監控情資內容正確性 | ▪ 完全正確<br>▪ 1 個欄位錯誤<br>▪ 2 個欄位錯誤<br>▪ 3 個以上欄位錯誤 |

| 項目 | 分析指標 | 項目名稱 | 統計呈現方式 |
|---|---|---|---|
| | | | ▪ 未回傳(未回傳相關資安監控情資) |
| | | 有效情資回傳率 | ▪ 多數有效(80%以上)<br>▪ 過半有效(60%以上)<br>▪ 半數有效(40%以上)<br>▪ 少數有效(少於 40%)<br>▪ 無效(0%)<br>▪ 未回傳(未回傳相關資安監控情資) |
| | | 萃取分析之指標情資 | ▪ 達標(表涵蓋 50%以上情資分析單數量) |
| | 3.2 資安監控情資回饋能量 | 額外回饋情資 | ▪ 達標(表涵蓋 80%以上情資分析單數量) |
| | | ATT&CK 威脅樣態涵蓋率 | ▪ 達標(表涵蓋 20%以上 ATT&CK 威脅樣態數量) |
| | | 情資調查率 | ▪ 完全調查(100%)<br>▪ 大部分調查(90%以上)<br>▪ 過半調查(60%以上)<br>▪ 少部分調查(少於 40%)<br>▪ 未調查(0%)<br>▪ 未回傳(未回傳相關資安監控情資) |

資料來源：資安院整理

## 4.2 政府領域資安監控服務廠商之監控有效性驗證統計

資安院依據聯防監控有效性驗證項目，統計 114 年第 4 季資安監控服務廠商各分析指標之表現，以呈現政府領域資安監控服務廠商之監控有效性能

量，詳見表 53 至表 56。

表53 政府領域資安監控服務廠商之監控有效性驗證－回傳能力

| 編號 | 資安監控服務廠商 | 回傳能力 | |
|---|---|---|---|
| | | 資安監控情資格式與回傳率 | 資安防護項目回傳率 |
| 1 | 中華資安國際股份有限公司 | 大部分正確 | 大部分符合 |
| 2 | 白帽犀牛有限公司 | 少部分正確 | 少部分符合 |
| 3 | 安碁資訊股份有限公司 | 完全正確 | 大部分符合 |
| 4 | 果核數位股份有限公司 | 大部分正確 | 大部分符合 |
| 5 | 凌群電腦股份有限公司 | 完全正確 | 過半符合 |
| 6 | 智慧資安股份有限公司 | 大部分正確 | 大部分符合 |
| 7 | 華電聯網股份有限公司 | 完全正確 | 大部分符合 |
| 8 | 雲智維科技股份有限公司 | 大部分正確 | 完全符合 |
| 9 | 漢昕科技股份有限公司 | 過半正確 | 完全符合 |
| 10 | 數聯資安股份有限公司 | 完全正確 | 大部分符合 |
| 11 | 線上探索科技有限公司 | 少部分正確 | 少部分符合 |
| 12 | 關貿網路股份有限公司 | 大部分正確 | 少部分符合 |

資料來源：資安院整理

表54 政府領域資安監控服務廠商之監控有效性驗證－偵測能力

| 編號 | 資安監控服務廠商 | 偵測能力 | | | |
|---|---|---|---|---|---|
| | | 網路攻防演練驗證開單率 | 資安院資安警訊驗證開單率 | 機關通報資安事件驗證開單率 | DDoS 攻擊偵測驗證開單率 |
| 1 | 中華資安國際股份有限公司 | 0.00% | 0.00% | 33.33% | 無結報資訊 |
| 2 | 白帽犀牛有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |
| 3 | 安碁資訊股份有限公司 | 50.00% | 58.33% | 100.00% | 50.00% |
| 4 | 果核數位股份有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |
| 5 | 凌群電腦股份有限公司 | 無結報資訊 | 0.00% | 無結報資訊 | 無結報資訊 |
| 6 | 智慧資安股份有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |
| 7 | 華電聯網股份有限公司 | 無結報資訊 | 0.00% | 0.00% | 無結報資訊 |
| 8 | 雲智維科技股份有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |
| 9 | 漢昕科技股份有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |
| 10 | 數聯資安股份有限公司 | 無結報資訊 | 100.00% | 0.00% | 無結報資訊 |
| 11 | 線上探索科技有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |

| 編號 | 資安監控服務廠商 | 偵測能力 | | | |
|---|---|---|---|---|---|
| | | 網路攻防演練驗證開單率 | 資安院資安警訊驗證開單率 | 機關通報資安事件驗證開單率 | DDoS 攻擊偵測驗證開單率 |
| 12 | 關貿網路股份有限公司 | 無結報資訊 | 無結報資訊 | 無結報資訊 | 無結報資訊 |

資料來源：資安院整理

表55 政府領域資安監控服務廠商之監控有效性驗證－情資品質

| 編號 | 資安監控服務廠商 | 情資品質 | | |
|---|---|---|---|---|
| | | 資安監控情資內容正確性 | 有效情資回傳率 | 萃取分析之指標情資 |
| 1 | 中華資安國際股份有限公司 | 完全正確 | 多數有效 | 達標 |
| 2 | 白帽犀牛有限公司 | 3 個以上欄位錯誤 | 過半有效 | 未達標 |
| 3 | 安碁資訊股份有限公司 | 完全正確 | 多數有效 | 達標 |
| 4 | 果核數位股份有限公司 | 完全正確 | 多數有效 | 未達標 |
| 5 | 凌群電腦股份有限公司 | 完全正確 | 多數有效 | 未達標 |
| 6 | 智慧資安股份有限公司 | 完全正確 | 少數有效 | 未達標 |
| 7 | 華電聯網股份有限公司 | 完全正確 | 多數有效 | 達標 |
| 8 | 雲智維科技股份有限公司 | 完全正確 | 多數有效 | 未達標 |
| 9 | 漢昕科技股份有限公司 | 完全正確 | 多數有效 | 達標 |
| 10 | 數聯資安股份有限公司 | 完全正確 | 多數有效 | 達標 |

| 編號 | 資安監控服務廠商 | 情資品質 | | |
|---|---|---|---|---|
| | | 資安監控情資內容正確性 | 有效情資回傳率 | 萃取分析之指標情資 |
| 11 | 線上探索科技有限公司 | 3 個以上欄位錯誤 | 無效或未回傳 | 未達標 |
| 12 | 關貿網路股份有限公司 | 完全正確 | 多數有效 | 達標 |

資料來源：資安院整理

表56 政府領域資安監控服務廠商之監控有效性驗證－情資品質(續)

| 編號 | 資安監控服務廠商 | 情資品質 | | |
|---|---|---|---|---|
| | | 額外回饋情資 | 威脅樣態涵蓋率 | 情資調查率 |
| 1 | 中華資安國際股份有限公司 | 達標 | 達標 | 過半調查 |
| 2 | 白帽犀牛有限公司 | 未達標 | 未達標 | 未調查 |
| 3 | 安碁資訊股份有限公司 | 達標 | 達標 | 未調查 |
| 4 | 果核數位股份有限公司 | 未達標 | 未達標 | 未調查 |
| 5 | 凌群電腦股份有限公司 | 未達標 | 未達標 | 未調查 |
| 6 | 智慧資安股份有限公司 | 達標 | 未達標 | 未調查 |
| 7 | 華電聯網股份有限公司 | 達標 | 未達標 | 未調查 |
| 8 | 雲智維科技股份有限公司 | 未達標 | 未達標 | 未調查 |
| 9 | 漢昕科技股份有限公司 | 達標 | 未達標 | 未調查 |
| 10 | 數聯資安股份有限公司 | 達標 | 達標 | 少部分調查 |

| 編號 | 資安監控服務廠商 | 情資品質 | | |
|---|---|---|---|---|
| | | 額外回饋情資 | 威脅樣態涵蓋率 | 情資調查率 |
| 11 | 線上探索科技有限公司 | 未達標 | 未達標 | 未調查 |
| 12 | 關貿網路股份有限公司 | 達標 | 未達標 | 未調查 |

資料來源：資安院整理

## 5. 參考文獻

[1]Traffic Light Protocol (TLP) Definitions and Usage, https://www.us-cert.gov/tlp

[2]RiskIQ PassiveTotal, https://www.passivetotal.org/

[3]VirusTotal, https://www.virustotal.com/

[4]Google Safe Browsing, https://transparencyreport.google.com/safe-browsing/search

[5]CVE.org - Search CVE Site, https://www.cve.org/SiteSearch

[6]國家資通安全研究院聯防監控專區 https://www.nics.nat.gov.tw/GSOC?lang=zh

[7]MITRE ATT&CK 官網 https://attack.mitre.org/

[8]CVE-202514847 漏洞資訊 https://nvd.nist.gov/vuln/detail/CVE-202514847

[9]MongoDB 官方安全性建議 https://jira.mongodb.org/browse/SERVER-115508

[10]CISA KEV 公告 https://www.cisa.gov/known-exploited-vulnerabilities-catalog

# 附件

附件 1 公務機關業務類別與資安責任等級說明

附件 2 資安情資類別說明

## 附件1 公務機關業務類別與資安責任等級說明

為綜整分析各不同業務屬性之公務機關受威脅情形，本月報將 SOC 監控之「政府機關」參考行政院業務分工區分為：內政衛福勞動、外交國防法務、交通環境資源、財政主計金融、經濟能源農業及教育科學文化等 6 類，再加上綜合行政(含行政院非屬前 6 類之機關及省、直轄市、縣市政府等)及非行政院(總統府、四院及其所屬)，共計 8 類詳見表 57。另外，依資安責任等級區分公務機關為 A、B、C、D 及 E 共 5 級機關詳見表 58。

表57 各業務類別公務機關數量[9]

| 機關類型 | 業務類別 | 機關個數 |
|---|---|---|
| 公務機關 | 綜合行政 | 6,391 |
| | 內政衛福勞動 | 110 |
| | 外交國防法務 | 198 |
| | 交通環境資源 | 111 |
| | 財政主計金融 | 52 |
| | 經濟能源農業 | 96 |
| | 教育科學文化 | 278 |
| | 非行政院 | 76 |
| 小計 | | 7,312 |

資料來源：資安院整理

[9]各業務類別排序參考行政院院本部組織架構圖。

表58 各資安等級公務機關數量[10]

| 機關類型 | 資安等級 | 機關個數 |
|---|---|---|
| 公務機關 | A | 49 |
| | B | 221 |
| | C | 892 |
| | D | 5272 |
| | E | 872 |
| 小計 | | 7,306 |

資料來源：資安院整理

[10]參考資通安全責任等級分級辦法

## 附件2 資安事件分類說明

本月報資安情資類別，係參照國家資通安全研究院所公布之 N-SOC 情資類別共 10 類，其定義詳見表 59，詳細內容請詳見國家資通安全研究院之聯防監控專區資訊[11]。

表59 政府領域聯防監控月報情資類別說明

| 編號 | 資安事件分類 | 說明 |
|---|---|---|
| 1 | 惡意內容 | 針對透過文字、照片、影片等形式散播不當內容之情資，如：<br>▪網頁惡意留言<br>▪寄送垃圾郵件 |
| 2 | 惡意程式 | 針對與相關惡意程式之情資，如：<br>▪散播惡意程式<br>▪系統存在惡意程式 |
| 3 | 資訊蒐集 | 針對透過掃描、探測及社交工程等攻擊手法取得資訊之情資 |
| 4 | 入侵嘗試 | 針對嘗試入侵未經授權(Authorization)主機之情資，如：<br>▪試圖透過暴力破解或利用已知與未知漏洞等攻擊手法，嘗試破壞與干擾系統與服務之嘗試 |
| 5 | 入侵攻擊 | 針對系統與服務成功破壞行為，造成未經授權(Unauthorized)存取或取得系統/服務資源與權限，包含成為殭屍網路之受害者。 |

[11] 國家資通安全研究院之聯防監控專區 (https://www.nics.nat.gov.tw/GSOC?lang=zh)

| 編號 | 資安事件分類 | 說明 |
|---|---|---|
| 6 | 服務阻斷 | 針對影響服務可用性(Availability)或造成服務中斷之攻擊情資，如：<br>▪ 阻斷服務攻擊 |
| 7 | 資訊內容安全 | 針對系統遭未經身分鑑別(Authentication)存取或影響資訊機敏性(Confidentiality)之情資，如：<br>▪ 機敏資訊外洩 |
| 8 | 詐欺攻擊 | 針對偽冒他人身分、系統服務及組織等進行攻擊行為之情資，如：<br>▪ 釣魚郵件<br>▪ 釣魚網站 |
| 9 | 系統弱點 | 針對系統存在弱點之情資，可能遭利用進而影響系統機敏性(Confidentiality)、完整性(Integrity)或可用性(Availability)，分享相關資訊予特定會員 |
| 10 | 其他 | 分享非屬前述情資類別之情資 |

資料來源：資安院整理