112年第2季資通安全技術報告

Quarterly Technical Report

國家資通安全研究院

National Institute of Cyber Security

目　次

1. 資安威脅現況與防護重點 3
1.1 全球資安威脅現況 3
1.2 政府資安威脅現況 5
1.3 資安防護重點 8
2. 資安專題分享_BlackTech 駭客族群反鑑識手法研究 10
2.1 駭客入侵手法分析與實證 10
3. 資安技術研析_ Text4shell 弱點研析與驗證實作 16
3.1 弱點成因分析 16
3.2 弱點攻擊驗證實作與修補方式 21
4. 結論 24
資安相關活動 25
112 年第 1 次政府資通安全防護巡迴研討會 25

圖 目 次

圖 1　112 年第 2 季通報事件影響等級比率圖 6
圖 2　112 年第 2 季通報類型比率圖 7
圖 3　112 年第 2 季資安事件發生原因比例圖 8
圖 4　惡意程式建立時間顯示相同 11
圖 5　惡意程式 Standard Information 中之 Metadata Time 12
圖 6　透過 Powershell 指令改變 Standard Information 時間 13
圖 7　鑑識工具分析 MFT 13
圖 8　FN 時間自動對應 SI 時間 14
圖 9　一般日誌記錄流程 18
圖 10　發送含惡意程式之網址 18
圖 11　字串插值建立惡意檔案 19
圖 12　url 前綴弱點驗證實作步驟 20
圖 13　DNS 前綴弱點驗證實作步驟 21
圖 14　傳送測試 payload 21
圖 15　撰寫 Payload 22
圖 16　以 Text4shell 下載並執行 Shell 腳本 22
圖 17　建立 Reverse Shell 22

摘要

「第 2 季資通安全技術報告」除分析本季全球資安威脅、政府通報資安事件外，並提供相對應之資安防護建議。同時，藉由資安專題分享與資安技術研析，提供政府機關需關注之資安風險重點。

「第 2 季資通安全技術報告」分為以下 4 個章節。

●資安威脅現況與防護重點

從分析全球資安威脅現況開始，第 1 起案例為駭客組織揚言公開美國知名社群討論平台之機敏資料；另外一起案例為 TP-Link AX21 路由器遭新型惡意程式利用於部署 DDoS 攻擊之殭屍網路。

分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」(占 61.34%)類型為主，排除綜合類型「其他」外，其次分別為「設備問題」(占 6.32%)與「網頁攻擊」(占 6.32%)為主要通報類型。

●資安專題分享

資安專題分享主題為 BlackTech 駭客族群反鑑識手法研究，BlackTech 鎖定東南亞與美國相關組織為入侵目標，竊取目標對象之機敏資訊。該組織運用可支援惡意程式之合法工具執行攻擊行動。於某次事件鑑識研究時，發現駭客運用特殊手法修改檔案時間，因此針對此手法進行相關研究，以期能精準判斷駭客入侵時間與進行相關攻擊資訊分析。

●資安技術研析

資安技術研析主題為 Text4shell 弱點研析與驗證實作，根據資安業者研究報告指出此弱點為高風險弱點，可讓駭客輕易入侵，因此將針對 Text4Shell 弱點(CVE-2022-42899)進行研析與驗證實作。

●結論

本報告透過分析全球與政府之資安事件與統計數據，了解最新資安威脅趨勢與因應之資安防護重點。資安專題分享 BlackTech 駭客族群反鑑識手法研究，了解此組織如何運用特殊手法修改檔案時間，以干擾鑑識活動之進行。此外，Text4shell 弱點研析與驗證實作，當駭客利用此弱點，將可成功發起遠端程式碼執行之攻擊，因此藉由研析與驗證實作，分析其入侵手法，以針對此弱點能適切處理。

1. 資安威脅現況與防護重點

本報告藉由檢視當季國內外所發生之資安事件或議題，研析事件發生之主要原因及可能之衝擊與影響。112 年第 2 季(以下簡稱本季)探討社群媒體所衍生之相關資安議題與網路設備遭新型惡意程式利用 DDoS 攻擊。

本章節之事件與議題皆配合整理相關之資安防護重點，提供政府機關就相關資安風險或議題進行評估，並依循資安管理規範與技術防禦進行強化。

1.1 全球資安威脅現況

AI 聊天機器人 ChatGPT 於 5 月時推出 APP，預料將讓使用者更加輕易使用且依賴 ChatGPT 之人工智慧成果。惟依據資安業者 Group IB 揭露近一年有駭客於暗網上販賣 ChatGPT 帳戶個資之情況，分析應有超過 10 萬筆 ChatGPT 帳戶個資外洩。隨著 AI 等新興科技之盛行，搭配社群媒體之運用，駭客可利用之社交工程手法將更為嫻熟，應預做準備。因此在全球關注 AI 運用之合宜性外，也衍生立法與管理規範之要求與討論，期盼規範 AI 於風險控管情境使用下，亦強調資料隱私之保護。

本季具指標性案例為駭客組織揚言公開美國知名社群討論平台之機敏資料；另外一起案例為 TP-Link AX21 路由器遭新型惡意程式利用於部署 DDoS 攻擊之殭屍網路。

首先，探討案例為駭客組織揚言公開美國大型社群討論平台 Reddit 之機敏資料，Reddit 為美國前五大之社群平台，使用者可將文字、圖片或連結發在於網站上，集結成電子佈告欄功能。根據 Reddit 自行揭露，其系統早於 2 月時遭受駭客攻擊，經內部調查發現此次攻擊來源為一位內部人員因遭到網路釣魚後，成為駭客組織入侵破口。因該入侵行動，致使惡意人士得以存取內部文件、原始碼、員工及部分平台廣告商資料。

勒索軟體駭客組織 ALPHV(又名為 BlackCat)聲稱是 2 月針對 Reddit 發起攻

擊之操盤者，且由該行動共竊取 80G 壓縮檔案，ALPHV 分別於 4 月與 6 月要求 Reddit 支付刪除資料代價之 450 萬美金，在首次未獲回覆後，近日因 Reddit 平台將展開 API 收費機制，ALPHV 認為這是難得機會，再次展開勒贖行動，並威脅公開所竊取之資料，包含 Reddit 是如何追蹤他們使用者之統計數據。

ALPHV 自 110 年崛起後，數個研究組織皆將 ALPHV 列為前十大最活躍之勒索團體，近年持續對全球組織展開網路攻擊造成嚴重危害。ALPHV 使用 Rust 語言程式開發之勒索軟體即服務(Ransomware as a Service)，具備客製且能阻擋偵測與分析惡意程式之功能，因此其隱匿與滲透力藉此持續提升，且由於該組織不斷釋出新版功能，導致此類勒索攻擊事件頻傳。

第 2 起案例為 TP-Link AX21 路由器遭新 Condi 惡意程式利用於部署 DDoS 攻擊之殭屍網路。資安業者 FortiGuard 實驗室揭露由其監控系統所蒐集之 Condi 惡意程式樣本有持續上升之趨勢，代表駭客團體 Condi Network 正積極運用該弱點擴大其殭屍網路勢力範圍。Condi 利用 TP-Link AX21 控制介面存在之 CVE-2023-1389 漏洞，遠距執行惡意程式以控制系統，且該團體甚至推出 DDoS 即服務於 Telegram 社群行銷。

而從所獲集之 Condi 樣本中分析，發現有多種 Shell 編碼版本，意謂著多個駭客組織可能購買 Condi 之 DDoS 即服務，且變動其攻擊方式。因此類型惡意程式於重開機將無法繼續存續，為了能常駐於受害者系統中，會採取刪除用於關閉或重啟系統之二進位檔案。惟遭惡意程式利用之設備，會頻繁出現過熱、網路中斷或設定值遭莫名修改等現象，使用者亦應提高警覺檢視異常之處。

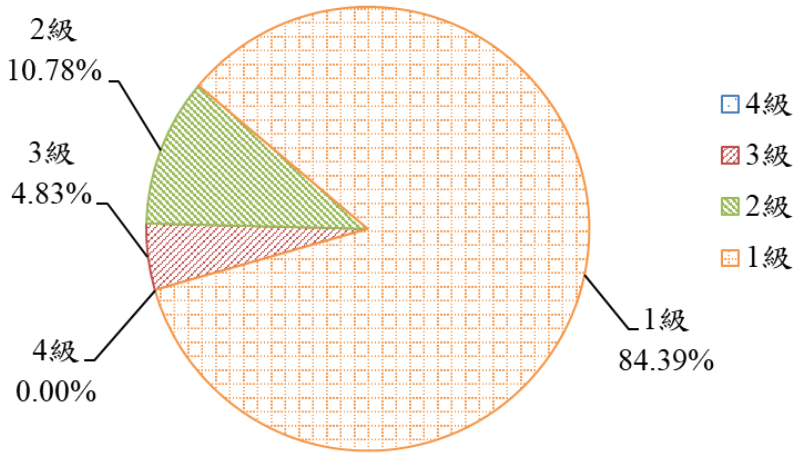
另外一值得省思之處為 CVE-2023-1389 漏洞於今年 1 月時由漏洞懸賞計畫(Zero Day Initiative, ZDI)發布，且設備廠商亦已 2 個月後公告漏洞修補方式，惟從事件攻擊數據顯示，有不少使用者並未進行更新，導致駭客仍廣

為利用該弱點。當然也可能因為此型號之無線路由器主要用戶多為家庭與中小型企業，資安意識明顯不足，且因疫情而增加之家戶使用需求，亦突顯端點設備安全極需全面檢視。

綜覽本季全球資安威脅與資安事件，新興科技崛起，帶來創新與未來發展，同時也造成數位落差、集權等問題。而駭客運用新興科技結合社交工程手法也正在興起，資安認知或相關教育訓練或身分識別等機制更加重要。資訊設備更新涉及之議題包含明確盤點所有使用之設備，包含軟、硬及韌體等範圍，同時發現有些設備因版本過於老舊或因應用系穩定度或可靠性等問無法更新，而此時應尋找維護廠商或專業意見，運用風險分析概念，提出可減緩風險之補償控制措施。

1.2 政府資安威脅現況

彙整本季所接獲之政府機關通報事件，藉由事件之影響等級、通報類型及事件原因，了解目前政府機關之資安威脅現況。通報事件依「機密性」、「完整性」、「可用性」3 個面向所造成之衝擊，將事件影響等級由輕至重分為 1 級、2 級、3 級及 4 級。彙整事件影響等級，本季以 1 級事件占 84.39%為大宗，2 級事件占 10.78%次之，3 級事件僅占 4.83%，而 4 級通報事件則未發生，相關統計情形詳見圖 1。

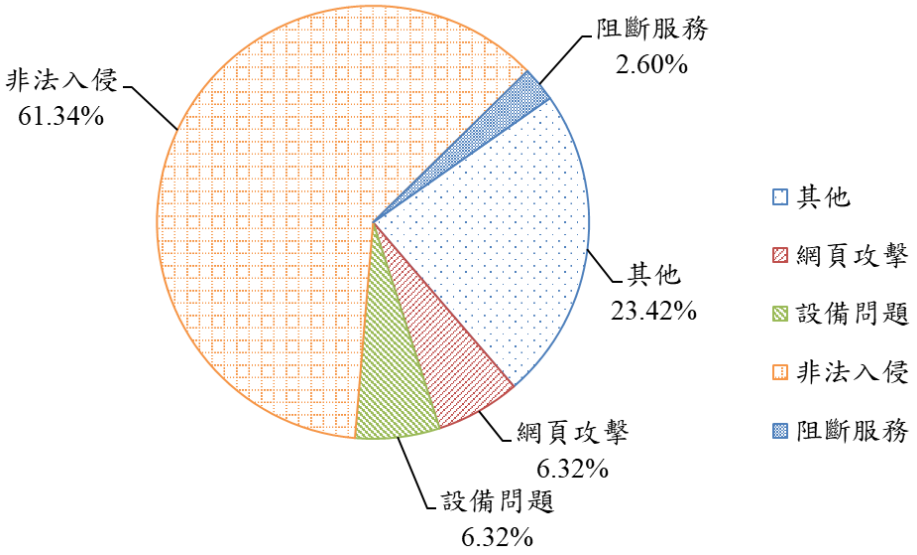


資料來源：本報告整理

圖1　112 年第 2 季通報事件影響等級比率圖

本季接獲之 3 級通報事件，有機關對外網站遭揭露於網站使用資料文件編號，只需修改流水編號後，得以查詢到其他人之個資，包含姓名、身分證字號、戶籍地址等。該機關於事件發生後增加身分驗證功能，避免個資再遭意外洩露。網頁攻擊一直占資安事件通報之比例居高不下，因此若有對外服務之網站上線前，應先進行原始碼檢測或弱點掃描，並定期維護與檢視其安全性。

整體通報事件類型，以「非法入侵」(占 61.34%)類型為主，排除綜合類型「其他」外，「設備問題」與「網頁攻擊」類型次之，詳見圖 2。

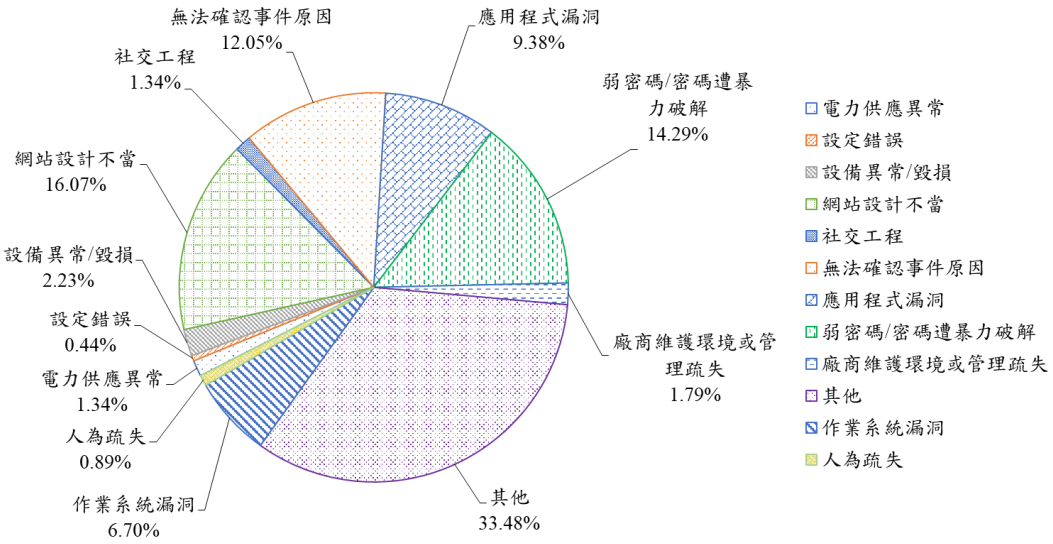


資料來源：本報告整理

圖2　112 年第 2 季通報類型比率圖

非法入侵通報事件中，發現路由器或防火牆等網通設備，因遭植入惡意程式對外連線至殭屍網路報到行為，評估應為近期網通設備屢傳有重大漏洞造成。分析通報事件發生原因，以其他(33.48%)為主，其次分別為網站設計不當(16.07%)、弱密碼/密碼遭暴力破解(14.29%)、無法確認事件原因(12.05%)、應用程式漏洞(9.38 %)、作業系統漏洞(6.7%)、設備異常/毀損(2.23%)、廠商維護環境或管理疏失(1.79 %)、電力供應異常(1.34 %)、社交工程(1.34 %)、人為疏失(0.89 %)及設定錯誤(0.44%)，詳見圖 3。

針對無法確認事件原因，包含因系統預設事件發生原因與事件項目無法對照、無足夠日誌可供追查或尚需進一步調查等，皆會先歸類為其他。在其他案例中，有一事件為因資料庫之系統紀錄檔滿載致影響系統服務，機關除依資通安全管理法確實估算稽核儲存容量外，另外應訂定日誌檔負載率，出現異常時，應積極處理。



資料來源：本報告整理

圖3　112 年第 2 季資安事件發生原因比例圖

分析第 4 季通報類型與通報事件發生原因分析，就實兵演練通報，所占之事件比幾近三成，而發現多數機關因網站存在認證及驗證機制失效弱點遭取得一般使用者權限，或網站存在注入攻擊弱點遭成功寫入攻擊語法。由此可見於系統開發過程中，如何從需求至最後部署維運階段皆需加入安全之概念甚為關鍵。建議若因網站為對外公開之服務，應避免暴露脆弱點，採取多層次防禦架構，除程式安全設計原則外，更應檢視所有端點之安全性，提升整體系統之安全性。

1.3 資安防護重點

分析本季全球資安威脅現況，社交工程能否成功部分取決於面對攻擊手法是否有足夠之認知與技術韌性防止其入侵成功，由社群討論平台 Reddit 之案例得知，當某內部人員遭到網路釣魚攻擊後，就能成功成為駭客組織入侵破口，因此更應強化社交工程演練、認知訓練及端點防護等機制。而面對持續發生之設備更新問題而導致之資安事件，更應了解其問題所在為資產盤點未落實或因有可用性疑慮而未更新，避免同樣事件重複發生。

國內部分從非法入侵通報事件中，網通設備因重大漏洞未更新或設備版本老舊無法及時更新，遭植入惡意程式而發生向殭屍網路報到或木馬程式連線狀況。另外，在事件中亦有委外廠商因發生程式碼外洩，涉及敏感資訊外洩。軟體供應鏈安全已成為現今重要之資安議題，從駭客將優先入侵目標從單純線上環境或設備轉向為軟體供應鏈，主要原因為軟體供應鏈之資安治理成熟度不足或輕忽概念致容易入侵成功。綜整以上資安威脅現況，提供資安防護建議如下：

●網通設備之資安管理

– 盤點並確認機關內部是否存在受影響之設備，因攻擊驗證程式已廣為散播，針對存在漏洞之設備，主動檢視該系統檔案完整性。

– 確認官方網站公告之最新軟、韌體版本，驗證更新對系統之穩定性後，儘速更新。且應限制或關閉設備上之管理介面，並限定可存取來源 IP。

– 所屬設備若為停產或終止維護(End of Life, EOL)之型號，應規劃補償控制措施，緩解措施相關風險。

●程式碼之資安管理

– 設定安全之組態與運用安全之 API，以確保委外程式碼部署之安全。

– 限制程式碼之特權，以最小權限存取原則，維護存取控制清單。

– 若使用開放原始碼，應評估與限制開放原始碼使用範圍，並注意開源軟體漏洞且適時進行原始碼檢測。

2. 資安專題分享_BlackTech 駭客族群反鑑識手法研究

BlackTech 駭客組織自發跡以來，經常鎖定東北亞與美國相關組織為入侵目標，主要攻擊目的為竊取目標對象之機敏資訊。該組織慣於利用反鑑識、反偵測手法開發所需惡意程式，導致資安防禦系統不易偵測其活動，同時亦增加現場針對惡意程式鑑識之難度，藉以隱匿其蹤跡。

BlackTech 針對台灣政府機關與企業之攻擊亦時有發生，近日於某資安事件鑑識時發現為該案件之電腦遭利用做為惡意程式回連之中繼站，研判應為 BlackTech 駭客族群入侵所致。現場蒐證時，除攜回受駭主機之映像檔，同時亦匯出相關日誌檔案，並針對該主機進行相關檢測。

於鑑識研究時，發現於現場所鑑識惡意程式與系統內顯示惡意程式建立時間有出入，推測時間應曾遭駭客修改過。進一步透過分析 Windows NTFS 文件檔案中之系統檔案$MFT，嘗試釐清實際植入時間，發現駭客運用特殊手法修改檔案時間，故決定針對此手法進行相關研究，以期能精準判斷駭客入侵時間與進行相關資訊比對。

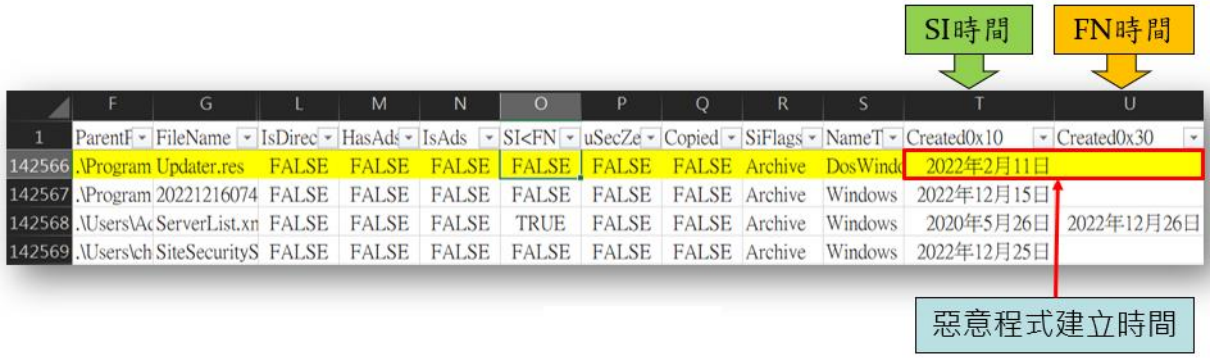
2.1 駭客入侵手法分析與實證

首先說明 NTFS 系統架構與$MFT 紀錄，以逐步分析其時間竄改之步驟。Windows 作業系統支援之硬碟格包含 NTFS、ReFS 及 exFAT 等，而 NTFS 因具有較高之安全與穩定性，且提供多樣功能與紀錄，為廣為大眾接受之 Windows 之硬碟格式。在所有紀錄中，最重要為$MFT 紀錄，該紀錄會標示每個檔案之詳細資訊，例如檔名、內容、時間等。在$MFT 中，有兩個欄位會帶有檔案相關時間，分別為標準資訊(Standard Information, SI)欄位與檔案名稱(File Name, FN)欄位。一般常見之時間標示為 SI，該欄位記錄一組時間，分別為 Creation Time、Last Write Time、Last Access Time 及 Metadata Time (此為隱藏欄位)；FN 欄位會記錄另一組時間，皆為

隱藏欄位，僅能用鑑識工具進行檢視。

因此若要針對檔案時間進行調整，僅能修改 Standard Information Time，無法修改 File Name Time，修改之方式則是透過指令或 API 修改 Standard Information Time。無法修改 File Name Time 原因主要是沒有可用之 API，一般認知若需修改 File Name Time，僅能利用未經驗證或未公開之 API，且有極大可能會被微軟內建之安全機制 PatchGuard 機制阻擋，因此常產生錯誤認知，認為僅有 Standard Information Time 可以修改，而 File Name Time 無法修改，惟早在 108 年就已有資料顯示，FN 並非是不可變更。

此次事件既為駭客成功修改 File Name Time 之案例，該事件經由鑑識分析，惡意程式植入時應為 111 年 12 月，惟受害系統顯示日期為 111 年 2 月，因此特別研究其手法，以期更進一步了解動機。在初始使用鑑識工具對硬碟中$MFT 進行分析時，發現該惡意程式之 Standard Information Time 與 File Name Time 顯示為相同，運用該工具若未顯示 FN 時間，則代表此檔案之 FN 時間與 SI 時間相同，惡意程式為下圖黃色區域，顯示建立時間未經修改，惡意程式植入日期為 111 年 2 月，詳見圖 4。



	F	G	L	M	N	O	P	Q	R	S	T	U
1	ParentF	FileName	IsDirec	HasAds	IsAds	SI<FN	uSecZe	Copied	SiFlags	NameT	Created0x10	Created0x30
142566	.\Program	Updater.res	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	DosWindo	2022年2月11日	
142567	.\Program	20221216074	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Windows	2022年12月15日	
142568	.\Users\Ac	ServerList.xn	FALSE	FALSE	FALSE	TRUE	FALSE	FALSE	Archive	Windows	2020年5月26日	2022年12月26日
142569	.\Users\ch	SiteSecurityS	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE	Archive	Windows	2022年12月25日	

資料來源：本報告整理

圖4　惡意程式建立時間顯示相同

進一步分析該惡意程式相關時間時，意外發現該程式 Standard Information 中之隱藏欄位之 Metadata Time 很接近正確之植入時間，應為 12 月，詳見

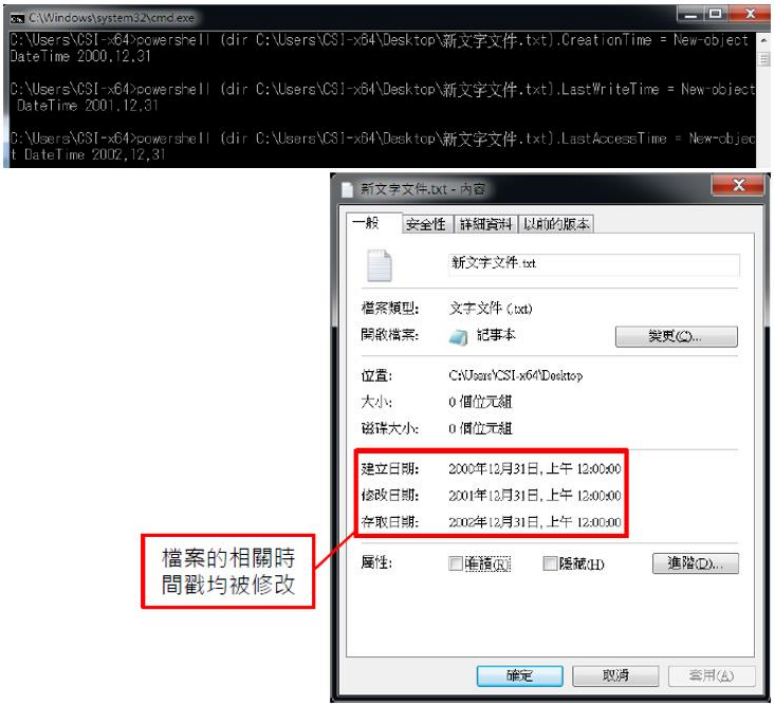
圖 5。

	J	S	T	U	V	X	Y	Z	AA
1	FN_FileN	SI_CTime	SI_ATime	SI_MTime	SI_RTime	FN_CTime	FN_ATime	FN_MTime	FN_RTime
114425	Updater.res	2022/2/11 0:28	2022/2/11 0:28	2022/12/14 23:41	2022/2/11 0:28	2022/2/11 0:28	2022/2/11 0:28	2022/2/11 0:28	2022/2/11 0:28
114426	201D14~1.P	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41	2022/12/15 23:41
114427	SERVER~1.	2020/5/26 18:15	2022/12/26 3:32	2022/12/26 3:32	2022/12/26 3:32	2022/12/26 3:32	2022/12/26 3:32	2022/12/26 3:32	2022/12/26 3:32
114428	SITESE~1.T	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16	2022/12/25 22:16

資料來源：本報告整理

圖5　惡意程式 Standard Information 中之 Metadata Time

為分析與驗證時間遭竄改之手法，於實驗環境對此進行實測，先準備一個檔案，建立日期為 2019/3/5、修改日期 2019/3/5 及存取日期為 2019/3/5。接續透過 Powershell 指令改變 Standard Information 之 3 個時間，異動為建立日期為 2000/12/31、修改日期 2001/12/31 及存取日期為 2002/12/31。詳見圖 6。



資料來源：本報告整理

圖6　透過 Powershell 指令改變 Standard Information 時間

利用鑑識工具分析 MFT 之內容，發現僅有 Standard Information 時間變動，而 File Name 時間並未異動，詳見圖 7。

資料來源：本報告整理

圖7　鑑識工具分析 MFT

參考 SANS 於 108 年公布有關檔案時間(Windwos Time Rules)之鑑識研究，關於檔案更名與檔案移動只更新 SI 之 Metadata Time，而 File Name

之 Metadata Time 並不會更新。接著進行檔名變更測試以便觀察是否仍會造成 File Name 之時間異動，完成檔名變更後，發現 SI 之 Metadata Time 會變成修改檔名後之時間，且確實發現所有 File Name 時間均變成其對應之 Standard Information 時間，詳見圖 8。

資料來源：本報告整理

圖8　FN 時間自動對應 SI 時間

由以上實驗驗證可得知，駭客是想要透過修改檔名達到修改 FN Time 目的，從其流程推測得知其步驟，首先駭客透過工具修改檔案 SI 之 4 個時間，包含隱藏欄位 Metadata Time，其次則將檔案進行更名或移動，最後為隱匿其惡意程式植入時間，再度修改檔案 SI 之 Metadata Time，以達成所有 SI 與 FN 時間都是駭客偽造日期之目的。而此案件中之所以會發現惡意程式植入時間有出入，猜測應是駭客疏漏修改檔案 SI 之 Metadata Time，才出現有落差情況致讓鑑識人員發現時間異常問題。而後續追蹤 SANS 於今年公布有關檔案時間(Windwos Time Rules)之鑑識研究，關於檔案更名與檔案移動，已更新 SI 與 File Name 之 Metadata Time 皆是會變動的。

具體偵測此駭客手法方式，可以透過 NTFS 檔案格式中其他相關日誌了解駭客是否使用前述反鑑識手法，例如分析 NTFS 之$Extend\$UsnJrnl 日

誌，可以知道檔案是否有改名/改路徑之紀錄，或是分析 NTFS 之 $Extend\$LogFile 日誌，可以得知檔案 FN Time 修改前後之紀錄，但因相關日誌記錄內容過多，通常僅能保存數小時，之後便會覆蓋舊有紀錄。BlackTech 駭客族群善用進階持續性滲透攻擊(Advanced Persistent Threat, APT)攻擊，由此事件案例中亦可實證，BlackTech 駭客族群已有能力完整修改檔案時間，干擾事件跡證分析。對於駭客之偵測與追蹤，除妥善規劃日誌紀錄之保存以外，並應在各端點部署資安防護機制時時偵測異常行為，以及時發現入侵軌跡。

3. 資安技術研析_Text4shell 弱點研析與驗證實作

本季探討之資安技術研析為 Text4shell 弱點研析與驗證實作，資安業者 XM Cyber 與研究機構 Cyentia Institute 聯合進行曝險管理(Exposure Management)研究，發表研究報告(The State of Exposure Management in 2023)，分析數據指出組織通常有 11,000 個安全漏洞可被攻擊者利用，而某些大型組織甚至會超過此數字之 20 倍。研究結果指出利用這些弱點，攻擊者只需 3 個步驟即可存取地端網路中 70%之關鍵資產，在雲端環境情況更為惡化，有 90%之關鍵資產，只需簡單一個步驟駭客便可展開攻擊。所幸，研究報告亦指出雖然組織存在許多可被利用之弱點，但僅有 2%存在之弱點可讓駭客輕易入侵。因此研究明確指出若能專注於處理這些關鍵性弱點，將得到事半功倍之效。

報告所提及之 2%高風險弱點其中之一為 Text4Shell 弱點，因此以下將針對 Text4Shell 弱點(CVE-2022-42899)進行研析與驗證實作，分析其入侵手法，並提供弱點修補建議。

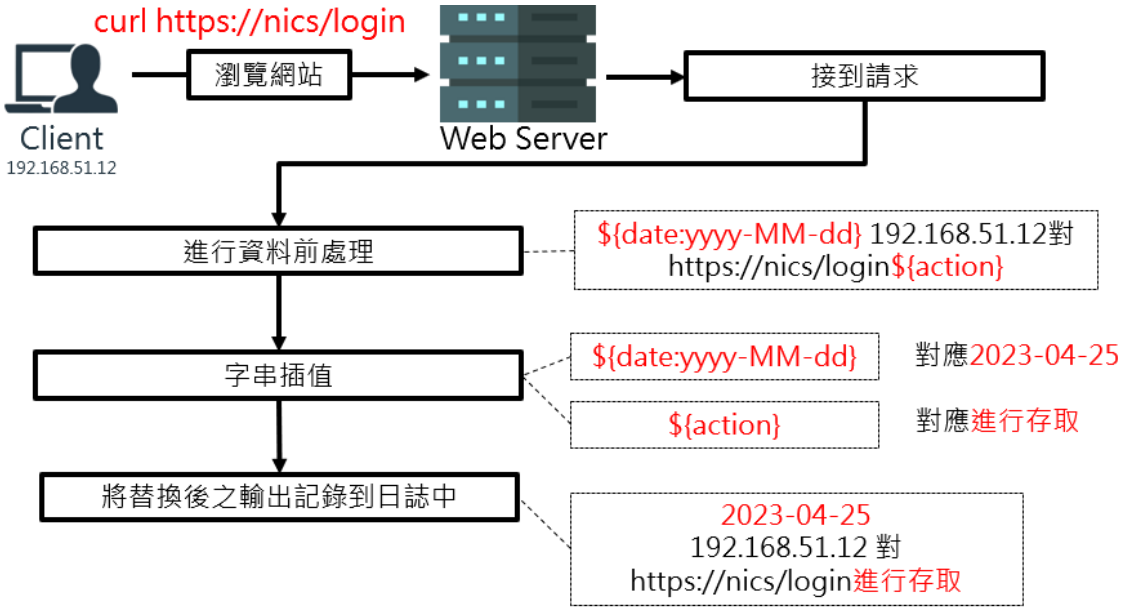
3.1 弱點成因分析

Text4Shell 弱點為 Apache Commons Text Java 函式庫弱點，攻擊者可透過此弱點執行任意程式碼，因 Commons Text 之預設組態存在可使攻擊者不需經身分驗證，輸入特製之惡意內容，進而遠端執行任意程式碼。此弱點 CVE 編號為 CVE-2022-42889，通用漏洞評分系統(Common Vulnerability Scoring System, CVSS)危險程度評分高達 9.8 分，危險程度評級達到最高等級之嚴重(Critical)等級，且此弱點揭露後，資安業者 Wordfence、Zscaler 及 Checkmarx 等皆發現針對此弱點之攻擊行為。

Apache Commons 包含許多開源工具，用以減少重覆程式碼之撰寫，加速程式開發。Commons Text 可應用於 Web 開發，處理各種表單、url、HTML 及 JSON、或應用於數據處理，處理與格式化各種數據、例如：日

期、時間、數值及應用於系統管理，處理各種環境變數、日誌檔案等，亦可應用於安全管理，調整與控管使用者之輸入。其中 Commons Text 一項功能為提供豐富之字串處理函式庫，以處理 Java 函式庫無法處理之字串。其字串替換 StringSubstitutor 類別之 replace 方法可運用進行字串替換，即存在 Text4Shell 弱點。

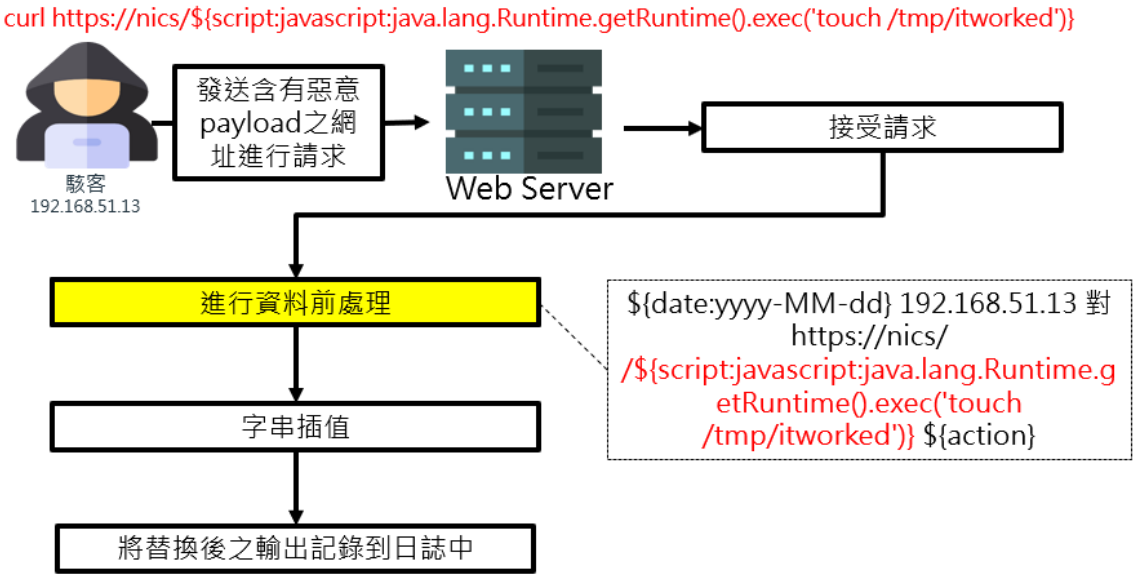
StringSubstitutor 類別主要用於替換字串，提供字串插值(String interpolation)功能，支援占位符號格式，如：${xxx}、${xxx:xxx}等，透過 StringSubstitutor 類別可建立一個替換函式，將占位符號替換為對應之變數值，即可達成替換字串之目的。以使用 script 前綴字串為例，若插入格式 ${script:ScriptEngineName:欲執行之程式碼}，在使用 Commons text 函式庫之網站，如可接受使用者輸入之字串(如日誌記錄功能)，攻擊者將可運用上述方式執行惡意程式碼。舉例說明，一般日誌記錄流程，使用者瀏覽網站，後台接收指令，進行資料整合與轉換，將對應之輸出記錄到日誌檔中，正常流程詳見圖 9。



資料來源：本報告整理

圖9　一般日誌記錄流程

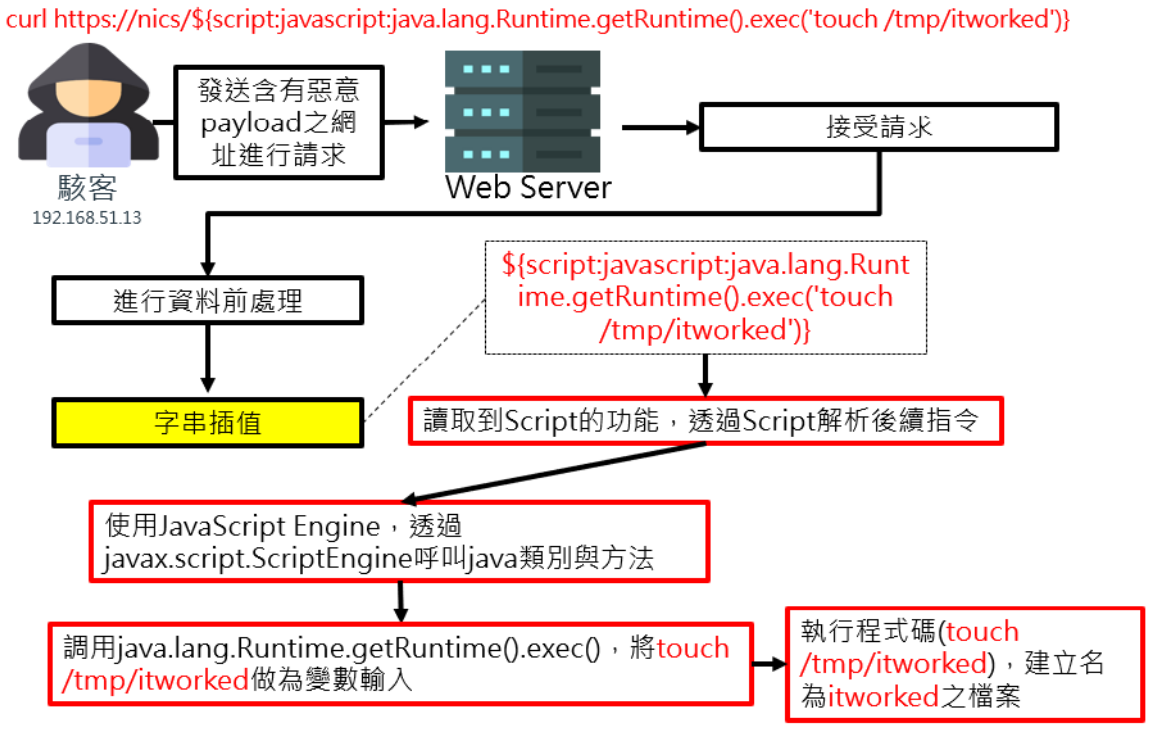
當攻擊者使用 script 前綴(Prefix)時之日誌記錄流程，發送含有惡意內容之網址請求時，原本只會有 2 個要替換之變數，現因網址包含替換語法，經 Web Server 解析後，將會有 3 個位置遭到替換，詳見圖 10。



資料來源：本報告整理

圖10 發送含惡意程式之網址

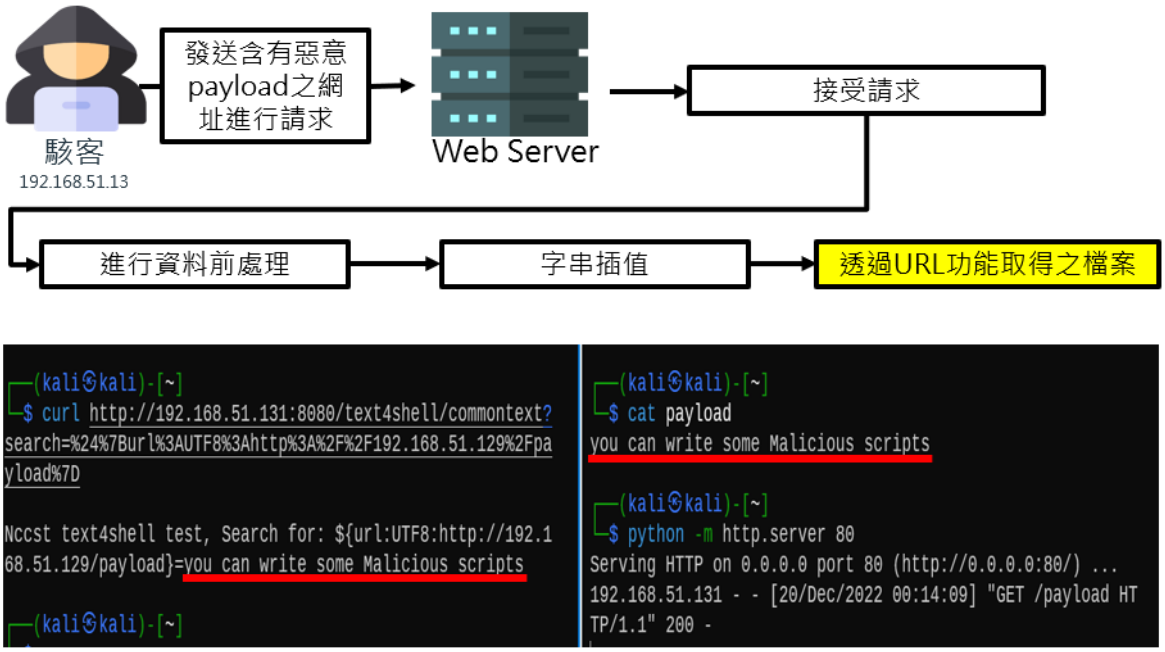
將字串插值讀取到 scrip 前綴，接續解析後續指令，之後將替換後之輸出記錄到日誌中，建立惡意檔案，詳見圖 11。



資料來源：本報告整理

圖11 字串插值建立惡意檔案

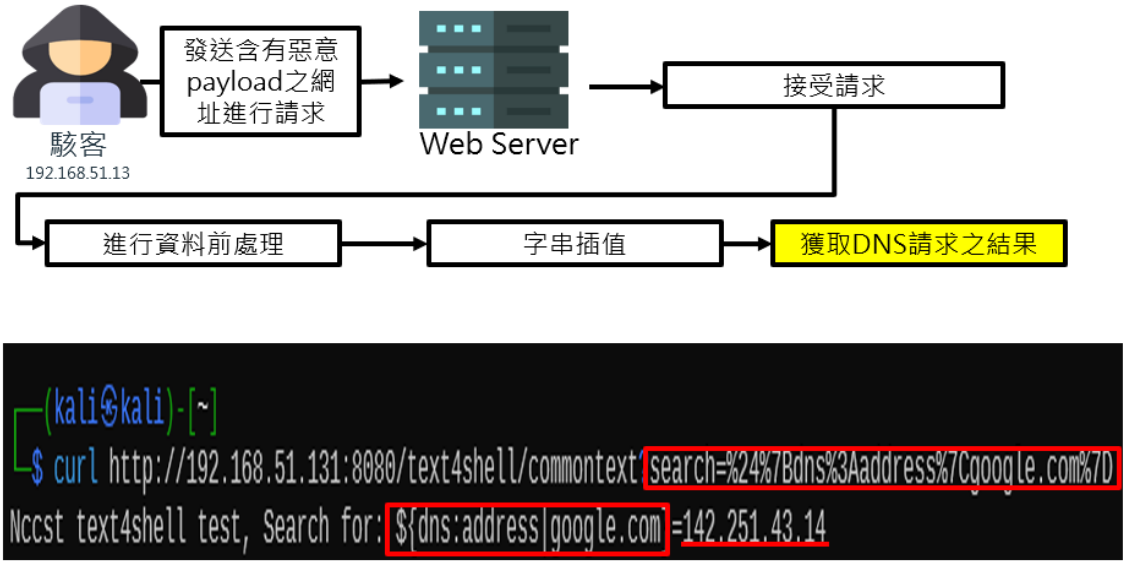
除 script 前綴外，url 前綴也存在可被執行程式碼之問題，此種攻擊手法為透過網址請求訊息，發送惡意 payload，也因未針對 url 前綴進行過濾，因此得以利用此漏洞，存取特定檔案，詳見圖 12。



資料來源：本報告整理

圖12 url 前綴弱點驗證實作步驟

同時經過測試驗證，DNS 前綴亦存在可被執行程式碼之問題，透過解析 DNS 紀錄，可取得內網 IP 資訊，詳見圖 13。

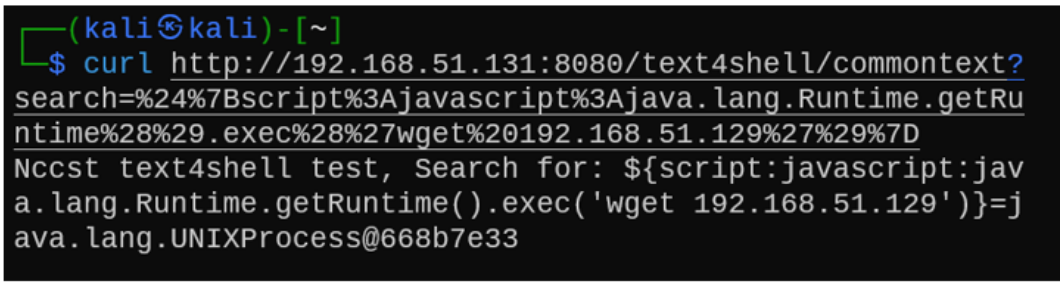


資料來源：本報告整理

圖13 DNS 前綴弱點驗證實作步驟

3.2 弱點攻擊驗證實作與修補方式

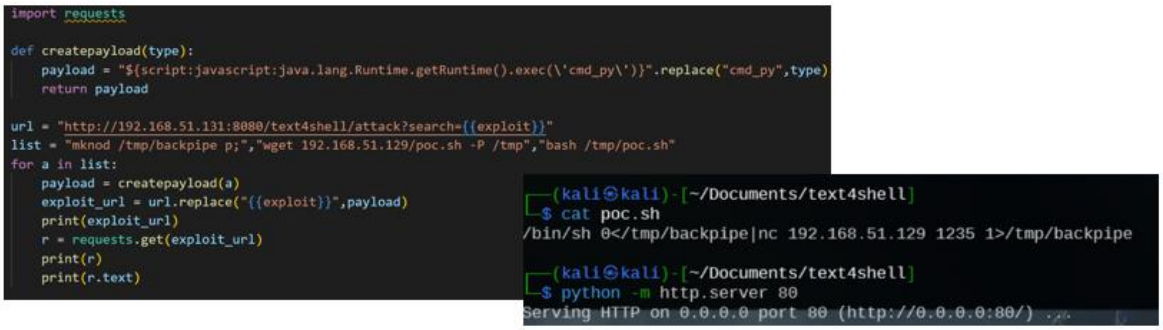
Text4Shell 弱點允許攻擊者運用字串插值，並藉由惡意 payload 呼叫 Java Function，進而執行任意程式碼。整個攻擊流程在滿足安裝套件、前綴可更改及啟用特定前綴等條件後即可進行惡意行為。以下將模擬建立攻擊流程與實作環境，了解攻擊步驟，並建議修補方式。首先設定以 Kali Linux 做為攻擊者主機，IP 設定為 192.168.51.129；另建立 Web Server，使用 Ubuntu linux，IP 設定為 192.168.51.131，網站框架採用 Spring framework。攻擊流程首先試著掃描以確認弱點是否存在，再傳送測試 payload，Text4Shell 弱點允許攻擊者運用字串插值，並藉由惡意 payload 呼叫 Java Function，進而執行任意程式碼。整個攻擊流程在滿足安裝套件、前綴可更改及啟用特定前綴等條件後即可進行惡意行為。以下說明模擬建立攻擊流程與實作環境，了解攻擊步驟，並建議修補方式。首先設定以 Kali Linux 做為攻擊者主機，IP 設定為 192.168.51.129；另建立 Web Server，使用 Ubuntu linux，IP 設定為 192.168.51.131，網站框架採用 Spring framework。攻擊流程首先嘗試確認弱點是否存在，傳送測試 payload，詳見圖 14。



資料來源：本報告整理

圖14 傳送測試 payload

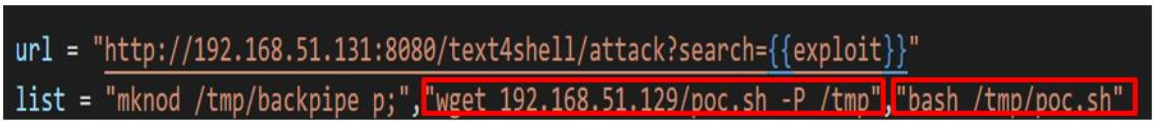
當發現 Web Server 回復請求後，即確認弱點確實存在於此主機。下一步驟則撰寫 Payload 弱點利用程式，詳見圖 15。



資料來源：本報告整理

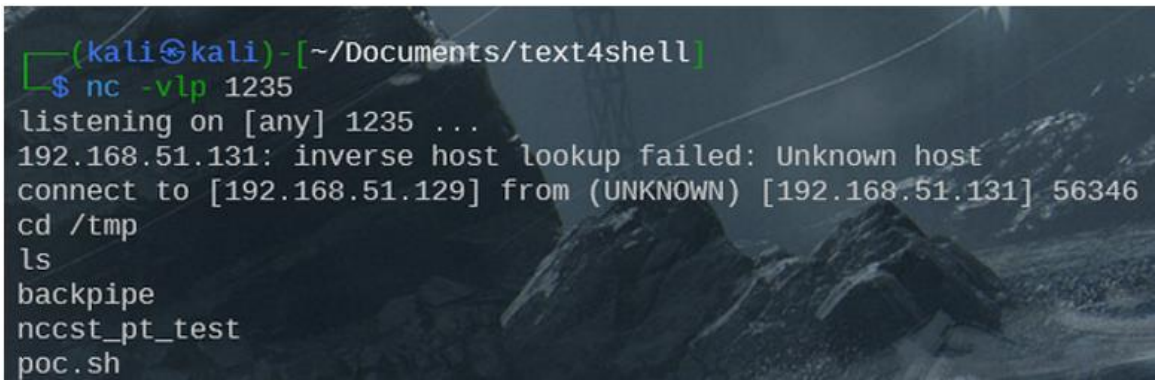
圖15 撰寫 Payload

透過 Text4shell 下載 Shell 腳本程式，再以 Text4shell 執行腳本，成功建立 Reverse Shell，詳見圖 16、圖 17。



資料來源：本報告整理

圖16 以 Text4shell 下載並執行 Shell 腳本



資料來源：本報告整理

圖17 建立 Reverse Shell

驗證實作結果於 Reverse Shell 建立成功後，亦代表攻擊者已掌握受害主機之控制權限。

針對此漏洞修補方式，若無法停止此項功能服務，暫時緩解方式為先過濾使用者輸入欄位，偵測可能具威脅之字串；同時亦應規範禁止使用 script、url 及 dns 前綴，若仍需開放前綴情況下，則僅授權受信任之使用者使用這些前綴。Apache 軟體基金會(Apache Software Foundation)已釋出更新版本 Apache Commons Text 1.10.0 解決這個漏洞，其修補方式為修改 Default String Lookups，透過 addLookup 設定 StringLookup 之預設組態，將 dns、url、script 之功能預設關閉。惟將預設功能關閉之作法並非修復弱點，而是移除該功能，因此仍應考量之風險情境為若程式開發者自行加入且開啟該功能時，攻擊者仍有機會利用這些功能執行程式，因此建議更新至最新版本後，應持續強化過濾輸入字串功能，以加強防範可能風險。

4. 結論

本季具指標性案例為美國大型社群討論平台 Reddit 之機敏資料，因內部人員遭到網路釣魚後個資外洩，致駭客攻擊成功，且提出若不支付贖金，將於暗網販售所竊取之資料。另一起案例為路由器遭新 Condi 惡意程式利用於部署 DDoS 攻擊之殭屍網路，從事件攻擊統計數據顯示，發現有不少使用者尚未進行更新，導致駭客仍廣為利用該弱點。

國內部分，分析政府資安威脅現況，發現政府機關通報事件原因，以「非法入侵」類型為主，排除綜合類型「其他」外，其次分別為「設備問題」與「網頁攻擊」為主要通報類型。針對本季全球與政府所面臨之主要資安威脅，本報告就「網通設備之資安管理」與「程式碼之資安管理」提出資安防護建議。

資安專題分享主題為 BlackTech 駭客族群反鑑識手法研究，從事件分析中發現 BlackTech 駭客族群已有能力完整修改檔案時間，干擾事件跡證分析。因此研究其修改檔案時間之手法，以期能精準判斷駭客入侵時間與進行相關資訊比對，以了解如何追蹤修改軌跡，並部署異常行為偵測機制。

另外，資安技術研析主題為 Text4shell 弱點研析與驗證實作，Text4Shell 弱點於通用漏洞評分系統危險程度評級達到嚴重等級。藉由弱點攻擊驗證實作，了解漏洞形成原因，同時針對於無法停止該項功能服務下，應規劃暫時緩解方案，於更新完成後，持續關注組態設定之正確性。

資安相關活動

本季數位發展部資通安全署辦理之資安相關活動，說明如下。

◆ 112 年第 1 次政府資通安全防護巡迴研討會

第 1 次政府資通安全防護巡迴研討會於 6 月至 7 月期間辦理，分別於臺北、花蓮、臺中及高雄等地共辦理 8 場研討會。政府資通安全防護巡迴研討會主要針對資通安全管理法納管對象之資安專職(責)人員，期許透過研討會方式宣導資安推動策略及重點工作、政府機關資安威脅與防護重點及概略說明 ISO 27001 改版重點。

議題一資安推動策略及重點工作，除說明資安法調修與資安推動略重點外，另外綜整近期政府機關所遭遇之資安事件，並針對事件提出防護建議。如因地緣政治議題，通報事件類型分散式阻斷服務(DDoS)有上升趨勢。針對此類事件，提出事前以預備靜態網頁、流量清洗方案及規劃網站內容傳遞網路服務(Content Delivery Network, CDN)，事中啓動事件通報與回應機制及事後檢視防禦之不足並落實 DDoS 防護演練。

議題二為政府機關資安威脅與防護重點，從說明全球資通安全威脅趨勢，再推展至政府資通安全威脅趨勢，統計國內 Mozi 與 Mirai 變種之殭屍網路持續針對物聯網進行攻擊，目標鎖定路由器、網通設備、DVR 等物聯網裝置。入侵破口為弱密碼與已知漏洞設備，橫向擴大殭屍網路感染範圍。政府機關應關注設備組態之安全性、宣導物聯網設備之相關威脅風險，提高使用者資安意識，避免設備遭殭屍網路感染。

議題三為 ISO 27001 改版簡介，改版重點在現行資訊安全基礎，將網際安全(Cybersecurity)與隱私保護(Privacy Protection)亦納入資訊安全管理系統範圍。除部分控制措施有更新調整外，另外新增 11 項全新之控制措施，包含威脅情資、使用雲端服務之資訊安全、實體安全監控、組態管理、資訊

刪除、資料遮蔽、資料洩露預防、監視活動、網頁過濾及安全程式設計，提醒已導入或規劃導入資訊安全管理系統(ISMS)之政府機關應針對改版重點調整資訊安全管理機制，以符合新版驗證要求。