行政院國家資通安全會報技術服務中心

漏洞/資安訊息警訊

發布編號	NCCST-ANA-2019-0052	發布時間	Wed May 08 10:41:55 CST 2019
事件類型	攻擊活動預警	發現時間	Wed May 01 00:00:00 CST 2019
警訊名稱	近期 GlobeImposter3.0 勒索軟體活動頻繁，請提高警覺		
內容說明	近期 GlobeImposter3.0 加密勒索軟體活動頻繁， GlobeImposter 勒索軟體最早出現於 2017 年，迄今已變種為第三個版本(GlobeImposter3.0)。GlobeImposter 結合使用 RSA 與 AES 加密機制來加密檔案資料，遭加密的檔案資料幾乎無法自行復原，目前尚無資安組織釋出解密工具。GlobeImposter 會勒索受害者 0.3 至 10 個比特幣（一個比特幣大約等於 179,000 元新台幣）以換取解密金鑰。 GlobeImposter 常見傳播方法是透過夾帶附件的社交工程郵件、攻擊可能具有漏洞的 Port(3389、445、139 及 135)或放置惡意廣告於網站頁面。若遭到該勒索軟體加密，副檔名將變為 Ox4444、dragon4444 或 skunk4444 等以 4444 結尾之字串，並會生成 HOW_TO_BACK_FILES 文字檔，內容顯示受駭電腦的識別序號與駭客的聯繫方式等。		
影響等級	中		
建議措施	1. 刪除收到的可疑電子郵件，特別是內含連結或附件的郵件。 2. 針對要求啟動巨集以觀看其內容的微軟 Office 檔案，必須提高警覺，必要時請與寄件者確認其檔案是否含有巨集。 3. 停用瀏覽器 Java Script 與 Flash 功能，並避免在公務主機上瀏覽非公務用相關網頁。 4. 關閉不需使用的 Port(3389、445、139 及 135 等)，並明確切割各業務使用之內部網路與外部網路網段。 5. 定期備份電腦上的檔案及演練資料還原程序，避免使用複寫或本機備份方式。		

	6. 確實持續更新電腦的作業系統、應用程式及防毒軟體等至最新版本。 7. 如不幸受到感染，請立即將受害電腦的網路連線及外接儲存裝置拔除。建議在清除惡意軟體前不要開啟任何檔案。 8. 我們不建議支付贖金，支付贖金只會助長勒索軟體更加猖獗。
參考資料	1. https://www.hkcert.org/my_url/en/blog/18092802 2. https://securelink.net/nb-nb/insights/threat-intelligence-report-globeimposter-ransomware/ 3. https://cloud.tencent.com/info/97dd960818889bbb193a220bade2f710.html 4. https://blog.360totalsecurity.com/en/globeimposter-which-has-more-than-20-variants-is-still-wildly-growing/

此類通告發送對象為通報應變網站登記之資安人員。若貴 單位之資安人員有變更，可逕自登入通報應變網站（https://www.ncert.nat.gov.tw）進行修改。若您仍為貴單位之資安人員但非本事件之處理人員，請協助將此通告告知相關處理人員。

如果您對此通告的內容有疑問或有關於此事件的建議，請勿直接回覆此信件，請以下述聯絡資訊與我們連絡。

地 址： 台北市富陽街 116 號
聯絡電話： 02-27339922
傳真電話： 02-27331655
電子郵件信箱： service@nccst.nat.gov.tw