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-2019-0051	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	Mon May 06 00:00:00 CST 2019
警訊名稱	北韓駭客組織 HIDDEN COBRA 利用惡意程式 HOPLIGHT 透過加密連線進行攻擊活動預警		
內容說明	美國國土安全部與聯邦調查局公布最新北韓駭客組織 HIDDEN COBRA 所利用的惡意程式：HOPLIGHT，透過加密連線進行惡意活動。 若資訊設備遭受感染會有以下風險： 1.個人或單位資料遭竊取。 2.個人工作或單位運作被影響而中斷停擺。 3.資訊設備資源被利用於對外攻擊。 4.單位財務損失。 建議除使用防毒軟體檢查資訊設備是否受惡意程式感染，也可透過已知惡意連線 IP 與惡意檔案存在路徑確認感染與否。		
影響平台	微軟作業系統(Microsoft Windows)		
影響等級	中		
建議措施	1. 檢查是否有資訊設備嘗試連線至下列 HIDDEN COBRA IP 黑名單： 112.175.92.57 113.114.117.122 128.200.115.228 137.139.135.151 181.39.135.126		

	186.169.2.237 197.211.212.59 21.252.107.198 26.165.218.44 47.206.4.145 70.224.36.194 81.94.192.10 81.94.192.147 84.49.242.125 97.90.44.200 2.檢查系統是否存在下列檔案： 2.1 %System32%\rdpproto.dll -MD5: dc268b166fe4c1d1c8595dccf857c476 -SHA-1: 8264556c8a6e460760dc6bb72ecc6f0f966a16b8 2.2 C:\WINDOWS\udbcgiut.dat 或 %AppData%\Local\Temp\udbcgiut.dat -MD5: ae829f55db0198a0a36b227addcdeeff -SHA-1: 04833210fa57ea70a209520f4f2a99d049e537f2 2.3 C:\WINDOWS\MSDFMAPI.INI 或%UserProfile%\AppData\Local\VirtualStore\Windows\MSDFMAPI.INI -MD5: c4103f122d27677c9db144cae1394a66 -SHA-1: 1489f923c4dca729178b3e3233458550d8dddf29 2.4 %System32%\UDPTrcSvc.dll

	-MD5: 0893e206274cb98189d51a284c2a8c83 -SHA-1: d1f4cf4250e7ba186c1d0c6d8876f5a644f457a4 3.若確認資訊設備已遭入侵，建議處理措施： 3.1 視狀況重新安裝作業系統，並更新作業系統及相關安裝軟體。 3.2 修改系統上所有帳號密碼，選用符合複雜性需求之密碼，並定期更換密碼，非必要使用的帳號請將其刪除或停用。 3.3 從防火牆設置阻擋來自外部存取該資訊設備/網站的所有連線，如有特殊情況必須從外部連線存取時，透過防火牆設定白名單的方式開放連線。
參考資料	https://www.us-cert.gov/ncas/analysis-reports/AR19-100A

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