

張貼日期：2020/05/19

【資安攻擊預警】【更新惡意檔案比對資訊】加密勒索軟體猖獗，請加強系統/應用程式更新與資料備份作業

主旨：【資安攻擊預警】【更新惡意檔案比對資訊】加密勒索軟體猖獗，請加強系統/應用程式更新與資料備份作業

• 內容說明：

- 轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202005-0424
轉發 國家資安資訊分享與分析中心 資安訊息警訊 NISAC-ANA-202005-0575
- 近期勒索軟體攻擊事件頻傳，使用者電腦一旦遭植入該惡意程式，將導致該電腦可存取的檔案(含網路磁碟機、共用資料夾等)全數加密無法開啟讀取，藉以勒索使用者支付贖金換取檔案解密。
- 依近期攻擊活動研究報告顯示，駭客透過進階持續性滲透攻擊(Advanced Persistent Threat, APT)方式成功入侵目標組織，並取得網域管理者權限後，以群組原則方式散布勒索軟體，達到大範圍資料加密目的，建議各級機關應提高警覺，定期檢視例行性排程設定與派送機制，如於相關日誌發現異常連線或警示，應深入釐清事件原因，避免錯失調查時機，目前調查已知惡意程式資訊(SHA1)如下：

```

03589DFFE2AB72A0DE5E9DCE61B07E44A983D857
0b4b8404e459a4e892ad06e69ac05ec09d40d3a3
0CB8ED29268EC9848FF1C7F25F28B620271E61C9
0f63da0ce881fd3979864a0731b14231682e8e5b
1acb8e1c912c00aa2de6fafedeff1869cfdbb254
1f2d2b311c0fc6e04b868b8c54f4e2a4312c6ed3
2051f0a253eced030539a10ebc3e6869b727b8a9
2367326f995cb911c72baadc33a3155f8f674600
275473714B3BDDDBDE3FF1BDA892E4BD65C383DEB
29cc0ff619f54068ce0ab34e8ed3919d13fa5ee9
2ab7cdcae22011ee91823854792ab962611c698b
2c68fbd1275de9a9ba0f5fbf742c3fffd4177e05
321901969d7e63d64769236940618aed444f8271
5B9B7FB59F0613C32650E8A3B91067079BCB2FC2
5ce619790d42d49453dbb479074d5a5ae294ee0e
5fc7165336fce9a2113da9ac4d28b56394e63fb1
63697b356cb278535d847e9b27c49bd989e013a2
65bc1801aca0af1a323bacc4b0208bc9321c879b
6aed0e607eab4d4a1e2c038b5790dafa27801b74
71431cbfb8d0090b1ba6877c2774a83f61546035
75e49120a0238749827196cebb7559a37a2422f8
7a1c5e1799bdeebb01527f54a7fd89d0b720dea7
95db7a60f4a9245ffd04c4d9724c2745da55e9fd
9d6feb6e246557f57d17b8df2b6d07194ad66f66
a0402754def2c4055f0ea6f5da2db91de1e271d1
a2046f17ec4f5517636ea331141a4b5423d534f0
AD6783C349E98C2B4A8CE0B5C9207611309ADCA7
b78e56a2e84ae36d5cfadcad09057381f50b97c0

```

bab4b926042aa271c3fdd8d913bc70539152d04b
de9a0386c9736b60e63defd99eb0eba9930561d2
e7aa8f55148b4548ef1ab9744bc3d0e67588d5b7
ec7a59e79be688928d6c2441ec5c8e95532619cf
ef8cd0f9ef1e20b119f1908978d2e74b587c275e
efa69a6be36d0d4ec787515799c15ad236502be0
f0ebd358ceea9a90090c1cd0e6704965e234396f
f7db1c8e17aae7b5b0a1c3d168a2663cbc541219
f8c4cc8505982994e2855a9eacfd7c73bdc11b4f
f908577ed2eb1e913d93eb6261a4ece692ade364

(此為SysinternalsSuite套件中之psping64.exe然請機關確認是否曾自行下載該程式，並注意其存放位置。)

efa69a6be36d0d4ec787515799c15ad236502be0
f0ebd358ceea9a90090c1cd0e6704965e234396f
f7db1c8e17aae7b5b0a1c3d168a2663cbc541219
f8c4cc8505982994e2855a9eacfd7c73bdc11b4f
f908577ed2eb1e913d93eb6261a4ece692ade364

- 此外，傳統勒索軟體傳染途徑以應用程式漏洞(如Flash Player)與社交工程為主，建議請各級政府機關除加強組織資安監控防護外，仍應持續確認相關應用程式更新情況，定期備份重要檔案，加強資訊安全宣導，避免開啟來路不明郵件或連結。
- 影響平台：
全
- 建議措施：
 1. 如發現資通訊系統存在可疑檔案，建議進行SHA1比對，以確認是否為惡意程式。
 2. 定期檢視資通訊系統日誌紀錄，同時檢視資通訊系統排程設定與派送機制，如發現異常連線或新增排程情形，應立即深入了解事件原因。
 3. 不定期檢視資通訊系統帳號使用情況，並定期變更帳號密碼，確保密碼設定符合複雜性原則，避免字符轉換情況發生。
 4. 清查重要資料，並參考下列做法定期進行備份作業：
 - 定期執行重要的資料備份。
 - 備份資料應有適當的實體及環境保護。
 - 應定期測試備份資料，以確保備份資料之可用性。
 - 資料的保存時間與檔案永久保存的需求，應由資料擁有者研提。
 - 重要機密的資料備份，應使用加密方式來保護。
 5. 檢視網路硬碟與共用資料夾之使用者存取權限，避免非必要使用存取。
 6. 確認作業系統、防毒軟體，及應用程式(如Adobe Flash Player、Java)更新情況，並定期檢視系統/應用程式更新紀錄，避免駭客利用系統/應用程式安全性漏洞進行入侵行為。
 7. 若使用隨身碟傳輸資料，應先檢查隨身碟是否感染病毒或惡意程式。
 8. 若疑似遭受感染時，可參考下列做法：
 - 應立即關閉電腦並切斷網路，避免災情擴大。
 - 通知機關資訊人員或廠商協助搶救還沒被加密的檔案。
 - 建議重新安裝作業系統與應用程式，且確認已安裝至最新修補程式後，再還原備份的資料。
 - 備份資料在還原至電腦之前，應以防毒軟體檢查，確保沒有殘存的惡意程式。
 9. 加強教育訓練，請使用者留意相關電子郵件，注意郵件之來源的正確性，不要開啟不明來源信件的附檔或連結，以防被植入後門程式。

網路系統組 敬啟

From:

<http://net.nthu.edu.tw/netsys/> - 網路系統組

Permanent link:

http://net.nthu.edu.tw/netsys/ mailing:announcement:20200519_01

Last update: **2020/05/25 11:33**

