# 勒索病毒 Mailto 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 02 月

# 一、事件簡介

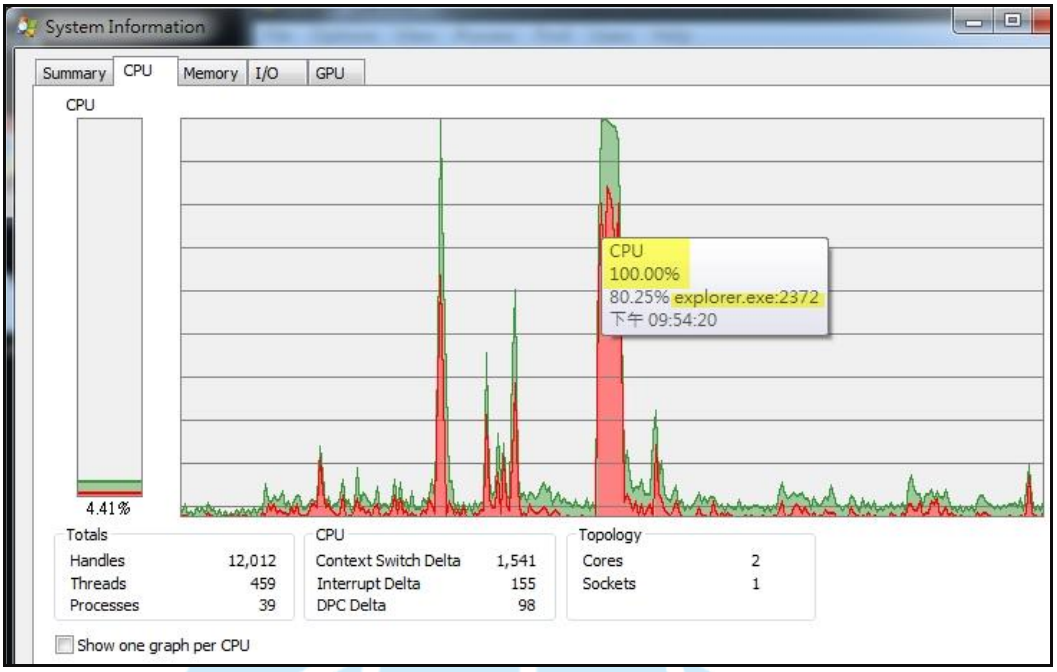
1. 2019 年 9 月左右發現了一個新變種的勒索病毒，該勒索病毒基於附加到加密文件的擴展名被命名為 Mailto (又名 NetWalker)。
2. 瞄準企業網路的 Mailto 病毒在 2020 年 1 月 31 日目標式攻擊澳洲貨運與物流公司 Toll Group 的公司網路，加密連接至公司網路的所有 Windows 設備，高達 1000 台主機被感染，導致該公司關閉許多 IT 系統。
3. 2020 年 2 月初澳洲 Australian Signals Directorate 的 Australian Cyber Security Centre (ACSC)發布此病毒的警報通知。
4. 為了瞭解勒索病毒 Mailto 的攻擊行為與對受害者的危害程度，本中心對病毒樣本 58e923ff.exe 進行檢測。

# 二、事件檢測

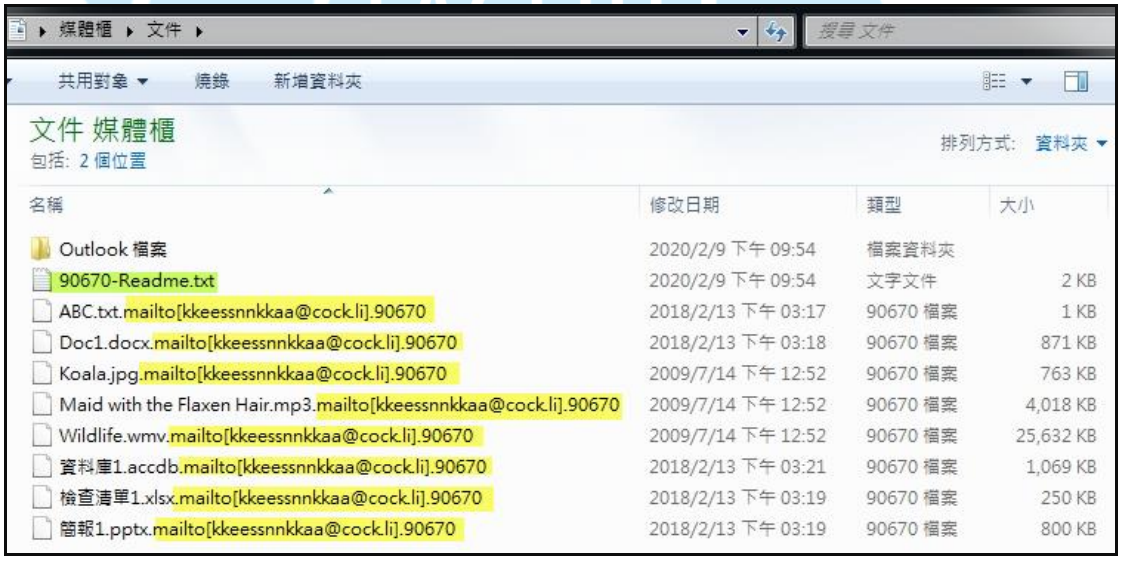
1. 首先，使用一台 32 位元 Windows 7 的虛擬主機，執行病毒樣本 58e923ff.exe (MD5: 73de5babf166f28dc81d6c2faa369379 )。執行後，58e923ff.exe 在原地消失。它會呼叫 explorer.exe 來執行 vssadmin.exe 刪除影子副本，也會開啟勒索通知信 90670-Readme.txt。

| Process | Command |
|---|---|
| 58e923ff.exe (1936) | "C:\Users\Mark\Downloads\58e923ff.exe" |
| explorer.exe (2372) | "C:\Windows\explorer.exe" |
| explorer.exe (3376) | "C:\Windows\explorer.exe" |
| vssadmin.exe (2068) | C:\Windows\system32\vssadmin.exe delete shadows /all /quiet |
| notepad.exe (9028) | C:\Windows\system32\notepad.exe "C:\Users\Mark\Desktop\90670-Readme.txt" |
| vssadmin.exe (6644) | C:\Windows\system32\vssadmin.exe delete shadows /all /quiet |

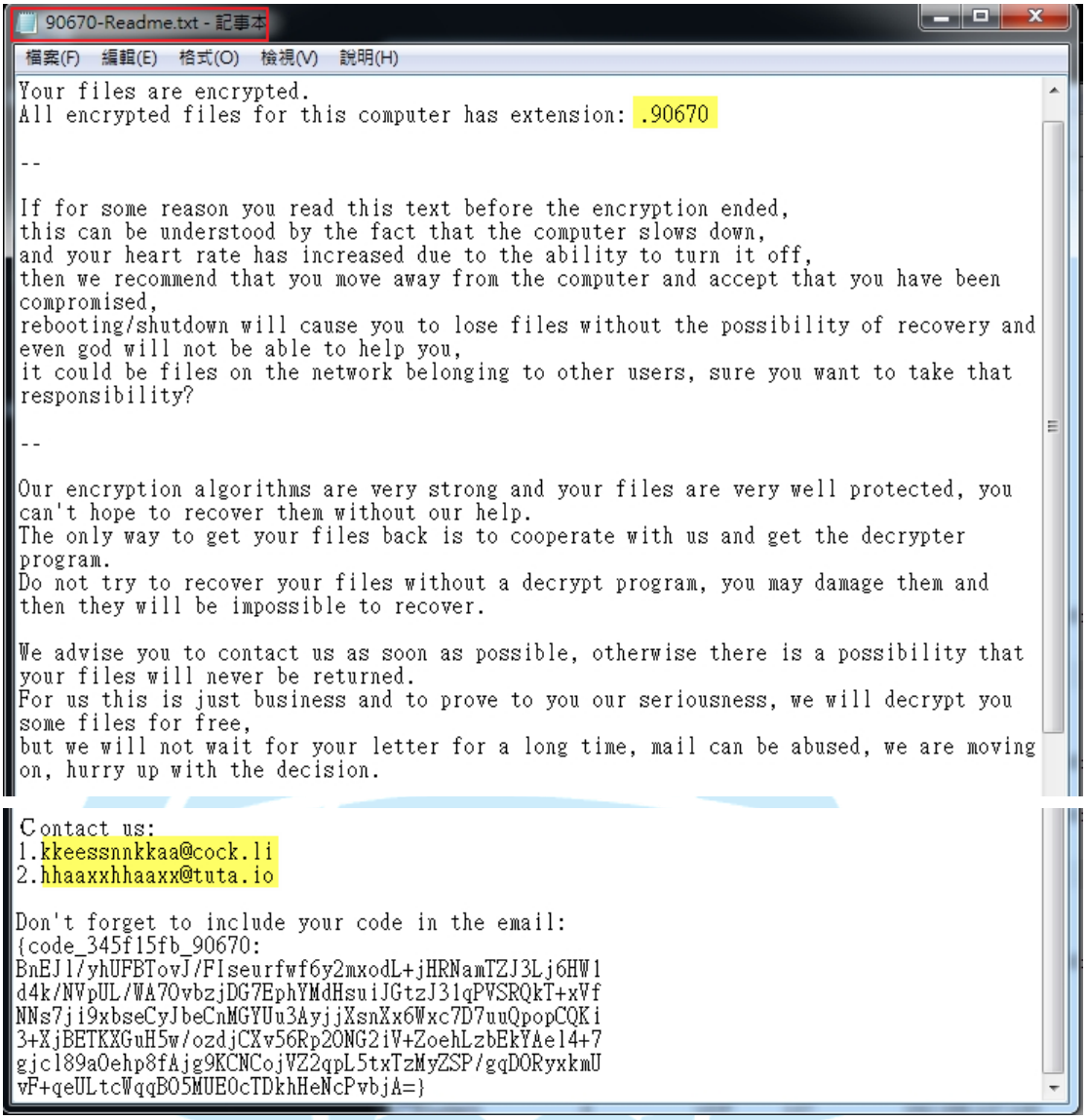
2. 檢視主機的系統效能，發現 explorer.exe(2372)執行時 CPU 衝高將近 80%。




3. 加密檔案時，Mailto 會延伸檔案名稱格式為「.mailto[mail address].檔案加密延伸 id」，例如:.mailto[kkeessnnkkaa@cock.li].90670。除 C:\windows 與 C:\Program Files 兩資料夾內檔案沒有被加密外，其餘檔案皆被加密。

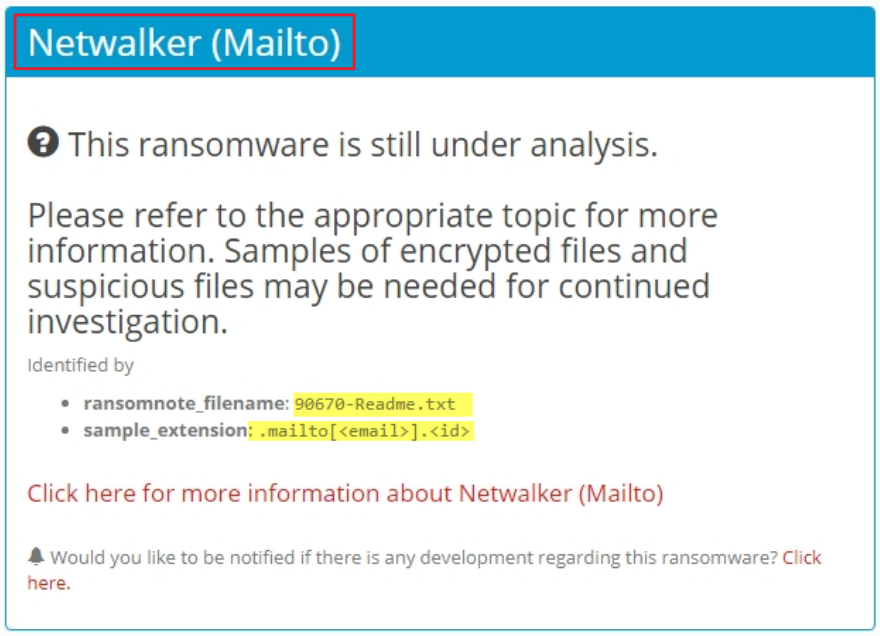



4. 該勒索病毒會產生一個有「受害者 id-Readme.txt」檔案名稱的勒索通知信，內含受害主機被加密的資訊、加密檔案延伸代碼(.90670)與兩個可以獲得付款金額與說明的電子郵件信箱。




5. 當 58e923ff.exe 首次執行，會在登錄檔「電腦\HKEY_CURRENT_USER\Software\90670739」內建立一個登錄機碼(registry key)。


6. 經 ID Ransomware(https://id-ransomware.malwarehunterteam.com)判定 58e923ff.exe 為 Mailto (Netwalker) 勒索病毒。




7. 該病毒經 Virustotal 檢測，其惡意比例為 58/70，而且多家防毒公司以 Mailto 或 Netwalker 命名它。

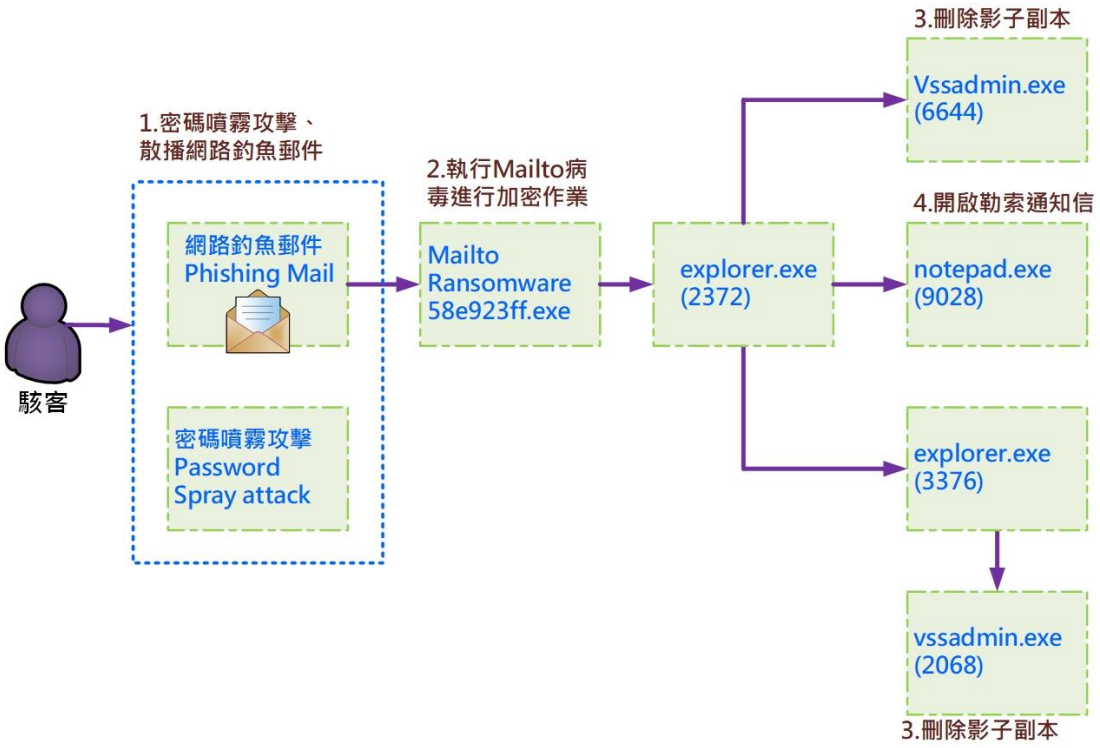

| | | | |
|---|---|---|---|
| Acronis | Suspicious | Ad-Aware | Trojan.Ransom.Netwalker.A |
| AhnLab-V3 | Malware/Win32.Ransom.C3552620 | Alibaba | Trojan:Win32/Nemty.03bbea72 |
| ALYac | Trojan.Ransom.Mailto | SecureAge APEX | Malicious |
| Arcabit | Trojan.Ransom.Netwalker.A | Avast | Win32:RansomX-gen [Ransom] |
| AVG | Win32:RansomX-gen [Ransom] | Avira (no cloud) | TR/Crypt.XPACK.Gen |
| BitDefender | Trojan.Ransom.Netwalker.A | BitDefenderTheta | AI:Packer.F588F44B1D |
| CAT-QuickHeal | Ransom.Mailto.P5 | Comodo | Malware@#r71gacf64c1h |
| CrowdStrike Falcon | Win/malicious_confidence_100% (W) | Cybereason | Malicious.bf166f |
| Cylance | Unsafe | Cyren | W32/Ransom.TDYK-8820 |
| DrWeb | Trojan.Encoder.29998 | Emsisoft | Trojan.Ransom.Netwalker.A (B) |

| | | | |
|---|---|---|---|
| Endgame | Malicious (high Confidence) | eScan | Trojan.Ransom.Netwalker.A |
| ESET-NOD32 | A Variant Of Win32/Filecoder.NXP | F-Prot | W32/Ransom.MG.gen!Eldorado |
| F-Secure | Trojan.TR/Crypt.XPACK.Gen | FireEye | Generic.mg.73de5babf166f28d |
| Fortinet | W32/Filecoder.NXP!tr.ransom | GData | Trojan.Ransom.Netwalker.A |

| | | | |
|---|---|---|---|
| Ikarus | Trojan-Ransom.FileCrypter | Jiangmin | Trojan.DelShad.rv |
| K7AntiVirus | Trojan ( 005573071 ) | K7GW | Trojan ( 005573071 ) |
| Kaspersky | HEUR:Trojan.Win32.DelShad.vho | MAX | Malware (ai Score=100) |
| MaxSecure | Trojan.Malware.74666482.susgen | McAfee | Ransom-CWall!73DE5BABF166 |
| McAfee-GW-Edition | BehavesLike.Win32.Downloader.nh | Microsoft | Trojan:Win32/Nemty.PDIMTB |

| | | | |
|---|---|---|---|
| NANO-Antivirus | Virus.Win32.Gen.ccmw | Palo Alto Networks | Generic.ml |
| Panda | Trj/CI.A | Qihoo-360 | Win32/Trojan.681 |
| Rising | Ransom.Mailto!1.BC36 (CLASSIC) | SentinelOne (Static ML) | DFI - Suspicious PE |
| Sophos AV | Troj/Ransom-FVD | Sophos ML | Heuristic |
| Symantec | Downloader | Tencent | Win32.Trojan.Filecoder.Aisk |
| Trapmine | Malicious.high.ml.score | TrendMicro | Ransom.Win32.MAILTO.AB |
| TrendMicro-HouseCall | Ransom.Win32.MAILTO.AB | VBA32 | BScope.TrojanPSW.Spy |
| VIPRE | Trojan.Win32.Generic!BT | ViRobot | Trojan.Win32.Z.Filecoder.96256.B |
| Webroot | W32.Trojan.Gen | Yandex | Trojan.DelShad! |

## 三、事件攻擊行為示意圖




1. 駭客使用密碼噴霧攻擊與散播網路釣魚郵件方式散播 Mailto 病毒。
2. 使用者開啟網路釣魚郵件感染 Mailto 病毒，進行檔案加密作業。

3. Mailto 病毒呼叫 explorer.exe 來執行 vssadmin.exe，以刪除影子副本。
4. 加密後，呼叫 notepad.exe 來開啟勒索通知信。

## 四、總結與建議

1. Mailto 勒索病毒的主要攻擊目標以企業網路為主。
2. 它喜歡針對在任何停機時間就無法正常運作的行業進行攻擊，因為會提高受害者支付贖金的機率。
3. 醫療保健組織、政府單位、工業控制系統以及運輸公司都是該勒索病毒的攻擊目標。
4. Mailto 病毒會在執行後在原地消失、加密檔案與刪除影子副本。
5. 關於 Mailto 病毒攻擊事件的預防措施，有下列幾點建議。
   (1) 更新防毒軟體與病毒碼，並且定期掃毒。
   (2) 修補程式或作業系統的漏洞。
   (3) 定期備份資料。
   (4) 掃描電子郵件內容。
   (5) 網路切割:
   將網路劃分為較小的部分，以分離和隔離特定主機和服務之間的通信。適當的分段和隔離將限制勒索病毒感染在網路上的散播程度。

## 五、相關報導

1. Advisory 2020-003: Mailto ransomware incidents
https://www.cyber.gov.au/threats/advisory-2020-003-mailto-ransomware-incidents
2. Toll Group hit by "new variant" of Mailto ransomware
https://www.itnews.com.au/news/toll-group-hit-by-new-variant-of-mailto-ransomware-537537