勒索病毒 WastedLocker
分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 08 月

一、事件簡介

1. 2020/5 初 WastedLocker 首次被揭露，該勒索軟體來自於惡名昭彰的俄羅斯駭客集團「Evil Group」。
2. 2020/6 賽門鐵克發現攻擊者試圖在其網路上部署 WastedLocker，並且對美國公司進行攻擊。 其最終目標是透過加密受害者的大部分電腦和伺服器來削弱受害者的 IT 基礎架構，以要求獲得數百萬美元的贖金。
3. 賽門鐵克發現了針對 31 個組織的攻擊，所有組織都位於美國。除了一些大型私人公司外，還有 11 家上市公司，其中有 8 家是《財富》 500 強公司。
4. WastedLocker 最近最受矚目的受害者之一是可穿戴技術和智能手錶製造商 Garmin。
5. 由賽門鐵克的統計資料得知「製造業」是受影響最嚴重的公司組織，緊隨其後的是「信息技術」和「媒體與電信」類的公司組織。

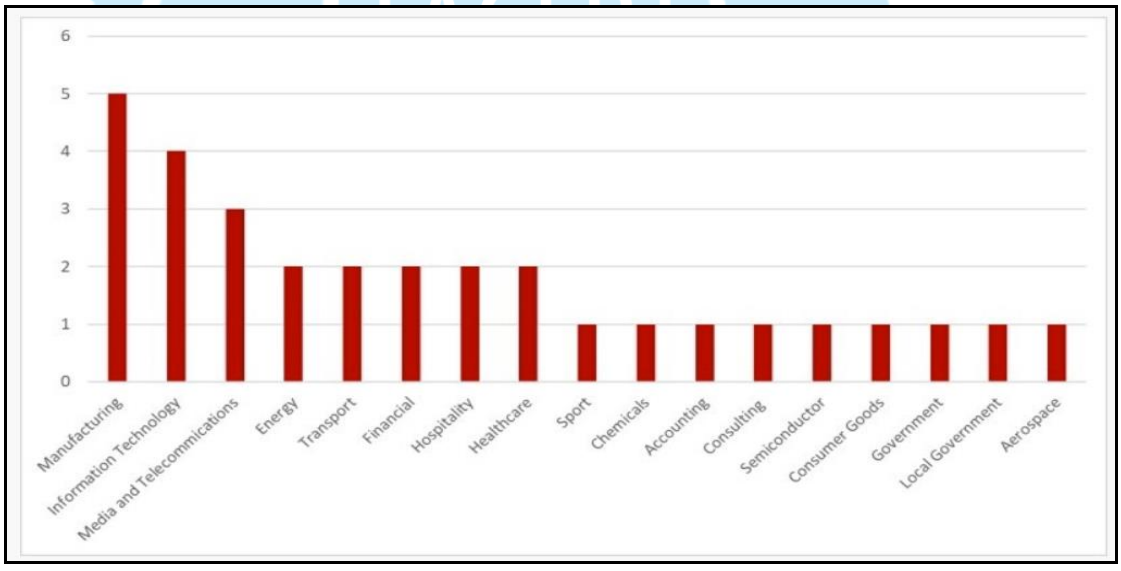


圖 1: WastedLocker 所目標式攻擊的各行業組織數量(資料來源:賽門鐵克)

6. 為了瞭解勒索 WastedLocker 的攻擊行為與對主機的危害程度，本中心取得樣本後進行分析。

二、事件檢測

1. 首先，將惡意程式樣本 905ea119.exe 於 Windows 10 (32 位元)的作業系統上執行，執行後該樣本程式會於原資料夾內消失。

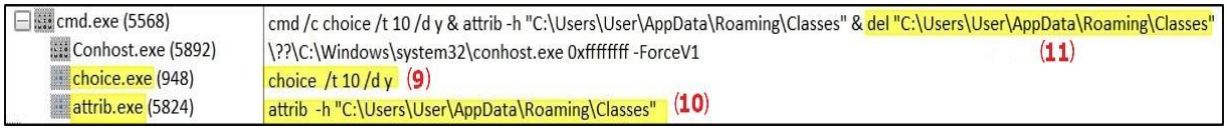
2. 檢視主機的背景程式運作情形，發現 905ea119.exe 執行後呼叫一些系統程式來執行一些指令。

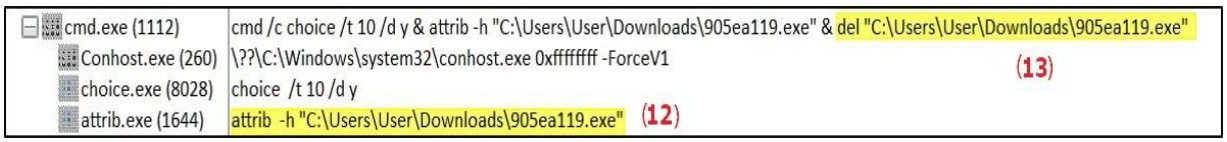
Process	Image Path	Command
905ea119.exe (4368)	C:\Users\User\Downloads\905ea119.exe	"C:\Users\User\Downloads\905ea119.exe"
winsat.exe (6028)	C:\Windows \system32\winsat.exe	"C:\Windows \system32\winsat.exe"
winsat.exe (5620)	C:\Windows \system32\winsat.exe	"C:\Windows \system32\winsat.exe"
Conhost.exe (4596)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Classes:bin (5076)	C:\Users\User\AppData\Roaming\Classes:bin	C:\Users\User\AppData\Roaming\Classes:bin
F79}:bin (5828)	C:\Users\User\AppData\Roaming\F79}:bin	C:\Users\User\AppData\Roaming\F79}:bin -r
vssadmin.exe (4784)	C:\Windows\system32\vssadmin.exe	C:\Windows\system32\vssadmin.exe Delete Shadows /All /Quiet
Conhost.exe (4140)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
takeown.exe (6736)	C:\Windows\system32\takeown.exe	C:\Windows\system32\takeown.exe /F C:\Windows\system32\Classes.exe
Conhost.exe (6724)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
icacls.exe (6684)	C:\Windows\system32\icacls.exe	C:\Windows\system32\icacls.exe C:\Windows\system32\Classes.exe /reset
Conhost.exe (5400)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (5964)	C:\Windows\system32\cmd.exe	cmd /c choice /t 10 /d y & attrib -h "C:\Users\User\AppData\Roaming\F79}" & del "C:\Users\User\AppData\Roaming\F79}"
Conhost.exe (2580)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
choice.exe (3364)	C:\Windows\system32\choice.exe	choice /t 10 /d y
attrib.exe (148)	C:\Windows\system32\attrib.exe	attrib -h "C:\Users\User\AppData\Roaming\F79}"
cmd.exe (5568)	C:\Windows\system32\cmd.exe	cmd /c choice /t 10 /d y & attrib -h "C:\Users\User\AppData\Roaming\Classes" & del "C:\Users\User\AppData\Roaming\Classes"
Conhost.exe (5892)	C:\Windows\System32\Conhost.exe	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
choice.exe (948)	C:\Windows\system32\choice.exe	choice /t 10 /d y
attrib.exe (5824)	C:\Windows\system32\attrib.exe	attrib -h "C:\Users\User\AppData\Roaming\Classes"

3. 905ea119.exe 執行後會在%system32%內產生 Classes.exe，之後如下列程序:

Process	Command
905ea119.exe (4368)	"C:\Users\User\Downloads\905ea119.exe"
winsat.exe (6028)	"C:\Windows \system32\winsat.exe"
winsat.exe (5620)	"C:\Windows \system32\winsat.exe"
Conhost.exe (4596)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Classes:bin (5076)	C:\Users\User\AppData\Roaming\Classes:bin (1)
F79}:bin (5828)	C:\Users\User\AppData\Roaming\F79}:bin -r (2)
vssadmin.exe (4784)	C:\Windows\system32\vssadmin.exe Delete Shadows /All /Quiet (3)
Conhost.exe (4140)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
takeown.exe (6736)	C:\Windows\system32\takeown.exe /F C:\Windows\system32\Classes.exe (4)
Conhost.exe (6724)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
icacls.exe (6684)	C:\Windows\system32\icacls.exe C:\Windows\system32\Classes.exe /reset (5)
Conhost.exe (5400)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
cmd.exe (5964)	cmd /c choice /t 10 /d y & attrib -h "C:\Users\User\AppData\Roaming\F79}" & del "C:\Users\User\AppData\Roaming\F79}"
Conhost.exe (2580)	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 (8)
choice.exe (3364)	choice /t 10 /d y (6)
attrib.exe (148)	attrib -h "C:\Users\User\AppData\Roaming\F79}" (7)

(1) 在%AppData%建立 Classes:bin。
(2) 在%AppData%建立 F79}:bin。
(3) 刪除影子副本。
(4) 重新指派 Classes.exe 的擁有權。
(5) 重置 Classes.exe 的存取控制權限。
(6) 若 10 秒內沒選擇，則自動執行預設值。
(7) 更改 F79 的屬性由隱藏改為顯示。
(8) 刪除 F79。





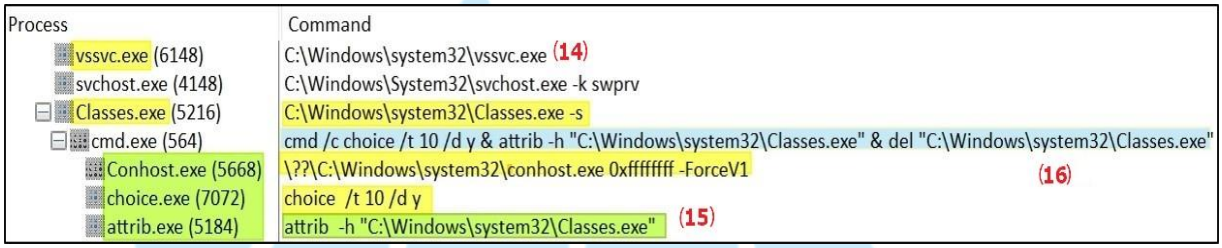
(9) 若在 10 秒沒有選擇則自動執行預設值。

(10) 變更 Classes 的屬性由隱藏改為顯示。

(11) 刪除 Classes。

(12) 變更 905ea119.exe 的屬性由隱藏改為顯示。

(13) 刪除 905ea119.exe。



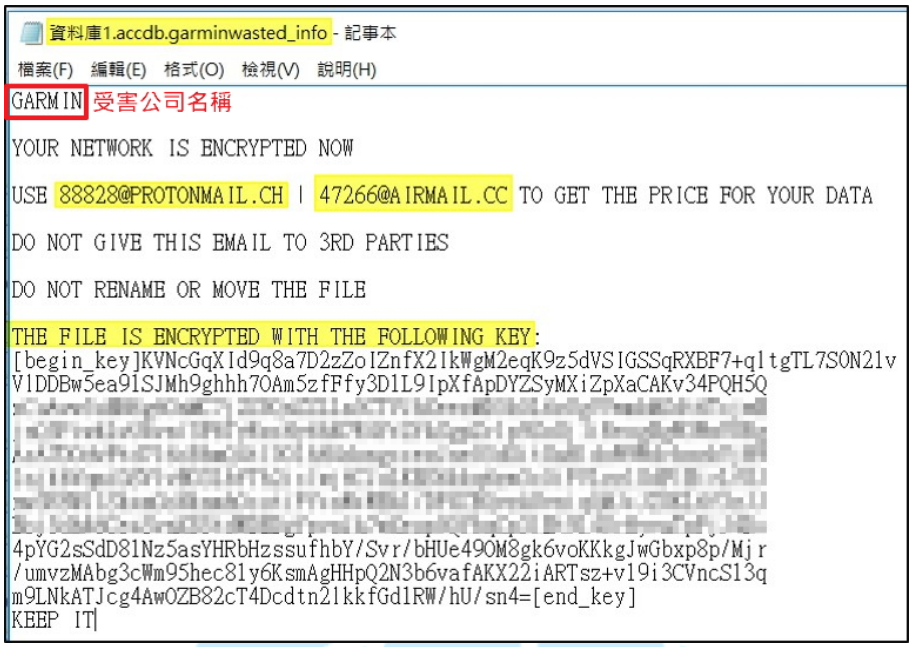
(14) 複製影子副本。

(15) 變更 Classes.exe 的屬性由隱藏改為顯示。

(16) 刪除 Classes.exe。

4. 主機內被加密的檔案皆會延伸副檔名為 garminwasted，並且產生一個以原被加密檔案檔名延伸出副檔名為 garminwasted_info 之檔案。Garmin 為受害企業之一，故該病毒會以受駭的目標企業名稱縮寫並加上字串「wasted」作為加密檔案的副檔名。除了 C:\Windows 與 C:\Program Files 資料夾沒被加密外，其餘資料夾的檔案都被加密，但該惡意程式不會對.txt 文字檔加密。

5. 檢視被加密後產生副檔名.garminwasted_info 的檔案，發現為勒索通知信。該檔案告訴受害者兩個取得贖金資訊的聯絡信箱與檔案被加密的 Key 資訊。每個被加密的檔案都會產生一個勒索通知信。



6. 將副檔名.garminwasted_info 的檔案與一個被加密的檔案上傳 ID Ransomware 勒索病毒識別網站，經檢測判定為 WastedLocker。該勒索病毒目前尚未有解密器，建議備份被加密的檔案，以待未來解密器的產生。

7. 905ea119.exe 經 Virustotal 檢測其惡意比例為 61/72。

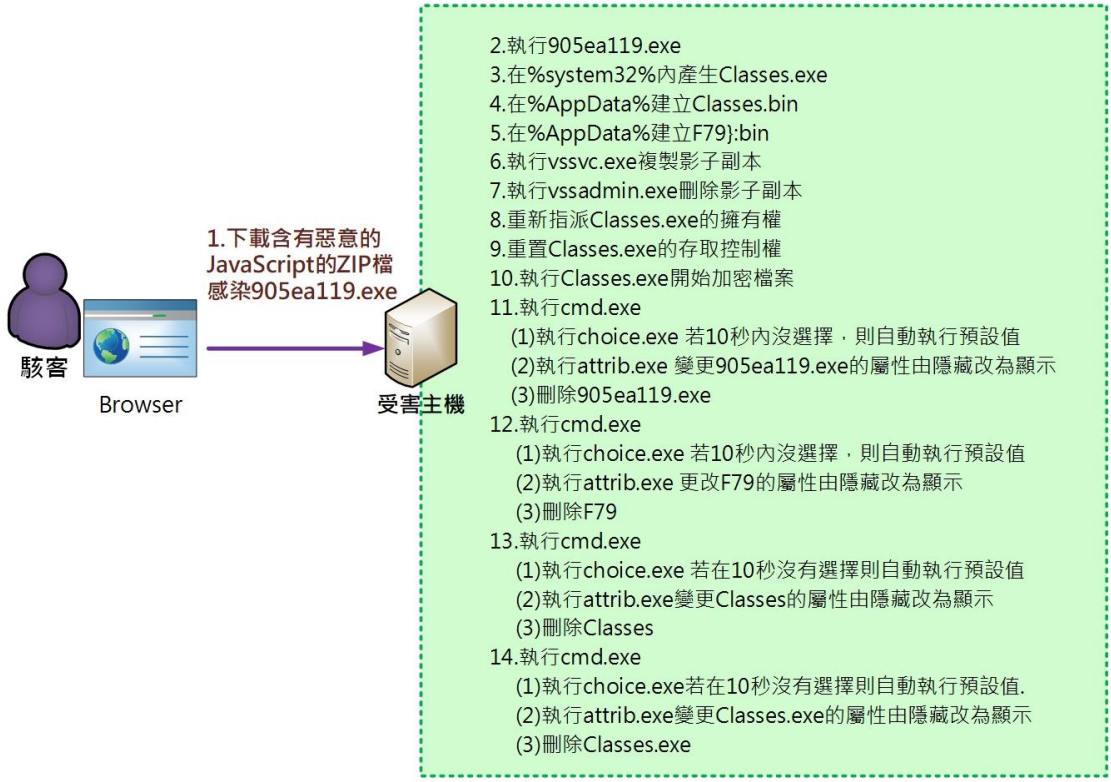
Acronis	Suspicious	Ad-Aware	Trojan.GenericKD.43531595
AegisLab	Hacktool.Win32.Krap.lKMc	AhnLab-V3	Trojan/Win32.WastedLocker.R345840
Alibaba	Ransom:Win32/WastedLocker.8d6cfcd2	ALYac	Trojan.Ransom.WastedLocker
Antiy-AVL	Trojan/Win32.Wacatac	SecureAge APEX	Malicious
Arcabit	Trojan.Generic.D2983D4B	Avast	Win32:DangerousSig [Trj]
AVG	Win32:DangerousSig [Trj]	Avira (no cloud)	TR/AD.Ursnif.gnhpn
BitDefender	Trojan.GenericKD.43531595	BitDefenderTheta	Gen:NN.ZexaF.34152.mrX@aq370@ni
Bkav	W32.AIDetectVM.malware2	CAT-QuickHeal	Trojan.Delshad
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.15c0b7
Cylance	Unsafe	Cynet	Malicious (score: 100)

Cyren	W32/Trojan.YJTP-3191	DrWeb	Trojan.Encoder.32185
Emsisoft	Trojan.GenericKD.43531595 (B)	Endgame	Malicious (high Confidence)
eScan	Trojan.GenericKD.43531595	ESET-NOD32	Win32/Filecoder.WastedLocker.A
F-Prot	W32/WastedLocker.A	F-Secure	Trojan.TR/AD.Ursnif.gnhpn
FireEye	Generic.mg.2cc4534b0dd0e1c8	Fortinet	W32/WastedLocker.Altr.ransom
GData	Trojan.GenericKD.43531595	Ikarus	Trojan.Win32.Krypt
Jiangmin	Trojan.DelShad.acj	K7AntiVirus	Trojan (0056b4141)
K7GW	Trojan (0056b4141)	Kaspersky	Trojan-Ransom.Win32.Wasted.d
Malwarebytes	Ransom.WastedLocker	MAX	Malware (ai Score=100)
MaxSecure	Trojan.Malware.104312461.susgen	McAfee	Packed-GCII2CC4534B0DD0

Microsoft	Ransom:Win32/WastedLocker.SKIMTB	NANO-Antivirus	Trojan.Win32.DelShad.hotbyz
Palo Alto Networks	Generic.ml	Panda	Trj/GdSda.A
Qihoo-360	Generic/HEUR/QVM20.1.C2DF.Malw...	Rising	Ransom.GarminI8.11E81 (CLOUD)
Sangfor Engine Zero	Malware	SentinelOne (Static ML)	DFI - Malicious PE
Sophos AV	Mal/EncPk-APV	Sophos ML	Heuristic
Symantec	Downloader	Tencent	Malware.Win32.Gencirc.11a8c1e3
Trapmine	Suspicious.low.ml.score	TrendMicro	Ransom.Win32.WASTEDLOCKER.T...
TrendMicro-HouseCall	Ransom.Win32.WASTEDLOCKER.T...	VBA32	Trojan.DelShad
VIPRE	Trojan.Win32.GenericIBT	ViRobot	Trojan.Win32.Z.Agent.1252752
Webroot	W32.Ransom.Wastedlocker	Zillya	Trojan.DelShad.Win32.586

8. classes.exe 經 Virustotal 檢測其惡意比例為 61/72，而且其 HASH 值與 905ea119.exe 相同，可見為相同的程式。

三、攻擊行為示意圖



1. 受害者下載含有惡意的 JavaScript 的 ZIP 壓縮檔感染到惡意程式 905ea119.exe。
2. 之後執行惡意程式 905ea119.exe。
3. 惡意程式 905ea119.exe 執行後會在%system32%內產生 Classes.exe。
4. 在%AppData%建立 Classes.bin。
5. 在%AppData%建立 F79}:bin。
6. 執行 vssvc.exe 來複製影子副本。
7. 執行 vssadim.exe 來刪除影子副本。
8. 重新指派 Classes.exe 的擁有權。

9. 重置 Classes.exe 的存取控制權。
10. 執行 Classes.exe 來開始加密檔案。
11. 執行 cmd.exe。
    (1) 執行 choice.exe 若 10 秒內沒選擇則自動執行預設值。
    (2) 執行 attrib.exe 變更 905ea119.exe 的屬性由隱藏改為顯示。
    (3) 刪除 905ea119.exe。
12. 執行 cmd.exe。
    (1)執行 choice.exe 若 10 秒內沒選擇則自動執行預設值。
    (2)執行 attrib.exe 更改 F79 的屬性由隱藏改為顯示。
    (3)刪除 F79。
13. 執行 cmd.exe。
    (1) 執行 choice.exe 若 10 秒內沒選擇則自動執行預設值。
    (2) 執行 attrib.exe 變更 Classes 的屬性由隱藏改為顯示。
    (3) 刪除 Classes。
14. 執行 cmd.exe。
    (1) 執行 choice.exe 若 10 秒內沒選擇則自動執行預設值。
    (2) 執行 attrib.exe 變更 Classes.exe 的屬性由隱藏改為顯示。
    (3) 刪除 Classes.exe。

四、總結與建議

1. 勒索軟體 WastedLocker 以目標式組織為攻擊對象，執行後會在原處自我消失。
2. 它所產生的勒索通知信內容一開始會有被攻擊的目標組織名稱。
3. 該病毒會以被攻擊的目標組織名稱當被加密檔案的副檔名開頭文字，之後加入 wasted 的用字作為副檔名。

4. 該病毒會產生一個分身 classes.exe 於%system32%內來執行檔案加密作業。
5. 目前該病毒尚未有解密器，可將被加密的檔案先保存起來，若未來有解密器產生則可能有機會恢復檔案內容。
6. 由於該病毒透過瀏覽器下載含有惡意 JavaScript 的 ZIP 壓縮檔來散播，之後該病毒會被下載執行，建議不要隨意下載或開啟不明來源的檔案。