

啟動安全模式的勒索病毒 Snatch 分析報告

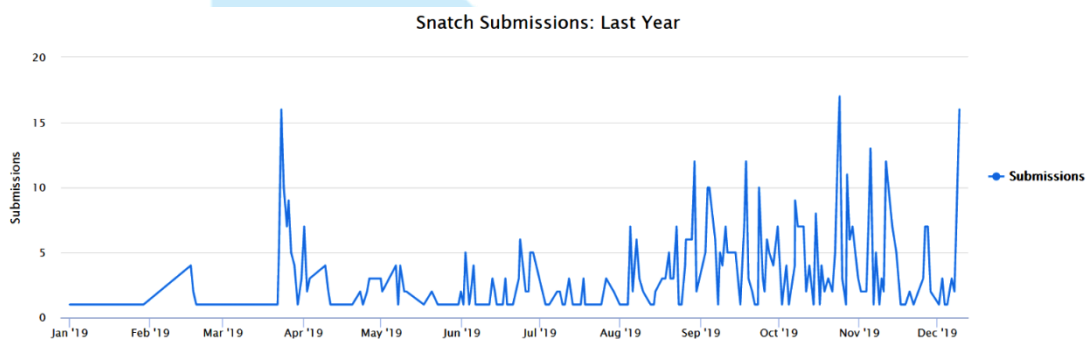


臺灣學術網路危機處理中心團隊(TACERT)製

2020 年 01 月

一、事件簡介

1. 勒索病毒 Snatch 最早於 2018 年底被發現，但於 2019 年 4 月開始活躍，它攻擊了美國、加拿大和幾個歐洲國家。由 2019 年提交到 Michael Gillespie 的 ID Ransomware 平台的勒索通知信和加密文件樣本的激增情形，可以得知此病毒的擴散速度如下圖所示，在 2019 年 4 月活躍後，在 2019 年 9~12 月期間該病毒有明顯地擴大攻擊的情形。



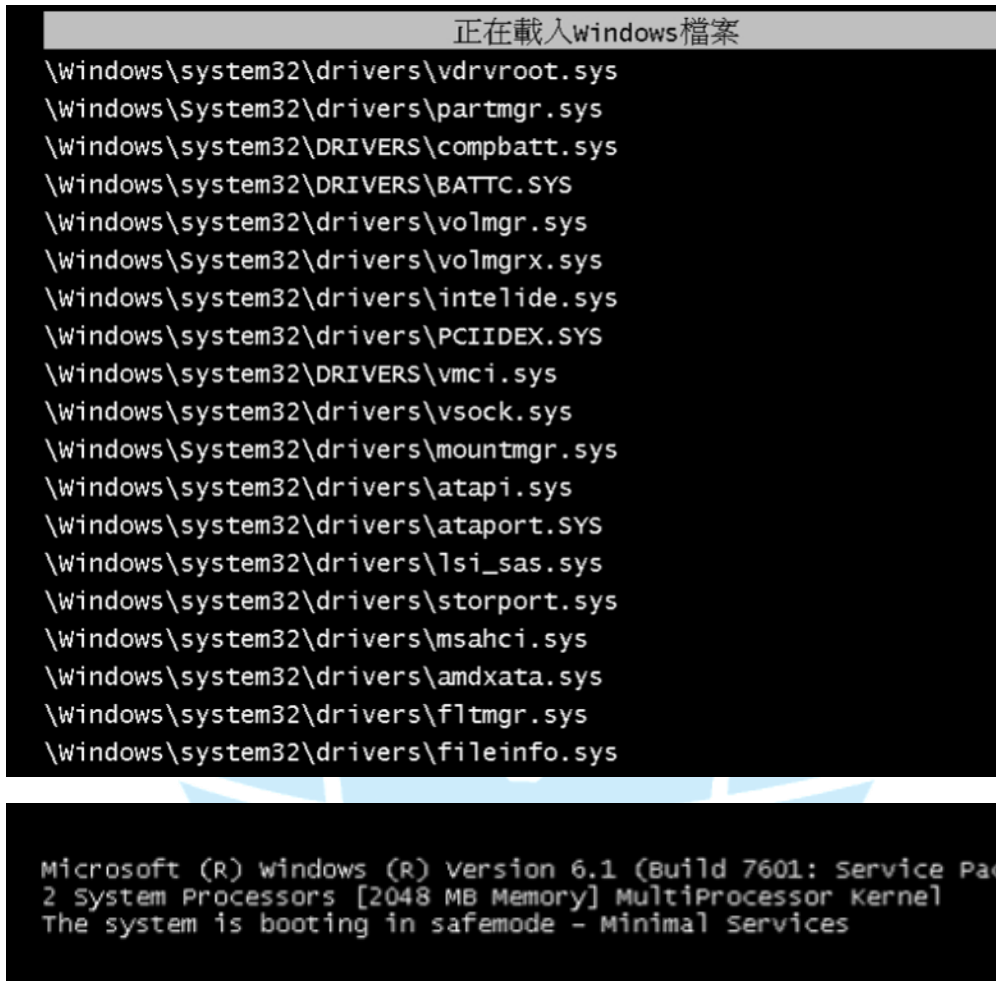
Snatch ransomware 2019 activity (ID Ransomware)

(資料來源:BLEEPINGCOMPUTER)

2. 它不以一般使用者為目標，也沒有利用垃圾郵件或瀏覽器漏洞大規模散播自己。該病毒鎖定特定目標進行攻擊，如攻擊公司或政府組織。
3. 它會利用微軟遠端桌面連線功能(RDP)、VNC 遠端連線軟體、Teamviewer、Webshell 和 SQL Injection 等工具的漏洞或公開的服務入侵到企業內部網路。之後會收集該企業的相關資訊和敏感資料，監視一段時間後才發動攻擊。
4. 該病毒在 2019 年 12 月初出現其變種，而安全模式的設計即是該變種的新功能。
5. 為了瞭解勒索病毒 Snatch 的攻擊行為與對受害者的危害程度，本中心對病毒樣本 KB4463527.exe 進行檢測。

二、事件檢測

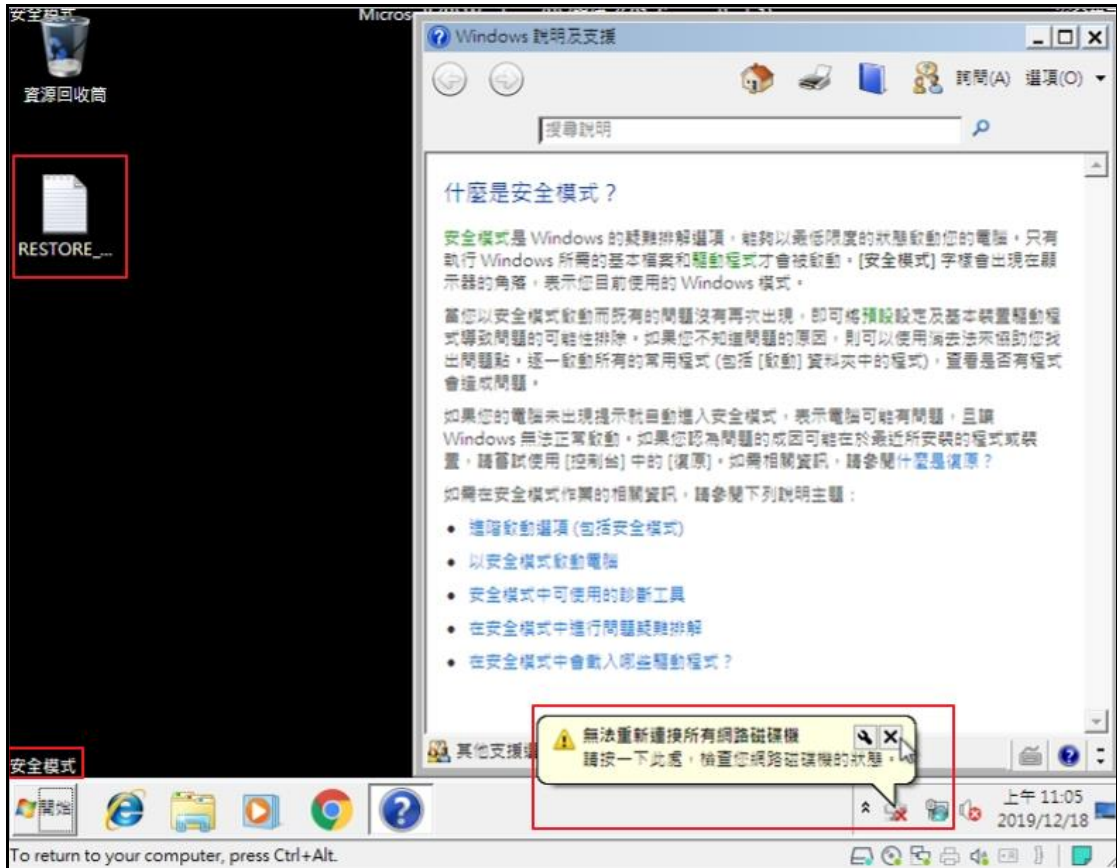
1. 首先，使用一台具有網路磁碟機與 32 位元 Windows 7 作業系統的虛擬主機，在提升權限模式下將惡意程式 KB4463527.exe (MD5:9E76E62FFF6C6C2D2DF58E4891AB6521)於該主機上執行，執行後主機機會重新開機，並且看到正在載入 Windows 檔案的畫面與啟動安全模式的訊息。



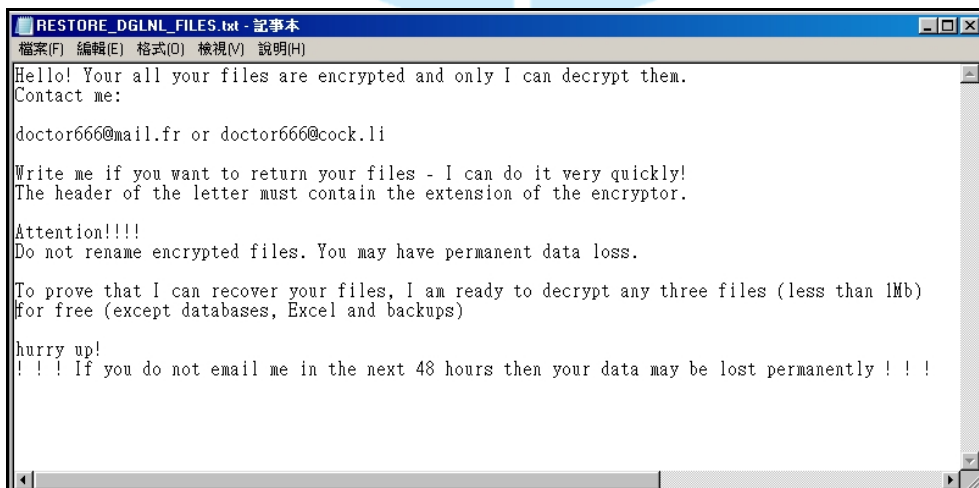
```
正在載入windows檔案
\Windows\system32\drivers\vdrvroot.sys
\Windows\system32\drivers\partmgr.sys
\Windows\system32\DRIVERS\compbatt.sys
\Windows\system32\DRIVERS\BATTC.SYS
\Windows\system32\drivers\volmgr.sys
\Windows\system32\drivers\volmgrx.sys
\Windows\system32\drivers\intelide.sys
\Windows\system32\drivers\PCIIDEX.SYS
\Windows\system32\DRIVERS\vmci.sys
\Windows\system32\drivers\vsock.sys
\Windows\System32\drivers\mountmgr.sys
\Windows\system32\drivers\atapi.sys
\Windows\system32\drivers\ataport.SYS
\Windows\system32\drivers\lsi_sas.sys
\Windows\system32\drivers\storport.sys
\Windows\system32\drivers\msahci.sys
\Windows\system32\drivers\amdxta.sys
\Windows\system32\drivers\fltmgr.sys
\Windows\system32\drivers\fileinfo.sys

Microsoft (R) windows (R) version 6.1 (build 7601: service pack 1)
2 system processors [2048 MB memory] multiprocessor kernel
The system is booting in safemode - minimal services
```

2. 在主機重新開機並進入安全模式後，發現惡意程式 KB4463527.exe 將主機對外的網路切斷，網路卡無法運作，並且桌面會出現 RESTORE_DGLNL_FILES.txt 的文字檔，可見在主機重開機、進入安全模式的過程中，主機內的檔案已被陸續加密，而且在安全模式下防毒軟體未啟動，無法攔阻此惡意程式的執行。當 KB4463527.exe 執行完加密作業後，會在原所在資料夾中消失。



3. 查看 RESTORE_DGLNL_FILES.txt 的內容，發現為一封勒索通知信。駭客告訴受害者所有檔案已被加密，只有他可以解密，並且告訴受害者可寫信到 doctor666@mail.fr 或 doctor666@cock.li 這兩個信箱與他聯絡。聯絡信件的主旨需含有主機被加密後延伸出的副檔名在內，也告訴受害者他可以免費對三個小於 1MB 的檔案解密，最後告訴受害者如果在 48 小時之內沒有寫信給他的話，被加密的資料將會永久遺失。



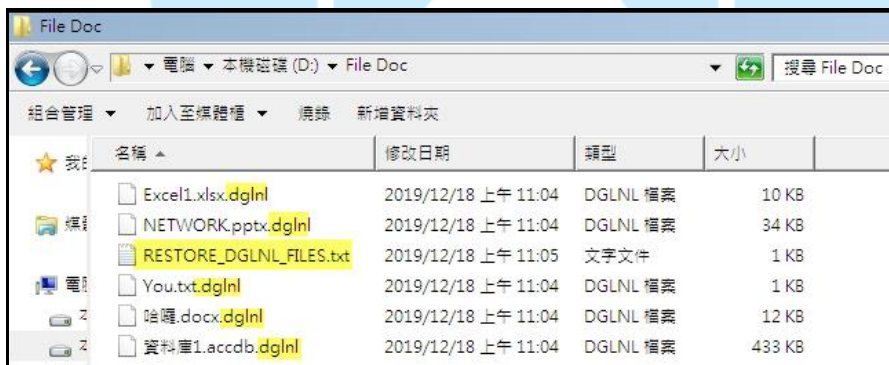
4. 檢視主機背景程式執行情形，發現 KB4463527.exe 執行後，會呼叫 bcdedit.exe 與 shutdown.exe 兩個程式。bcdedit.exe 會設定重開機後進入安全模式，而 shutdown.exe 則讓主機關機。

Process	Description	Command
KB4463527.exe (3512)		"C:\Users\Mark\Downloads\KB4463527.exe"
bcdedit.exe (2464)	開機設定資料編輯程式	c:\windows\System32\bcdedit.exe /set {current} safeboot minimal
bcdedit.exe (3732)	開機設定資料編輯程式	bcdedit /set {current} safeboot minimal
shutdown.exe (284)	Windows 關機與註釋工具	shutdown /r /f /t 00
shutdown.exe (3748)	Windows 關機與註釋工具	c:\windows\System32\shutdown.exe /r /f /t 00

(1) bcdedit.exe /set{current}safeboot minimal 是指使用 Windows 上的 BCDEDIT 工具，它會發出將 Windows 操作系統設置為以安全模式啟動的命令，然後立即在受感染的主機上強制地重新啟動。

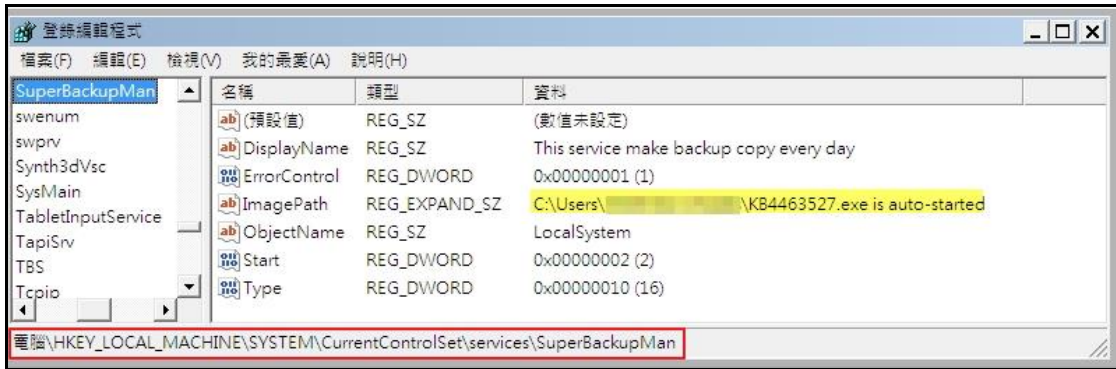
(2) shutdown /r /f /t 00 是將主機關機的命令。

5. 查看主機內各檔案的狀況，發現除了 C:\Windows 與 C:\Program Files 內的檔案外，所有檔案都被加密，並且在檔名後延伸出副檔名 dglnl，可見勒索病毒 Snatch 為了維護系統穩定性，才未對 C:\Windows 與 C:\Program Files 兩資料夾的檔案加密。此外，因主機重開機後對外網路不通的關係，使原先連線主機的網路磁碟機內的檔案未被加密。



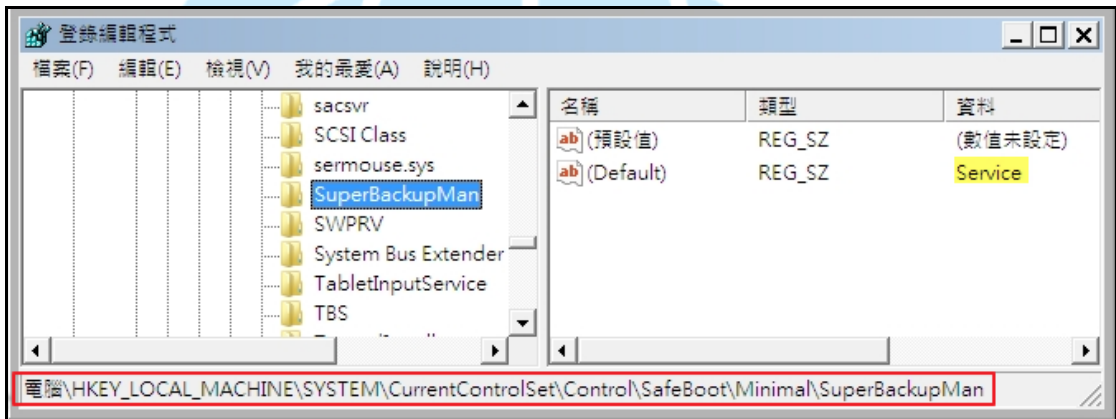
名稱	修改日期	類型	大小
Excel1.xlsx.dglnl	2019/12/18 上午 11:04	DGLNL 檔案	10 KB
NETWORK.pptx.dglnl	2019/12/18 上午 11:04	DGLNL 檔案	34 KB
RESTORE_DGLNL_FILES.txt	2019/12/18 上午 11:05	文字文件	1 KB
You.txt.dglnl	2019/12/18 上午 11:04	DGLNL 檔案	1 KB
哈囉.docx.dglnl	2019/12/18 上午 11:04	DGLNL 檔案	12 KB
資料重1.accdb.dglnl	2019/12/18 上午 11:04	DGLNL 檔案	433 KB

6. 檢視主機之登錄檔內容，發現在「電腦 \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\SuperBackupMan」內將 KB4463527.exe 設定為自動執行，而且定義 SuperBackupMan 服務為每天執行系統備份，有效地偽裝成一個合法的 Windows 系統服務。

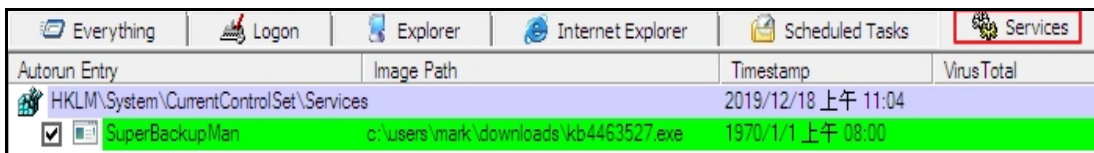


7. 在登錄檔「電腦

\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SafeBoot\Minimal\SuperBackupMan」內，發現勒索軟體 Snatch 將 SuperBackupMan 服務註冊在 Windows 登錄檔中，以便在安全模式啟動期間啟動它。



8. 使用 AutoRun 工具檢視，發現 RESTORE_DGLNL_FILES.txt 被設定在重開機後開啟，而 KB4463527.exe 被設定為一個名叫 SuperBackupMan 的 Windows 服務。



9. 檢視 SuperBackupMan 服務的屬性，得知它具有防止其在執行時被使用者卸載、暫停或停止的屬性，而 SuperBackupMan 的名稱通常會被使用者認為該

服務是系統備份工具的服務，將放鬆使用者的警惕心。

```

ca. 系統管理員: C:\Windows\system32\cmd.exe
Microsoft Windows [版本 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Mark>sc start SuperBackupMan

SERVICE_NAME: SuperBackupMan
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE                : 2   START_PENDING
                        <NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN>
        WIN32_EXIT_CODE       : 0   <0x0>
        SERVICE_EXIT_CODE   : 0   <0x0>
        CHECKPOINT           : 0x0
        WAIT_HINT            : 0x7d0
        PID                  : 2024
        FLAGS                 :
C:\Users\Mark>
    
```

10. 檢視 KB4463527.exe 的程式碼，發現該程式內含有 PGP 公鑰區塊，可見該勒索軟體的編碼者將 PGP 公鑰硬編碼到該檔案中。

```

.rdata:005CC620 aBeginPgpPublic db '-----BEGIN PGP PUBLIC KEY BLOCK-----',0Ah
.rdata:005CC620 ; DATA XREF: .text:0054408Fto
.rdata:005CC620 db 0Ah
.rdata:005CC620 db 'mQENBF2aIIIBCADBN685GzDuQ15Fin4zpnpcZnhbdjUQ74Rq7irrPEQYL1SowXj',0Ah
.rdata:005CC620 db 'n40Sud/xnwCNeoMIA2FeLPN+fS9cPasSgXqd6FRDGCAnfEe5JBlrSni0B4iU+MFe',0Ah
.rdata:005CC620 db '/RRH08UEe63MWTuoA3k5qwbvpaJPesX0tIQF+4F2YhkhRyNGUuoJ1ePc1F2Knhcg',0Ah
.rdata:005CC620 db '4JwsRwMgU/y0y3HsFWRb7BLlGdy0CaRmKuXa7Doo3mHD9FsuITh/MbFlA2v27ab5',0Ah
.rdata:005CC620 db 'mNY/Ehg5JAbF3Wm7jSfCRcBvEwu4571PDT4Huy2aCpn3L/SA/BFUGtoZeapxmcy',0Ah
.rdata:005CC620 db 'Em9S4S09pyuGJyJc6XMbYH+7FHwH1KxysUzXABEBAAG0FH11YnBzbGpmeHJldmdu',0Ah
.rdata:005CC620 db 'd2F0ZG16iQFUBBMBCAA+FiEEAafunu8Dq/zRU0diEqGvgbE0/y0FA12aIICGwMF',0Ah
.rdata:005CC620 db 'CQPCZwAFcWkIBWIGFQoJCAASBBYCAwEChgECF4AACgkQEgGvgbE0/y3f8gf/ayin',0Ah
.rdata:005CC620 db 'A311IxaSemsqUy+qTN5i9yi3sGQ6ItDrQOE0qnx8cx70cmX11a+MJ03UjR1Ux6B',0Ah
.rdata:005CC620 db 'h7rCwMfbxH5r8j9Ga/Uuci5doTQ9hSaBCcod1oWxuky6nYtFiHhNUhNRZ31WASek',0Ah
.rdata:005CC620 db 'y5aw9a2kngwA05n8b004jd2y3n1SKpN8S0gwbDw8MBH4mfTqpyM7Un2tXcKyh4T+',0Ah
.rdata:005CC620 db 'wGd5Nx2tzU0+awx6n2jqrQeU1aKu7hLK5WHPqkYpJUm0+3YUADSDo718p2z9L5X',0Ah
.rdata:005CC620 db 'zyUkaXWXC3qW0xU0zR2KZkEx/VuJ199zgpdd3U7n2eFC6W32v2aJv015yCaooa',0Ah
.rdata:005CC620 db 'dnkCwp9Y3X+18DXPtBkBDQRdmiCCAQgAt3AtiseIou9Ze75CHH00/mX80dkAjqhC',0Ah
.rdata:005CC620 db '4bK5WM2YCFifzZm9SANS/zxzUc5AeTfxyU5LXfhF5USJHZBa276G6jUD8u46Vwpi',0Ah
.rdata:005CC620 db '0QUJ/VDkjggAm4rEGwEsGj0x5bx366mrGiPydTU4e8g544v/o+U7ByxhiPnEoEp2',0Ah
.rdata:005CC620 db 'ciTANpI8ZL/qMTJ/P7E25UEpL/meBfuZ1F1Z2NB1NgStuPn/92Suk0Wyu0wC0yE',0Ah
.rdata:005CC620 db '1dp8KPGAvN00H00ymgXTEN2aaVir932r5p4T540pE2wkLHnFGBLTknv0rDAWDzY8',0Ah
.rdata:005CC620 db 'oAxLYGwME/fpUoC9aFQmhsFjcyEhK9DURAI/0tdvHLwEr3uN5ksF2QARAQABiQE2',0Ah
.rdata:005CC620 db 'BBgBCAAgFiEEAafunu8Dq/zRU0diEqGvgbE0/y0FA12aIICGwAAcQkQEgGvgbE0',0Ah
.rdata:005CC620 db '/y309Af/exVH5UBL4j9d17NStn0mUsa56YSH0A2U743SIJOPib9r+UkBeTur4oEe',0Ah
.rdata:005CC620 db '2T0cXZd5BwMdXc27eZ10UUVudGgZ8uzQ/AaujXZUN/6zEqzIXQ01MMDFKJf/dUz',0Ah
.rdata:005CC620 db '0bSSZ1a96amJSL43P7pEL4WiW2RoPQbLF9oMmq1MaapJyGHF29G7FhHE1e3UkzXM',0Ah
.rdata:005CC620 db 'ewIur86aYyF7FJq0m0Wvup2BFULx8i1Az7a1Gx8wMTLtnMa4rEQC0jL4sUQb+x',0Ah
.rdata:005CC620 db 'GLTKTJxiSuX87SBP3si60XUzkyteyNqChsa3GW7EU0u4RjypATCUNy89YSF',0Ah

.rdata:005CC620 db 'OqAL/ehJMc820ZnYc/acROujBW253A==',0Ah
.rdata:005CC620 db '=gCZP',0Ah
.rdata:005CC620 db '-----END PGP PUBLIC KEY BLOCK-----',0
    
```

11. 程式 KB4463527.exe 經 Virustotal 檢測，其惡意比例為 49/70，仍有多家防毒軟體公司無法識別它，而且有多家防毒軟體公司以 Snatch 命名它。



Community Score

49 engines detected this file

081fb13b0f7ee9750c2ea3ae037a29ec87a313b99a693027d4202
1cfda869fd8
KB4463527.txt

4.04 MB Size

2019-12-16 07:51:10 UTC
a moment ago

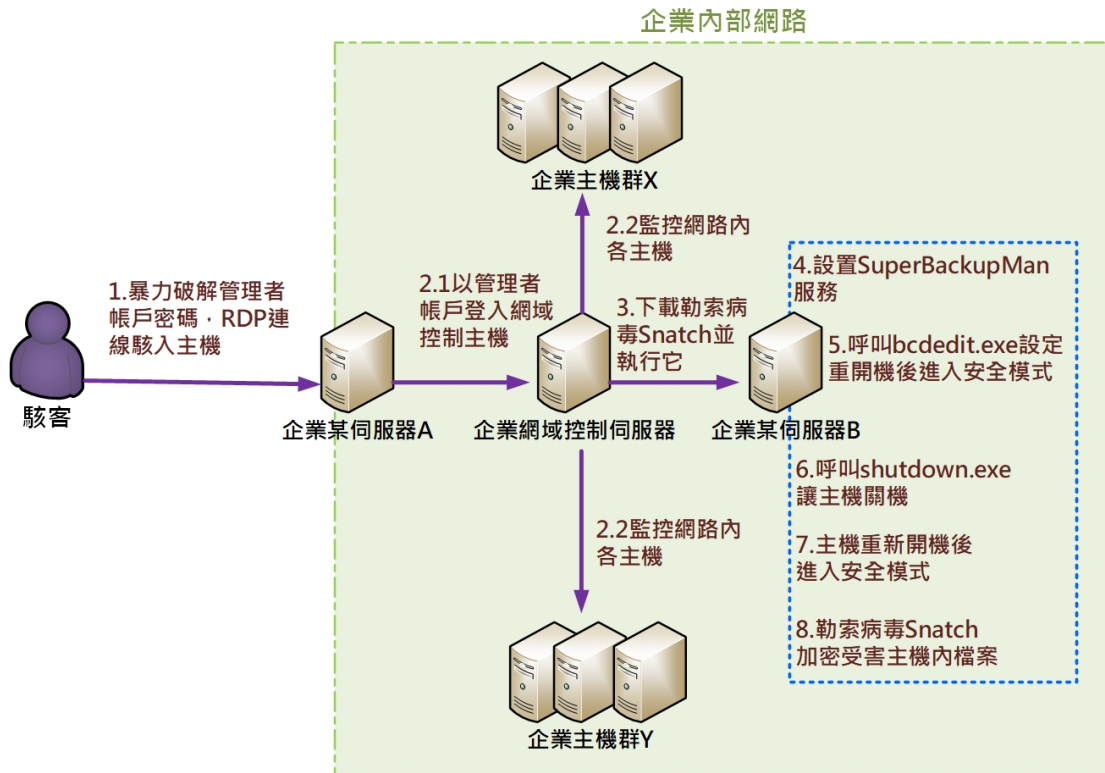
peexe




Ad-Aware	Trojan.GenericKD.41958056	AhnLab-V3	Trojan/Win32.FileCoder.C3631228
Alibaba	Ransom:Win32/Agent.cf9440ed	ALYac	Trojan.Ransom.Filecoder
Antiy-AVL	Trojan[Ransom]/Win32.Snatch	Arcabit	Trojan.Generic.D2803AA8
Avast	Win32:Xpaj-gen	AVG	Win32:Xpaj-gen
Avira (no cloud)	TR/Ransom.Gen	BitDefender	Trojan.GenericKD.41958056
BitDefenderTheta	Gen.NN.ZexaF.33550.@7W@aqmk36l	CAT-QuickHeal	Ransom.Gocoder
Comodo	Malware@#uwau74izvfhp	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cyren	W32/Trojan.YQMF-1641
DrWeb	Trojan.Encoder.29918	Emsisoft	Trojan.GenericKD.41958056 (B)
eScan	Trojan.GenericKD.41958056	ESET-NOD32	A Variant Of Win32/Filecoder.NYH
F-Secure	Trojan.TR/Ransom.Gen	FireEye	Trojan.GenericKD.41958056
Fortinet	W32/Agent.AVYDtr	GData	Trojan.GenericKD.41958056
Ikarus	Trojan-Ransom.Snatch	Jiangmin	Trojan.Snatch.b
K7AntiVirus	Trojan (0055a7ee1)	K7GW	Trojan (0055a7ee1)

Kaspersky	Trojan-Ransom.Win32.Agent.avyd	MAX	Malware (ai Score=100)
McAfee	Ransom-Snatch!9E76E62FFF6C	McAfee-GW-Edition	BehavesLike.Win32.PUPXER.rh
Microsoft	Ransom:Win64/Gocoder.P	NANO-Antivirus	Trojan.Win32.Encoder.gfsewh
Palo Alto Networks	Generic.ml	Panda	Trj/CI.A
Qihoo-360	Win32/Trojan.7e0	Rising	Trojan.Generic@ML.82 (RDML:iy0g...
Sangfor Engine Zero	Malware	Sophos AV	Troj/Snatch-H
Symantec	ML.Attribute.HighConfidence	TrendMicro	Ransom.Win32.SNATCH.B
TrendMicro-HouseCall	Ransom.Win32.SNATCH.B	VBA32	TrojanRansom.Agent
VIPRE	Trojan.Win32.GenericIBT	Webroot	W32.Ransom.Snatch
Yandex	Trojan.Agent!EkyOZ5Eagtc	Zillya	Trojan.Filecoder.Win32.10869
ZoneAlarm by Check Point	Trojan-Ransom.Win32.Agent.avyd	Dr.Web vxCube	RANSOM MALWARE
SecondWrite	MALWARE RANSOM	Acronis	Undetected

三、事件攻擊行為示意圖



1. 駭客透過暴力攻擊破解管理者帳戶的密碼後，侵入企業內部網路，並且使用遠端桌面連線登入伺服器。
2. 利用管理者帳戶登入同一網路上的網域控制伺服器，並且監控整個網域內的主機。
3. 受害主機下載勒索軟體 Snatch 的檔案到硬碟中，並且執行它。
4. 勒索軟體 Snatch 設置自己為一個名為 SuperBackupMan 的 Windows 服務。
5. 勒索軟體 Snatch 呼叫 bcdedit.exe 設定重開機後進入安全模式。
6. 勒索軟體 Snatch 呼叫 shutdown.exe 讓主機關機。
7. 受害主機重新開機後進入安全模式。
8. 勒索軟體加密受害主機內的檔案。

四、總結與建議

1. 勒索軟體 Snatch 會將自身設置為在安全模式啟動期間運行的服務。它可

以快速將主機重新啟動到安全模式，並且在大多數軟體無法執行的安全模式環境中，Snatch 會對受害者的硬碟資料進行加密。

2. 勒索軟體 Snatch 將主機重開機進入安全模式後，主機對外的網路呈現斷網狀態，故惡意程式 Snatch 的加密檔案範圍僅限受害主機。
3. 勒索軟體 Snatch 透過啟動安全模式的方式繞過防毒軟體的阻攔，增加攻擊成功的機會，非一般典型的勒索軟體。
4. 勒索軟體 Snatch 建立降低使用者防備心的 Windows 服務 SuperBackupMan，讓自己在主機重新開機後在安全模式下持續進行著。
5. 關於 Snatch 攻擊事件的預防措施，有下列幾點建議。
 - (1) 不將遠端桌面連線(RDP)的平台暴露在未受保護的網路上，當有連線需求時，可透過 VPN 的方式進行企業內部網路的 RDP 連線。
 - (2) 對提供遠端連線服務的軟體與可能造成 Webshell 和 SQL Injection 攻擊的漏洞進行控管與偵測。
 - (3) 當系統管理者帳戶登入主機時，應實施多因素身分驗證的方式來進行伺服器的登入，降低暴力攻擊成功的機率。
 - (4) 多台伺服器的管理者帳戶不可使用相同一組帳戶名稱與密碼。
 - (5) 加強管理者帳戶的密碼設定之複雜度，並且定期更換密碼。
 - (6) 企業內部網路內所分享的重要文件資料夾，應設置存取權限的管控機制。
 - (7) 定期檢測各伺服器內系統與軟體之漏洞，並進行修補。
 - (8) 定期檢查各伺服器是否存在異常事件行為。如是否有新增帳戶、Guest 帳戶是否被啟用、Windows 系統日誌是否有異常、防毒軟體是否有執行錯誤或異常中止之現象等。
 - (9) 定期備份各伺服器的資料與定期更新防毒軟體病毒碼。

五、相關報導

1. Snatch Ransomware Reboots to Windows Safe Mode to Bypass AV Tools

<https://www.bleepingcomputer.com/news/security/snatch-ransomware-reboots-to-windows-safe-mode-to-bypass-av-tools/>

2. 勒索軟體將電腦以安全模式重開機以躲過防毒偵測

<https://www.ithome.com.tw/news/134771>

3. Snatch ransomware reboots PCs into Safe Mode to bypass protection

<https://news.sophos.com/en-us/2019/12/09/snatch-ransomware-reboots-pcs-into-safe-mode-to-bypass-protection/>

