

**TLP:WHITE**

# **勒索軟體 Big Head 分析報告**



**臺灣學術網路危機處理中心團隊(TACERT)製**

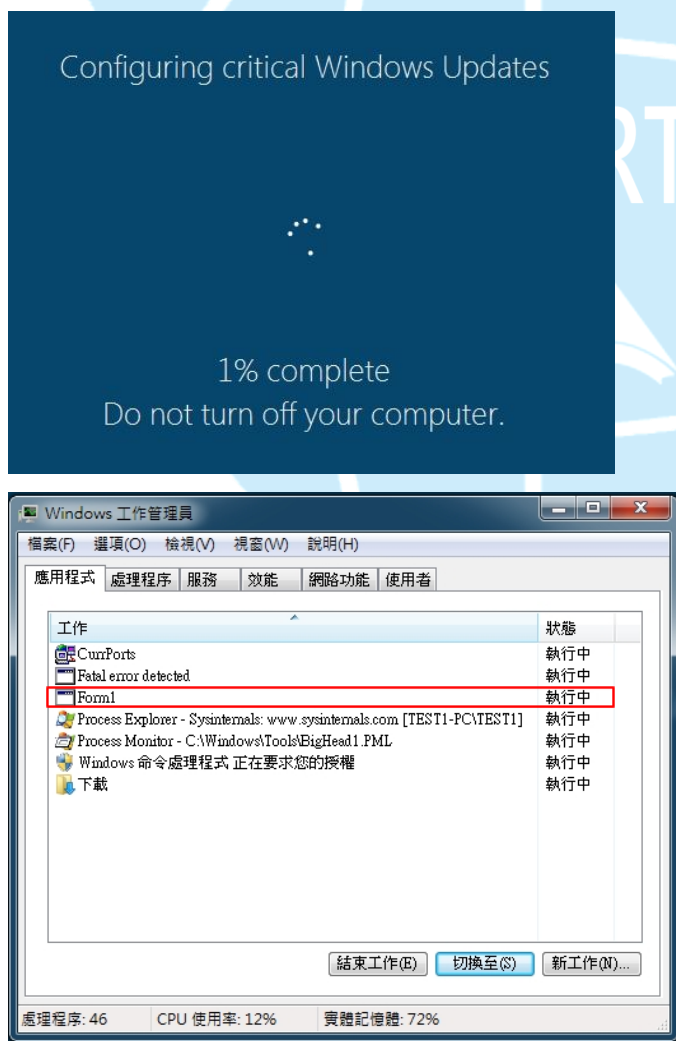
**2023 年 08 月**

## 一、事件簡介

1. 2023/5 出現勒索軟體 Big Head，它藉著 Windows 更新程式或 Word 安裝檔案的方式來利用惡意廣告散布。為了解該勒索軟體之攻擊行為，故進行該樣本檢測作業。

## 二、事件檢測

1. 在 64 位元的 Windows 7 作業系統上，執行 Big Head 樣本 6d27c1b457.exe。  
在執行後，主機出現 Windows Update 的畫面。該畫面會執行很久，X% complete 會跑很慢，最終只能使用 Windows 工作管理員關閉該執行程序 Form1。



2. 在 6d27c1b457.exe 執行後，會每間隔一秒重複呼叫 1.exe 來執行，產生很多呼叫程序。除了關機外，無法利用 Windows 工作管理員來中斷執行中的 1.exe。

Process	D. Command	Start Time	End Time
6d27c1b457.exe (1616)	"C:\Users\TEST1\Downloads\6d27c1b457.exe"	2023/8/4 下午 04:45:38	2023/8/4 下午 04:45:39
1.exe (1080)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:39	2023/8/4 下午 04:45:40
1.exe (752)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:40	2023/8/4 下午 04:45:42
1.exe (948)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:42	2023/8/4 下午 04:45:43
1.exe (876)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:43	2023/8/4 下午 04:45:44
1.exe (2252)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:44	2023/8/4 下午 04:45:46
1.exe (1656)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:45	2023/8/4 下午 04:45:47
1.exe (168)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:47	2023/8/4 下午 04:45:48
1.exe (780)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:48	2023/8/4 下午 04:45:49
1.exe (2528)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:49	2023/8/4 下午 04:45:50
1.exe (1424)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:50	2023/8/4 下午 04:45:52
1.exe (2652)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:52	2023/8/4 下午 04:45:53
1.exe (2504)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:53	2023/8/4 下午 04:45:54
1.exe (1452)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:54	2023/8/4 下午 04:45:55
1.exe (1544)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:55	2023/8/4 下午 04:45:57
1.exe (1428)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:57	2023/8/4 下午 04:45:58
1.exe (1420)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:58	2023/8/4 下午 04:45:59
1.exe (964)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:45:59	2023/8/4 下午 04:46:00
1.exe (740)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:00	2023/8/4 下午 04:46:01
1.exe (1196)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:01	2023/8/4 下午 04:46:03
1.exe (2492)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:03	2023/8/4 下午 04:46:04
1.exe (1032)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:04	2023/8/4 下午 04:46:05
1.exe (2984)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:05	2023/8/4 下午 04:46:07
1.exe (3068)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:07	2023/8/4 下午 04:46:10
1.exe (168)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:09	2023/8/4 下午 04:46:11
1.exe (2784)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:11	2023/8/4 下午 04:46:12
1.exe (988)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:12	2023/8/4 下午 04:46:14
1.exe (1412)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:13	2023/8/4 下午 04:46:15
1.exe (2212)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:15	2023/8/4 下午 04:46:16
1.exe (2816)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:16	2023/8/4 下午 04:46:17
1.exe (23)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:17	2023/8/4 下午 04:46:19
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:19	2023/8/4 下午 04:46:20
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:20	2023/8/4 下午 04:46:21
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:21	2023/8/4 下午 04:46:22
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:22	2023/8/4 下午 04:46:24
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:23	2023/8/4 下午 04:46:25
1.exe ( )	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"	2023/8/4 下午 04:46:25	2023/8/4 下午 04:46:26

3. 在 6d27c1b457.exe 執行後，會呼叫 1.exe、archive.exe 與 xarch.exe 來執行。1.exe 是一款勒索軟體，會產生自身的副本以進行散播。archive.exe 會產出一個名為 teleratserver.exe 的檔案來執行。teleratserver.exe 是一個 Telegram 機器人，負責與威脅參與者的聊天機器人 ID 建立通訊。xarch.exe 會產出一個名為 BXIUssB.exe 的檔案來執行。BXIUssB.exe 是一款加密檔案並將檔案名稱編碼為 Base64 的勒索軟體。它還會顯示虛假的 Windows 更新畫面，以欺騙受害者，讓他們認為惡意活動是合法程序。

6d27c1b457.exe (1616)	"C:\Users\TEST1\Downloads\6d27c1b457.exe"
1.exe (1080)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\1.exe"
archive.exe (1384)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\archive.exe"
teleratserver.exe (904)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\teleratserver.exe"
teleratserver.exe (1428)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\teleratserver.exe"
teleratserver.exe (2808)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\teleratserver.exe"
Xarch.exe (3048)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Xarch.exe"
BXIUssB.exe (2424)	"C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\BXIUssB.exe"

4. Big Head 樣本 6d27c1b457.exe 執行後會產出下表所列相關惡意程式，大致可分為三種程式：勒索軟體(BigHead)、下載器(Downloader/ Dropper)與 Telebot。

惡意程式	Virustotal	說明
6d27c1b457.exe	42/55	木馬/Downloader/Dropper
1.exe	59/71	木馬/Dropper/Agent/解密後產出 1.exe

惡意程式	Virustotal	說明
archive.exe	54/71	木馬/Agent/Dropper/解密後產出 teleratserver.exe
Teleratserver.exe	43/70	木馬/Telerat/telebot/
Xarch.exe	56/71	木馬/Dropper/Agent/解密後產出 BXIuSsB.exe
BXIuSsB.exe	62/71	Ransom.BigHead.D/執行時會出現 Windows update 畫面

5. 6d27c1b457.exe 執行後被加密的檔案之檔名呈現亂碼。經檢測發現是將原來的檔案名稱使用 Base 64 加密後產生亂碼的檔名。此方法與以往勒索病毒將副檔名延伸之命名方式不同。



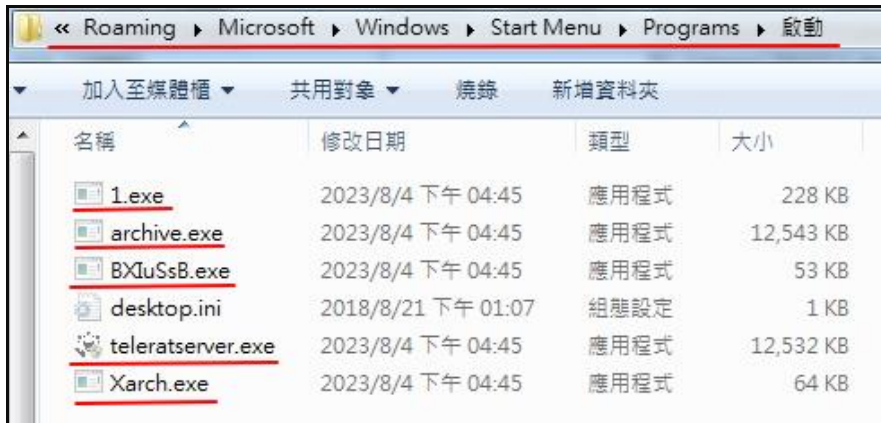
6. 6d27c1b457.exe 執行後，會在

C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start

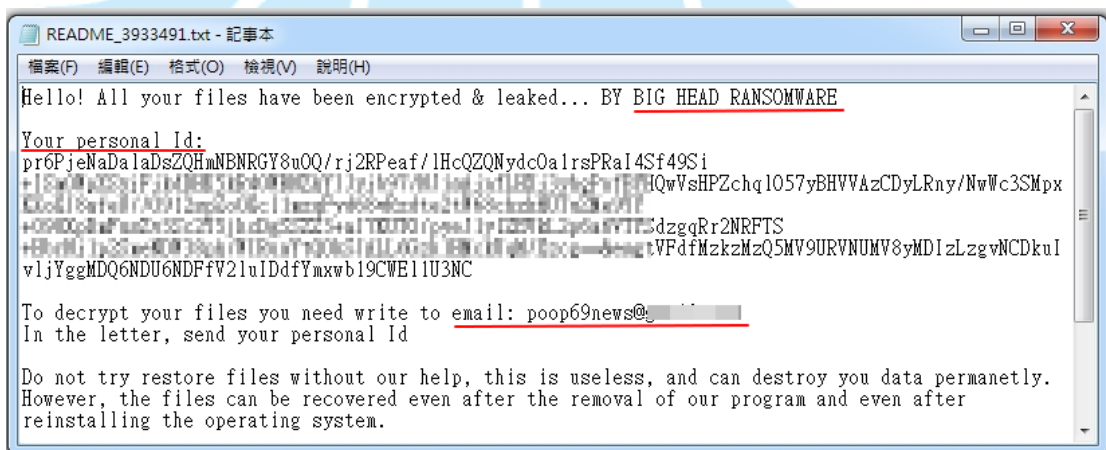
Menu\Programs\Startup 資料夾內存放五個隱藏的惡意程式，並且修改登錄檔，讓這些程式在每次開機後執行。

Autorun Entry	Description	Publisher	Image Path	Timestamp
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				2023/8/4 下午 04:45
1			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\1.exe	2023/4/13 上午 12:29
archive			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\archive.exe	2023/4/13 上午 12:17
BXIuSsB	Biclavex	Osoutpek	c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\bxiussb.exe	2021/12/13 上午 01:44
teleratserver			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\teleratserver.exe	2020/1/5 下午 08:15
Xarch			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\xarch.exe	2023/4/13 上午 12:18
C:\Users\TEST1\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup				2023/8/4 下午 05:42
1.exe			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\1.exe	2023/4/13 上午 12:29
archive.exe			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\archive.exe	2023/4/13 上午 12:17
BXIuSsB.exe	Biclavex	Osoutpek	c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\bxiussb.exe	2021/12/13 上午 01:44
teleratserver.exe			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\teleratserver.exe	2020/1/5 下午 08:15
Xarch.exe			c:\users\test1\appdata\roaming\microsoft\windows\start menu\programs\startup\xarch.exe	2023/4/13 上午 12:18

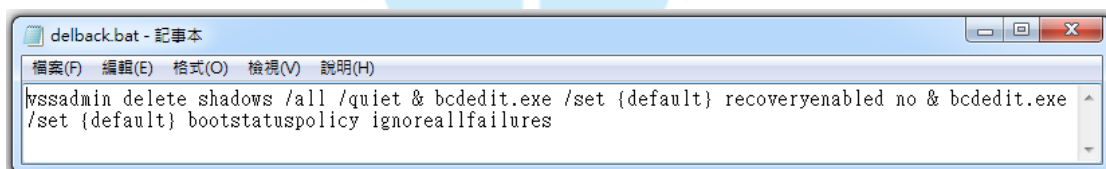




7. 6d27c1b457.exe 執行後，會在每個訪問過的資料夾與桌面放入勒索通知信 README\_3933491.txt。該 txt 檔說明所有檔案已被 BIG HEAD 勒索病毒加密，告知受害者 Personal ID 資訊，並且提供一個 E-mail 信箱給受害者聯絡駭客使用。



8. 它會使用 C:\使用者\TEST1\AppData\Roaming\delback.bat 下命令，並繼續刪除可用的影子副本。



9. 該勒索軟體會避開包含以下子字串的目錄，不加密檔案。

- (1) Windows。
- (2) RECYCLER、Recycler、Recycle.Bin、RECYCLE.BIN。
- (3) Program Files、Program Files (X86)。

(4) ProgramData。

(5) TEMP、Temp。

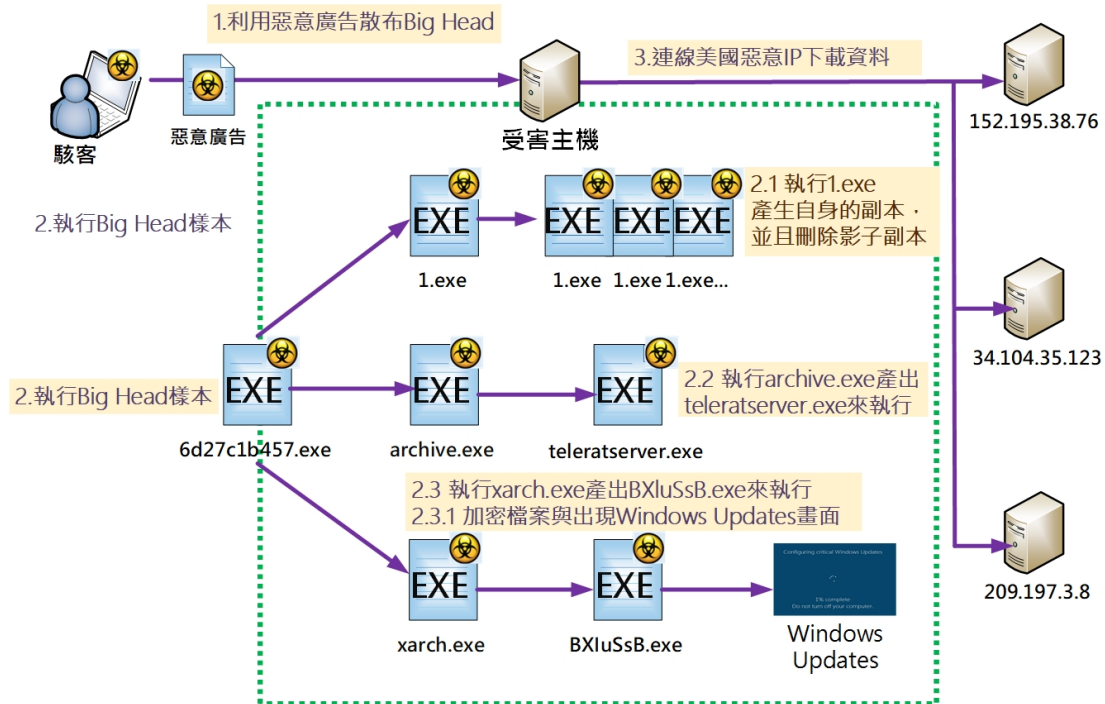
(6) AppData。

10.從側錄封包發現主機會對外連線下表 IP，其中有 3 個惡意 IP，而且這些 IP 有下載資料之行為。

目的 IP	Location	Host	Virustotal
152.195.38.76	US	ocsp.digicert.com Csc3-2010-crl.verisign.com	1/88
152.199.38.90	US	ocsp.verisign.com s2.symcb.com	—
172.217.163.35	US	ocsp.pki.goog Crl.pki.goog	—
34.104.35.123	US	Edgedl.me.gvtl.com ( download-server)	2/88
209.197.3.8	US	www.download.windowsupdate.com (下載)	9/88

### 三、攻擊行為

經由樣本檢測，可推測出駭客攻擊手法。首先 Big Head 透過惡意廣告散布，當受害主機執行 Big Head 後，會產生一些隱藏的惡意程式於受害主機內執行。它除了加密檔案外，會出現 Windows updates 畫面欺騙受害者、刪除影子副本，將被加密檔案之檔名以 Base64 加密產生之亂碼命名。它也會連線美國 IP 下載資料。從其攻擊手法可看出它與傳統的勒索軟體單純地將檔案加密不同，它演變成除了勒索功能外，還搭配多種的惡意程式來進行多樣化的攻擊行為。



#### 四、總結與建議

1. 經由檢測 BigHead 變種樣本，發現勒索軟體 Big Head 試圖結合不同的惡意程式來增加攻擊威力。
2. 被它加密過的檔案會經由 base64 編碼產生新檔名，此點與以往之勒索軟體特徵不同。
3. Big Head 利用提供 Windows 更新程式來欺騙使用者，一旦使用者不慎依照駭客的指示執行前述的「安裝程式」，螢幕會顯示正在更新的畫面，但在此同時，勒索軟體也在背景執行檔案加密。
4. 駭客所使用的攻擊手法不複雜，也不難讓防毒軟體察覺，但對於使用者還是有很高風險，因為使用者很有可能因為是 Windows 更新或是應用程式安裝畫面，而忽略其危險性。
5. 為了預防它，建議使用者不開啟或執行不明來源的網頁或檔案。