TLP:WHITE

雙重勒索軟體 LockBit 3.0 分析報告

臺灣學術網路危機處理中心團隊(TACERT)製

2022 年 07 月

一、事件簡介

1. 2019/9 LockBit 首次出現，至 2021/6 出現升級版 LockBit 2.0 (勒索軟體即服務(RaaS))。到 2022/6 新版 LockBit 3.0（又名 LockBit Black）產生，而 LockBit 3.0 的新變種採用了新的勒索軟體策略，並首次推出了勒索軟體漏洞賞金計劃。
2. 由下圖發現在 Conti 攻擊下降的情況下，LockBit 的攻擊在 2021/7 開始出現逐漸上升的大量攻擊趨勢，至 2022/3 達到高峰。

上圖為 2020 年 8 月至 2022 年 3 月期間受 LockBit(綠色直條)攻擊之每月受害組織的統計和累計數量(資料來源:趨勢科技 Conti vs. LockBit: A Comparative Analysis of Ransomware Groups (June 27, 2022 發佈))

3. 為了解 Lockbit 3.0 的攻擊行為，故對其樣本進行檢測作業。

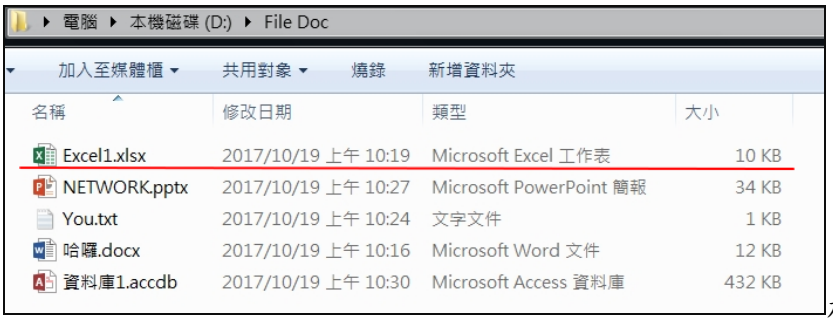
二、 事件檢測

1. 在 32 位元的 Windows 7 作業系統上執行 LockBit 3.0 樣本 d61af.exe (MD5:628e4a77536859ffc2853005924db2ef)後，馬上出現勒索通知信 HLJkNskOq.README.txt。在執行加密完成後，d61af.exe 在原資料夾內消失。

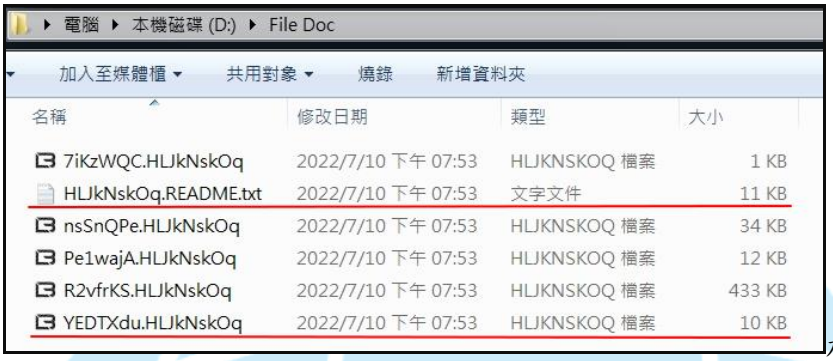
執行前

執行後

2. 該樣本 d61af.exe 執行後，不會加密圖檔，只會將主機內一些資料類型的檔案加密，並將檔名改為「亂碼.HLJkNskOq 」。

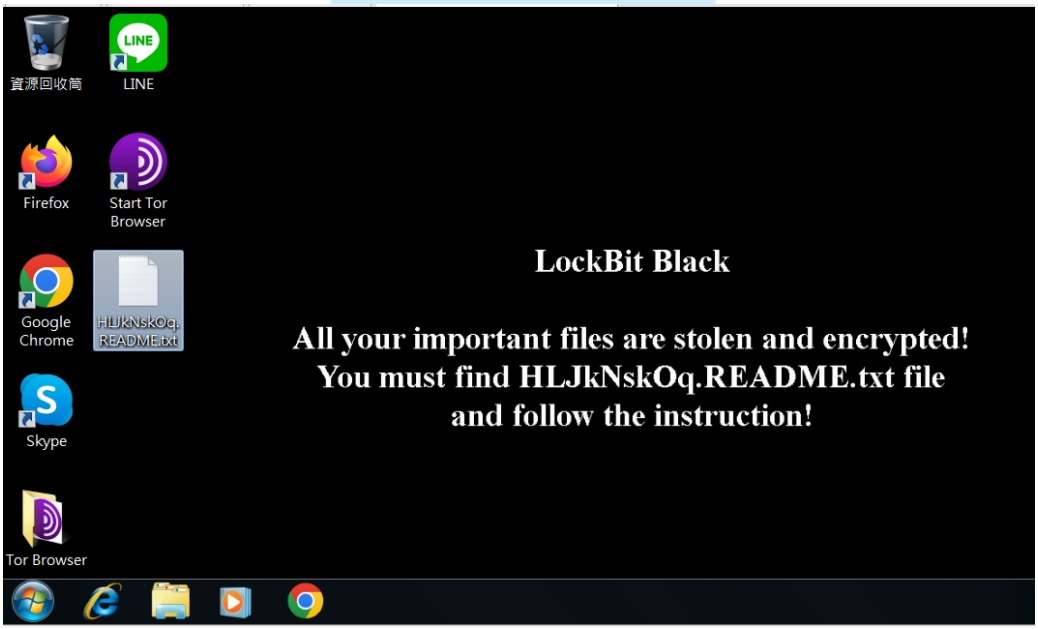


加密前



加密後

3. 接著桌面會出現標題為 LockBit Black 的桌布與 HLJkNskOq.README.txt 的勒索通知信。

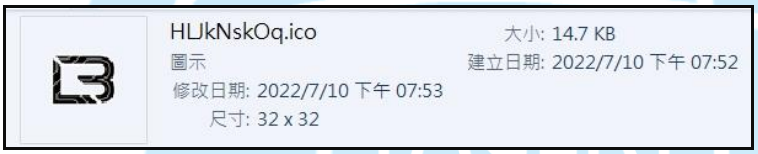


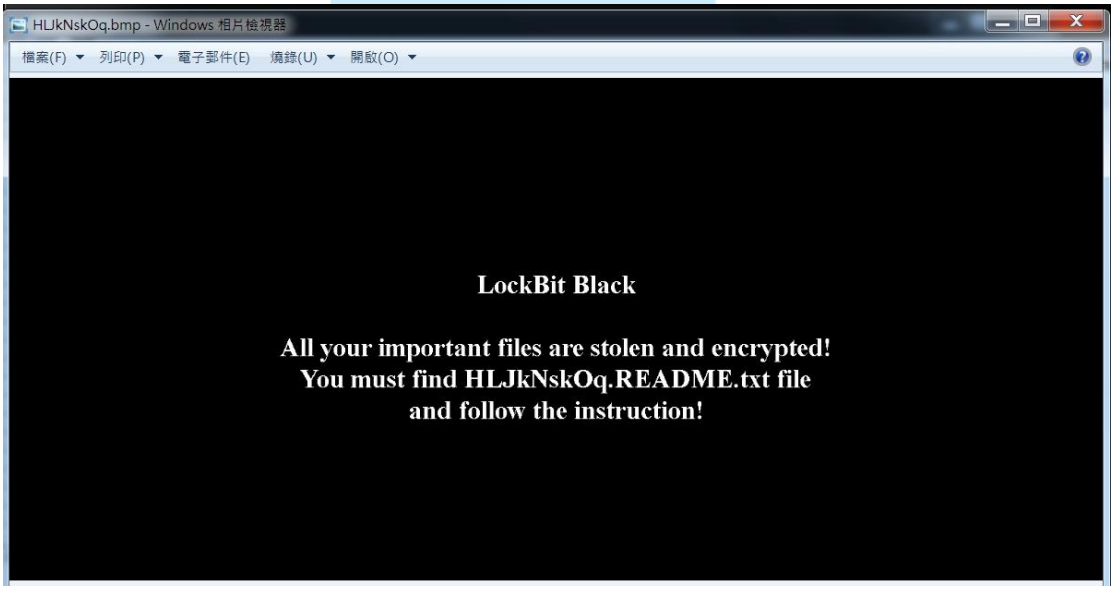
4. d61af.exe (PID:2420)執行後，會加密資料類型的檔案、變更檔名、產生勒索通知信，並且竊取這些加密資料。

5. d61af.exe (PID:2420)執行後，會啟動服務執行另一個程序 d61af.exe(PID:3148)。該程序會在 C:\ProgramData 產生 1376.tmp 此暫存檔，最後會執行 cmd.exe 刪除 1376.tmp。

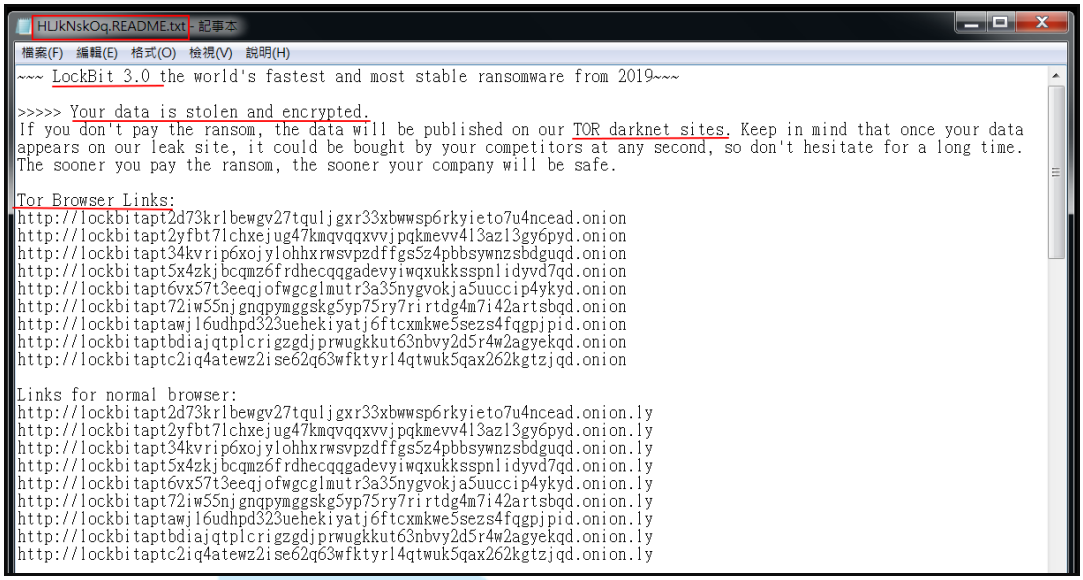
Process	Command	Start Time	End Time
wininit.exe (408)	wininit.exe	2022/7/10 下午 07:34:55	n/a
services.exe (500)	C:\Windows\system32\services.exe	2022/7/10 下午 07:34:55	n/a
svchost.exe (644)	C:\Windows\system32\svchost.exe -k DcomLaunch	2022/7/10 下午 07:34:56	n/a
DllHost.exe (3620)	C:\Windows\system32\DllHost.exe /Processid:{3E5FC7F9-9A51-4367-9063-A120...	2022/7/10 下午 07:52:57	2022/7/10 下午 07:53:02
d61af.exe (3148)	"C:\Users\Ruby\Downloads\d61af.exe"	2022/7/10 下午 07:52:57	2022/7/10 下午 07:53:20
1376.tmp (632)	"C:\ProgramData\1376.tmp"	2022/7/10 下午 07:53:20	2022/7/10 下午 07:55:15
cmd.exe (2564)	"C:\Windows\System32\cmd.exe" /C DEL /F /Q C:\PROGRA~2\1376.tmp >> NUL	2022/7/10 下午 07:55:15	2022/7/10 下午 07:55:15

6. 在 C:\ProgramData 內發現 d61af.exe 加密檔案後做為桌布之圖檔 HLJkNskOq.bmp 與做為被加密檔案之圖示的 HLJkNskOq.ico 。

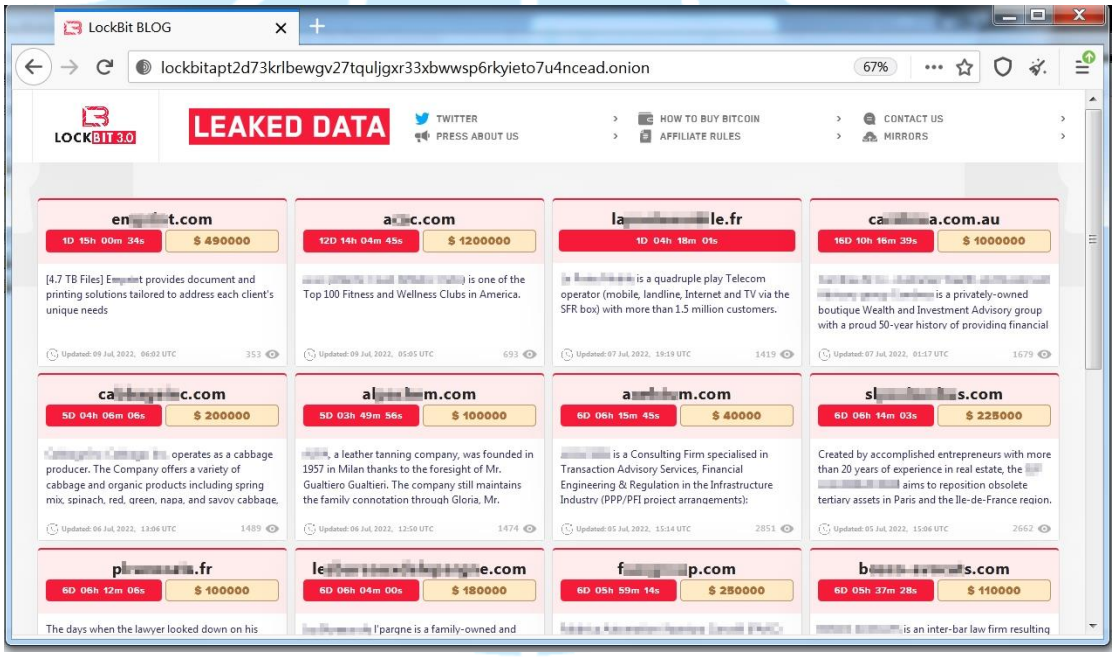




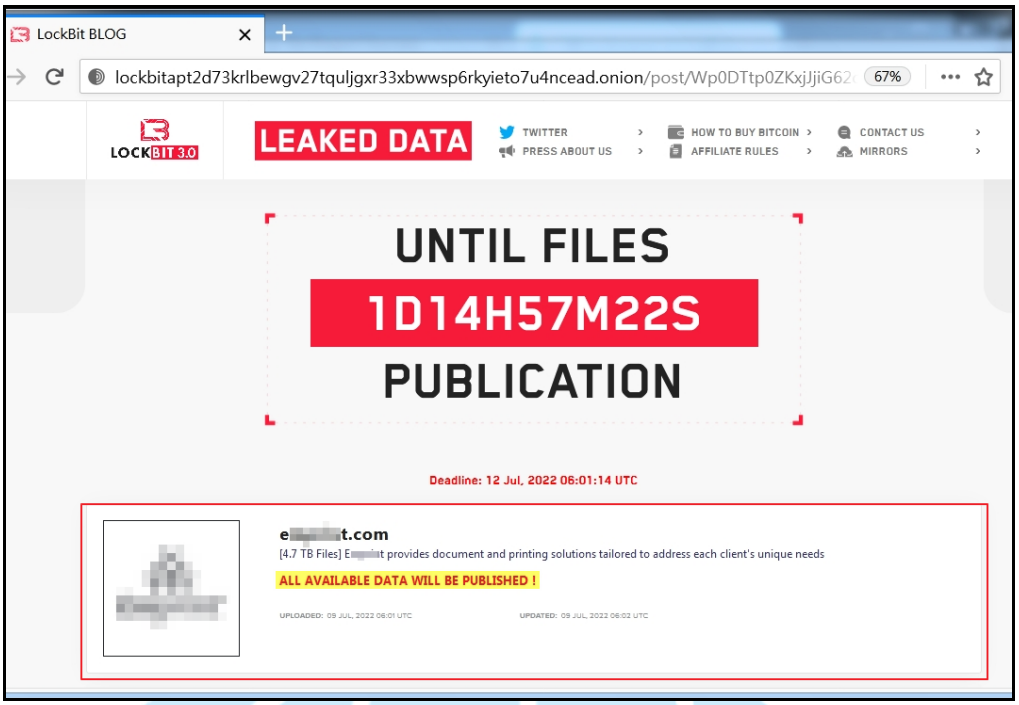
7. 勒索通知信 HLJkNskOq.README.txt 內容攏長，一開始告訴受害者你的資料被竊取與被加密，若不給付贖金會將資料公布於 TOR 暗網上，而且可能瞬間被您的競爭者買走資料。



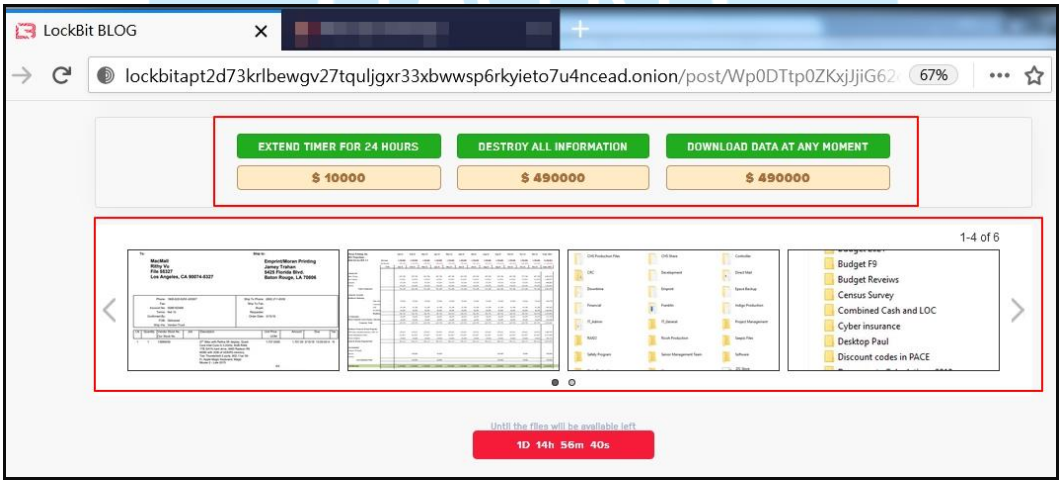
8. 它提供多個 LockBit BLOG 連結，連結開啟可以看到許多個即將贖金到期的受害組織名稱與其資料。



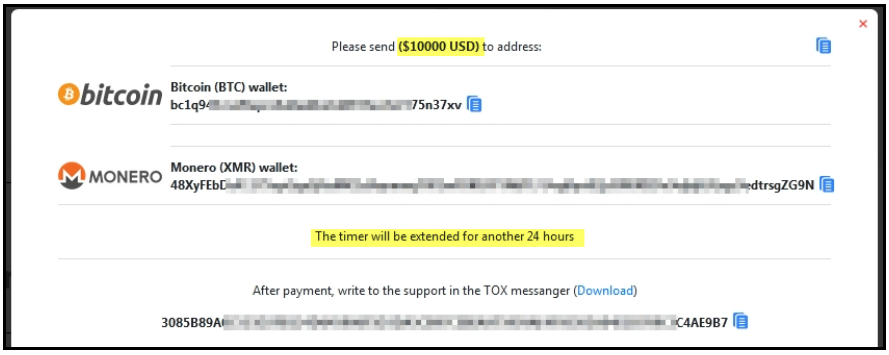
9. 瀏覽某受害組織被公告的內容，發現網頁上會有檔案預計被發佈的剩餘時間、組織名稱、被竊資料檔案的大小、給付贖金的最後期限時間、付贖金的方式與被竊取資料的樣本等資訊。此種建置受害組織公告網站的方式與以往勒索軟體的攻擊策略不同，它告知受害者若不付贖金的後果將會很大，加強受害者的壓力。



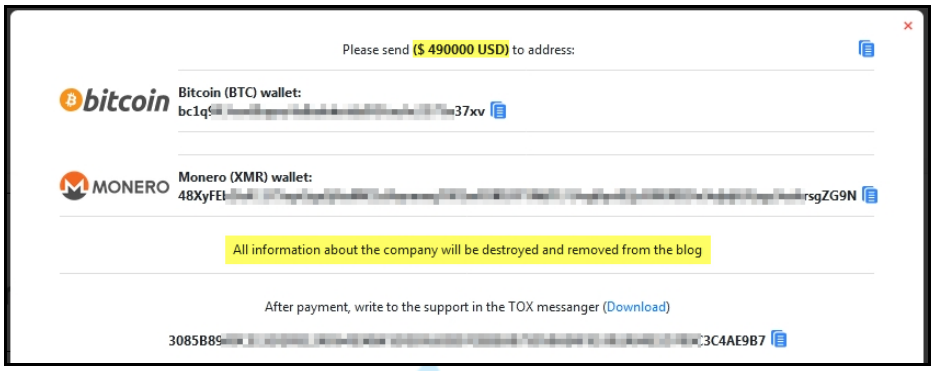
10.LockBit 3.0 提供受害組織三個選擇方案，分別為展延時間 24 小時($10,000)、銷毀所有資料($490,000)與取得獨家下載所有公司資料的權限($490,000)，而每個方案的支付金額會因受害組織不同而有差異。



方案 1:支付一萬美金，計時器將再延長 24 小時。

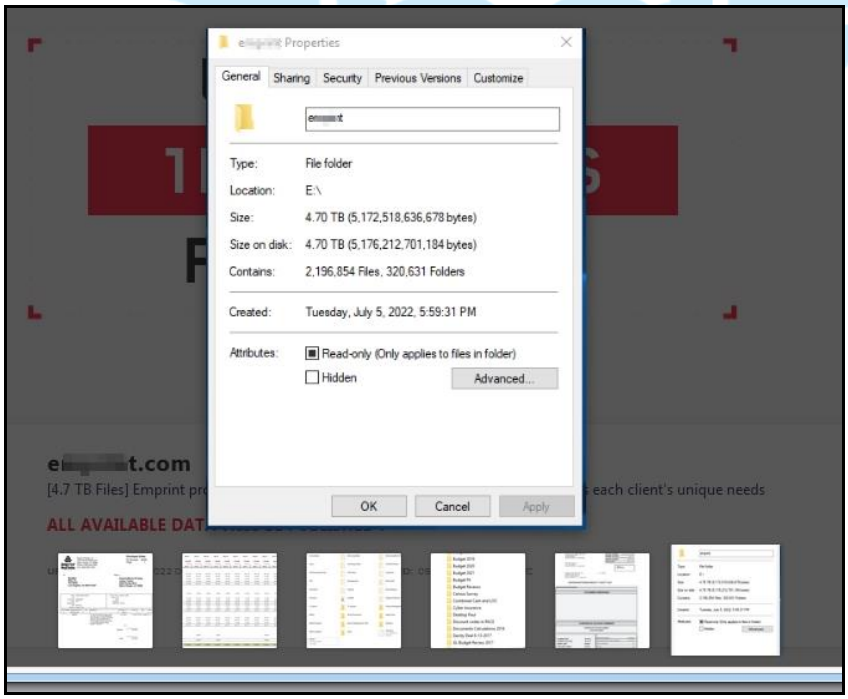


方案 2:支付 49 萬美金，所有有關公司的所有資訊將被銷毀，並且從 BLOG 中刪除。

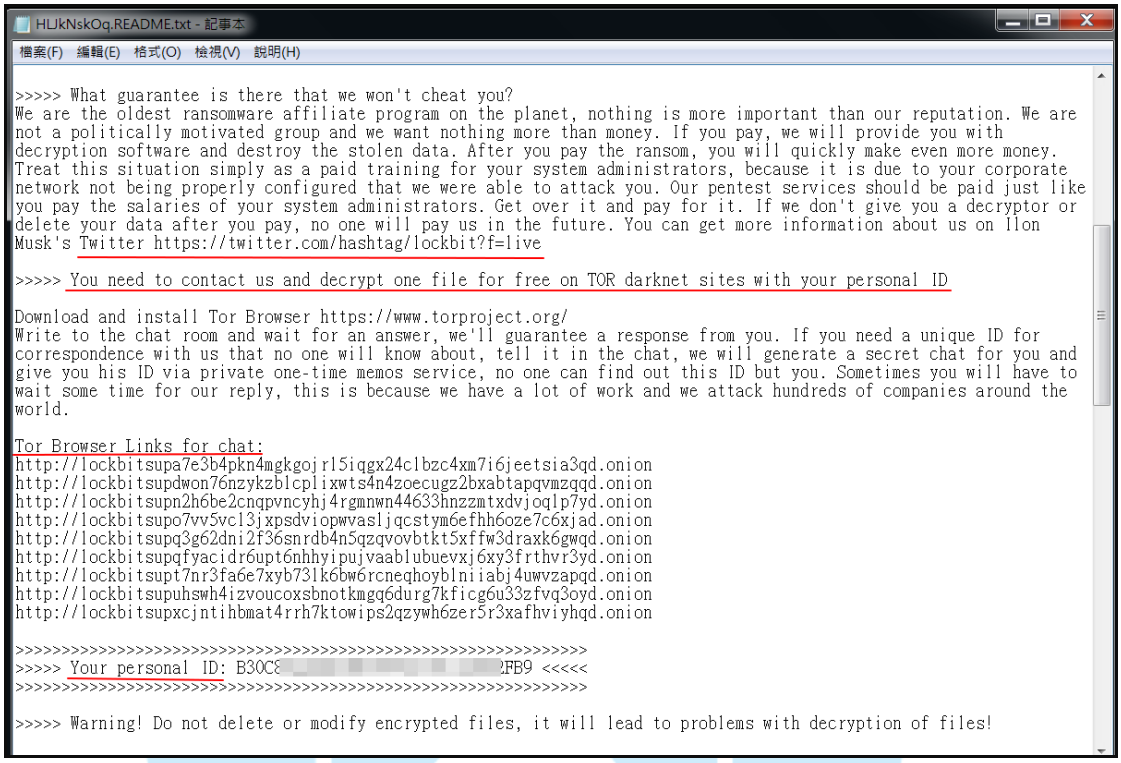


方案 3:支付 49 萬美金，獲得獨家下載所有公司資料的權限。

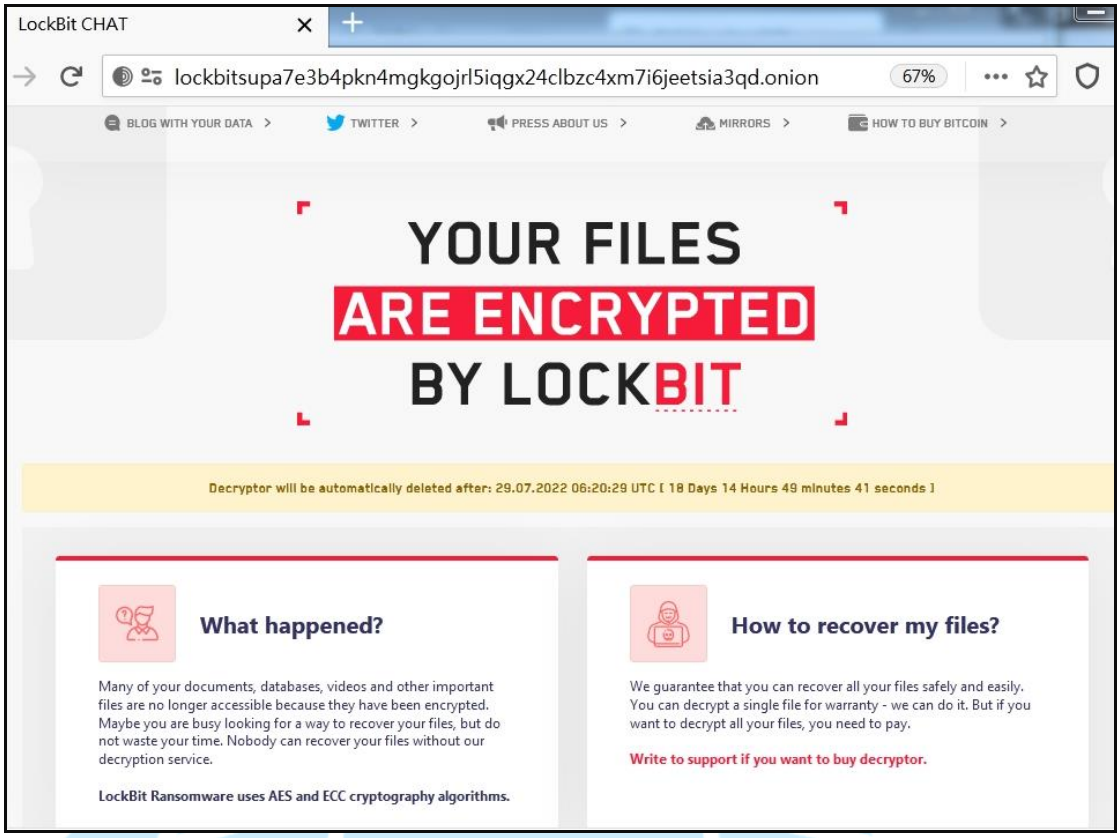
11. 為了取信於受害組織，駭客在 BLOG 上公開受害組織資訊的頁面也提供所竊取資料的佐證與截圖，以證明有竊走該組織之資料。

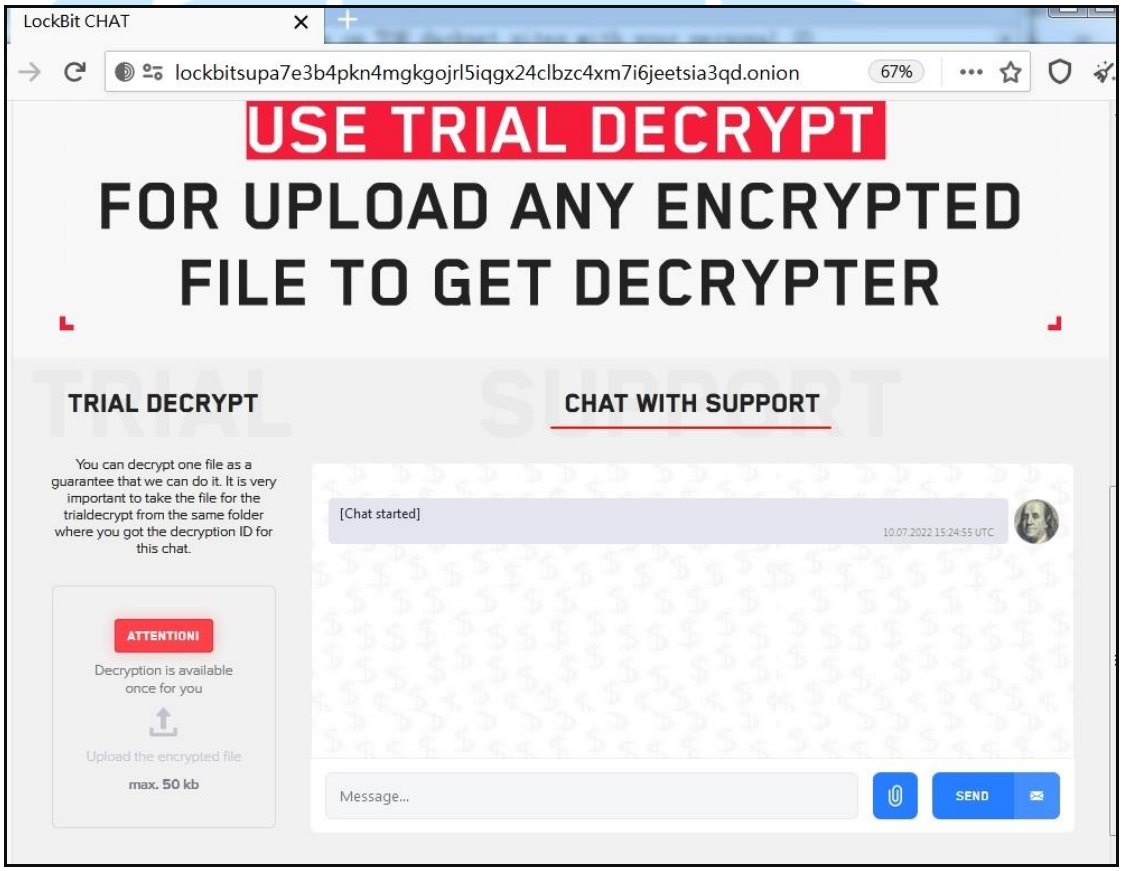


12.該勒索團體告訴受害者如何保證不欺騙受害者，並且提供 Twitter 上大家討論 LockBit 攻擊的連結。他們也告訴受害者可以透過 LockBit CHAT 的連結與 Personal ID 與他們聯絡。在 LockBit CHAT 頁面輸入 Personal ID 與驗證碼即可登入到受害者專屬與駭客洽談頁面。

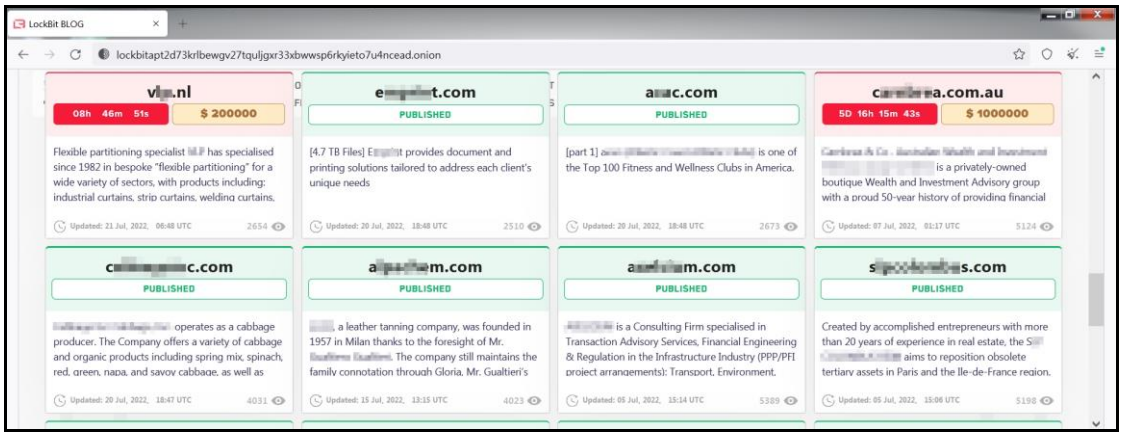


13.在受害者與駭客洽談頁面，駭客再次告訴受害者你的檔案被加密了，以及要如何復原檔案。該網頁可讓受害者給駭客留言與提供受害者試用解密器解密一個檔案。

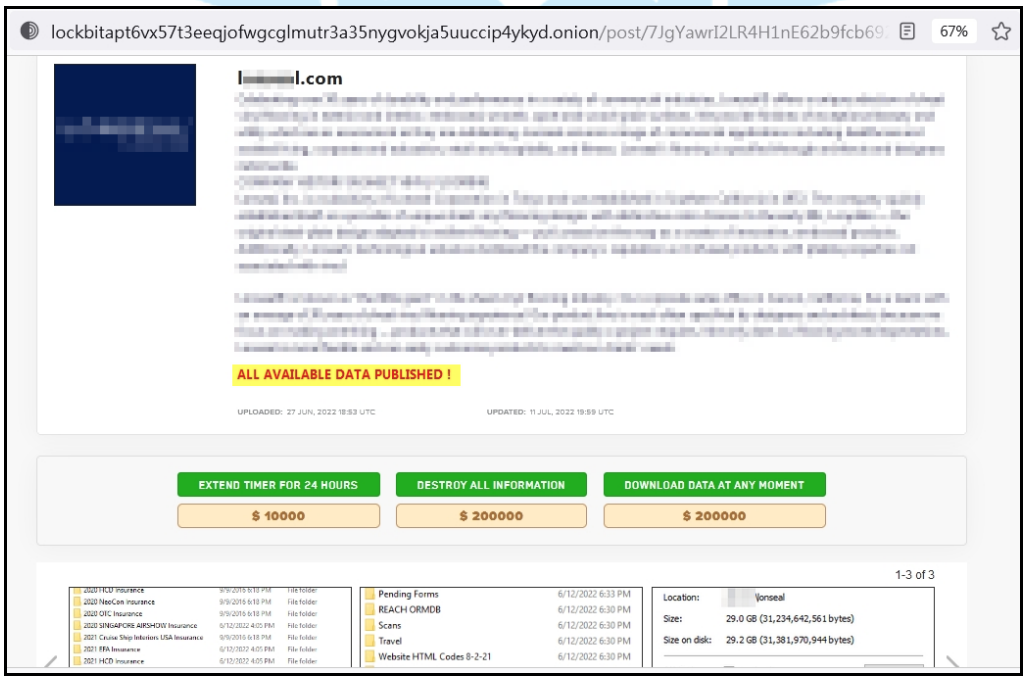




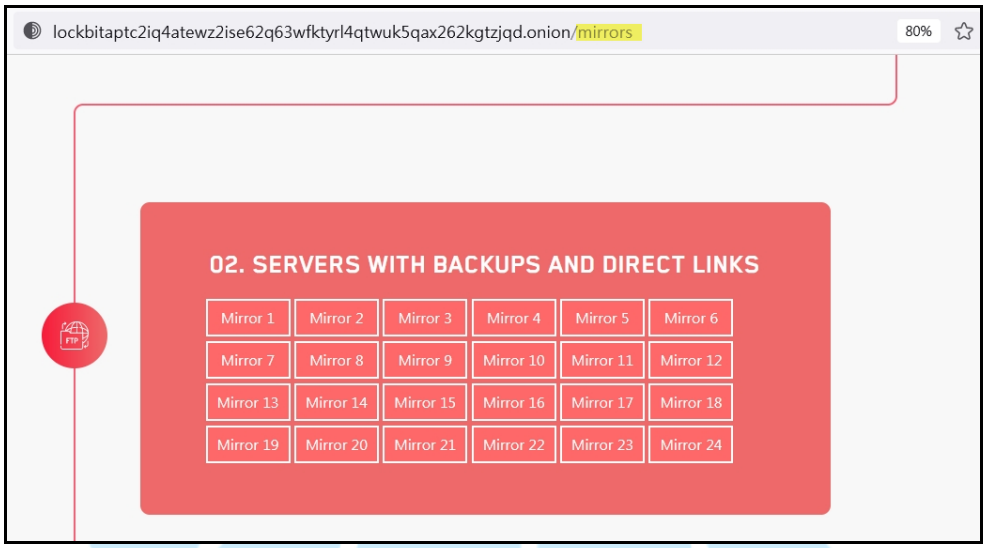
14. 當受害組織給付贖金期限已過後，將會以 PUBLISHED(已發佈)標示於 LockBit BLOG 上。



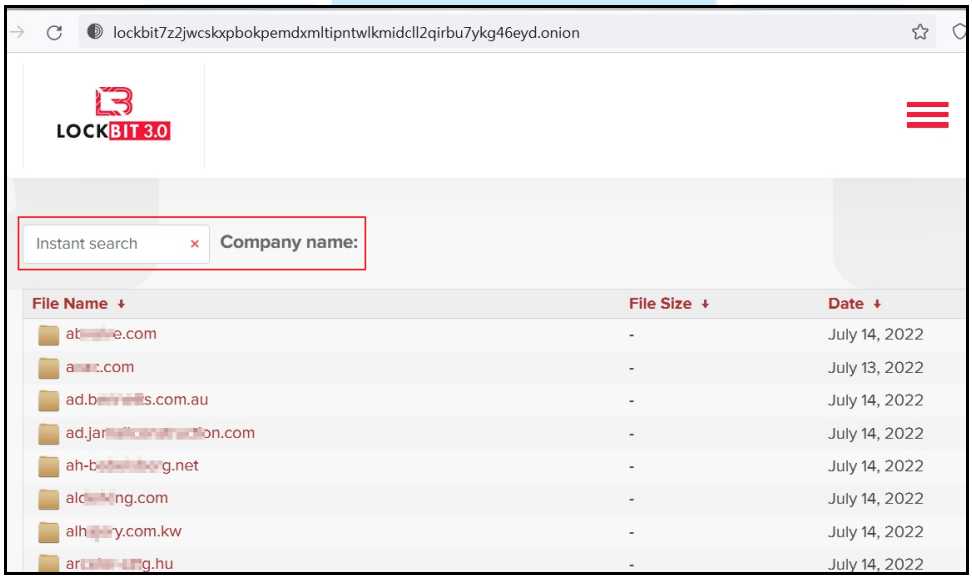
15. 在 LockBit BLOG 上瀏覽某個已到期的受害組織資訊，可看到駭客將受害組織資料標示為 PUBLISHED，並於該網站上公開發佈所竊取的資料。



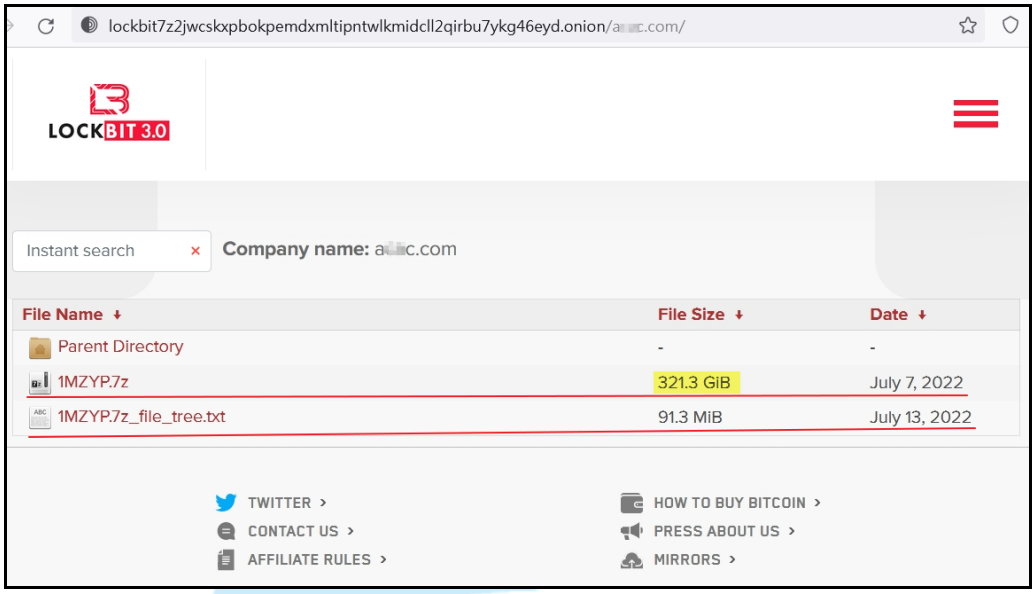
16. 在 LockBit BLOG 上點選 Mirrors 後可看到分成三個部分的內容，分別為 BLOG MIRRORS、SERVERS WITH BACKUPS AND DIRECT LINKS 與 CHATS RESERVE MIRRORS。



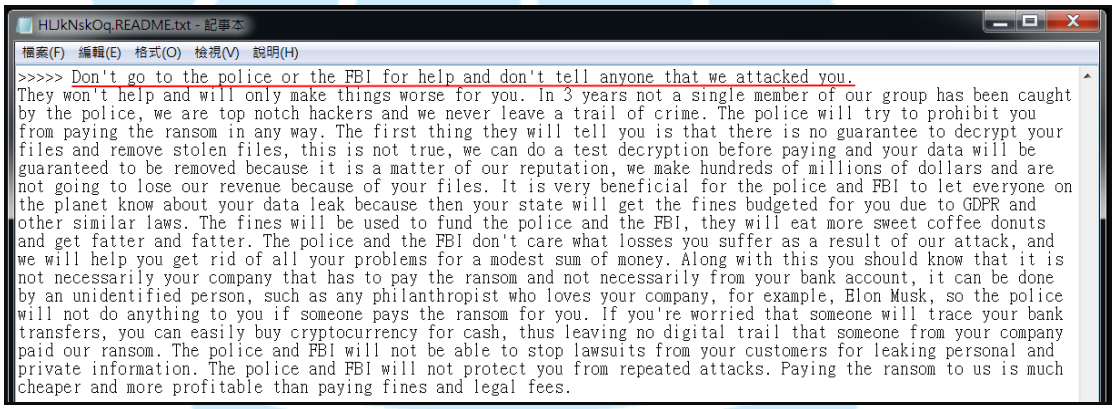
17. 在 02. SERVERS WITH BACKUPS AND DIRECT LINKS 內容，選擇任一個 Mirror 點選進入後，會看到可用公司名稱來搜尋受害組織資訊。這種在網站新增搜尋功能的方式，將便利其他網路犯罪者找尋可下手的目標。



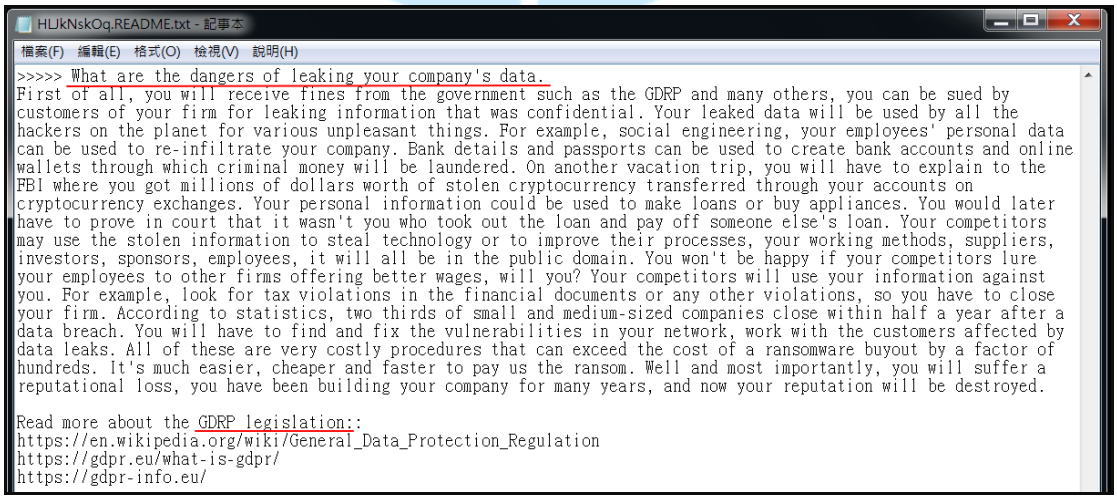
點選某個受害組織名稱後，可看到該組織已被駭客公開發佈的資料，並且可免費下載這些資料。



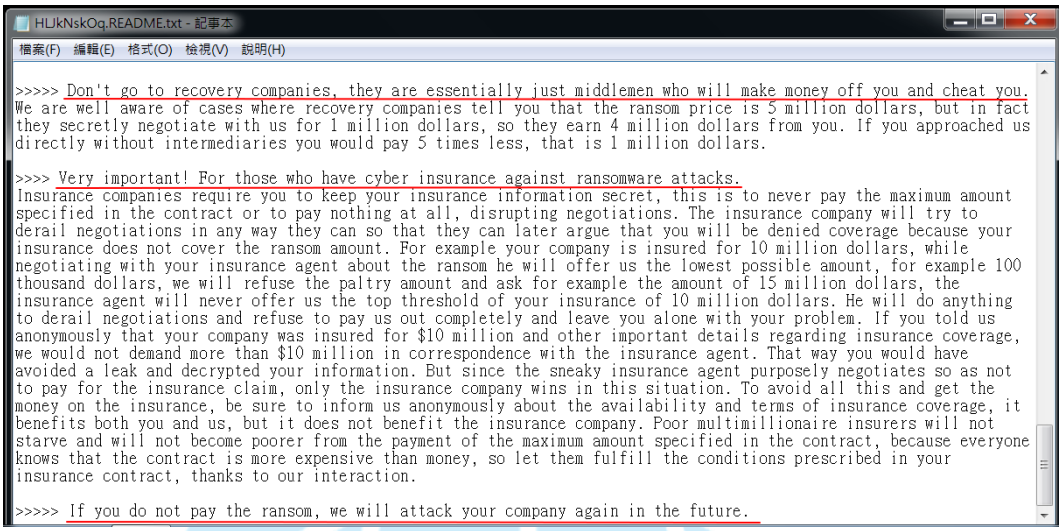
18. 在勒索通知信 HLJkNskOq.README.txt 中，駭客警告受害者不要要求警察或 FBI 幫忙，也不要告訴任何人你受到 LockBit 攻擊。



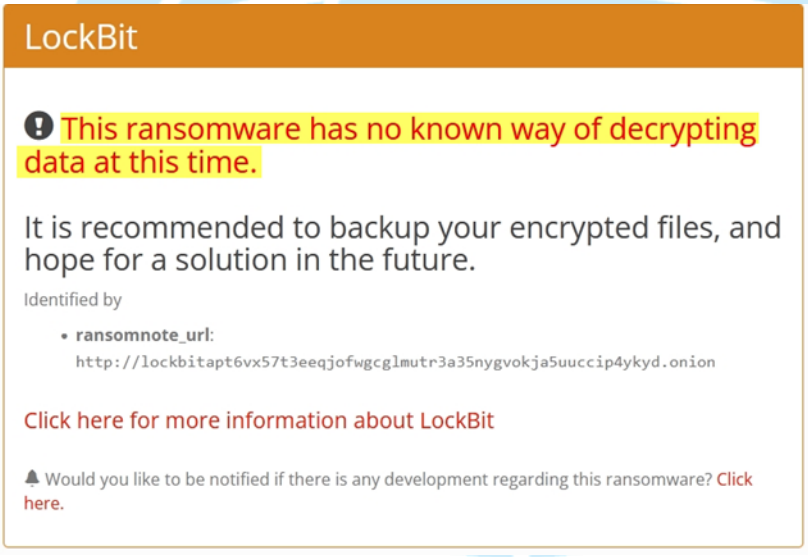
駭客告訴受害者你公司的資料被洩漏後會產生什麼危險，例如:會有來自政府的罰款。



駭客也警告不要找資料復原公司，因為他們只想賺你的錢並且騙你。最後警告受害者如果不付錢，在未來就會攻擊你的公司。

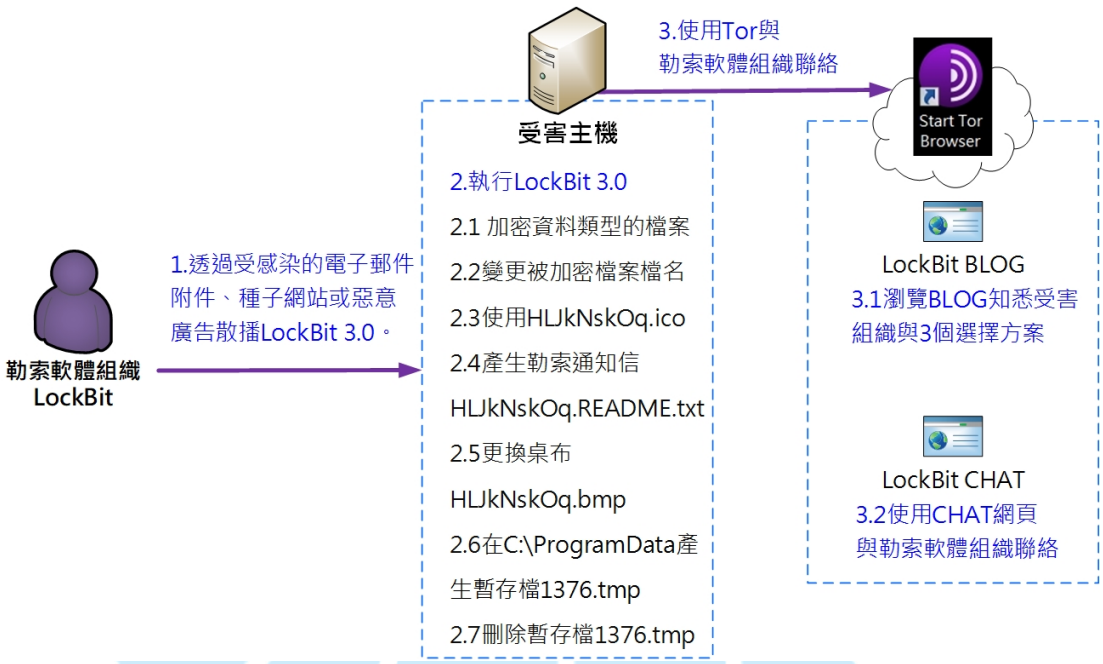


19. 將勒索通知信與被加密檔案送至 ID Ransomware 勒索軟體識別網站檢測，確認其目前尚未有解密器。



20. 該樣本首次被上傳至 Virustotal 檢測日為 2022-07-03 20:20:43 UTC，為很新的樣本。Virustotal 檢測其惡意比例為 56/69。

三、 攻擊行為



1. 勒索軟體組織 LockBit 透過受感染的電子郵件附件、種子網站或惡意廣告來散播勒索軟體 LockBit 3.0。
2. 受害主機感染 LockBit 3.0 後執行下列各步驟:

   2.1 加密資料類型的檔案。

   2.2 變更被加密檔案檔名。

   2.3 使用 HLJkNskOq.ico。

   2.4 產生勒索通知信 HLJkNskOq.README.txt。

   2.5 更換桌布 HLJkNskOq.bmp。

   2.6 在 C:\ProgramData 產生暫存檔 1376.tmp。

   2.7 刪除暫存檔 1376.tmp。

3. 受害者可使用 Tor 與勒索軟體組織聯絡。

   3.1 在 LockBit BLOG 可瀏覽 BLOG 知悉受害組織資訊與 3 個選擇方案。

   3.2 在 LockBit CHAT 可使用 CHAT 網頁與勒索軟體組織聯絡。

四、 總結與建議

1. 本案檢測時發現 LockBit 3.0 僅加密資料類型之檔案、修改檔案名稱、更改桌面桌布，並在桌面上放置一個名為 HLJkNskOq.README.txt 的勒索通知信。它將被加密檔案之檔案名稱及其擴展名稱替換為隨機動態與靜態字串([random_string].HLJkNskOq)。
2. LockBit 3.0 採用雙重勒索的策略，使用 Tor 在其專屬暗網 BLOG 上宣布新的受害組織與提供搜尋功能。在 BLOG 上公告即將要發佈的受害組織資料，造成受害者無形的壓力。又提供 CHAT 網頁作為受害者聯絡 LockBit 勒索團體的管道。這些做法加強雙重勒索的實現，與以往勒索軟體攻擊手法不同。
3. LockBit 透過受感染之電子郵件附件、種子網站或惡意廣告散播，故預防其方法為定期備份資料，不隨意開啟或瀏覽不明來源之惡意檔案或網站。
4. 若感染 LockBit，因尚無解密器，建議可將被加密檔案留存，以待未來有解密器時解密。
5. 對於 LockBit 所竊取資料的安全性防護，建議對於重要或機敏資料以輸入密碼存取方式保存，以防資料遭竊後被讀取。