# 賽門鐵克安全摘要--2021年6月

## 勒索軟體：我們還需要多說嗎？

貝絲・斯塔克波爾
記者

**追回大部分勒索軟體的贖金。**在一系列新的勒索軟體攻擊中，我們終於聽到了一些好消息：支付給犯罪企業的勒索軟體贖金罕見地追回了大部分。

在網路犯罪分子上個月入侵了它的 IT 網路後，美國司法部追回了向駭客支付大部分加密貨幣贖金，該攻擊導致東岸大部分的燃料運輸癱瘓。這家大型管道營運商負責美國東岸多達45%的燃料供應，因攻擊事件而暫停所有管道作業長達 11 天，導致天然氣短缺和價格上漲，並證實已向 DarkSide 勒索軟體集團支付了 440 萬美元的比特幣。DarkSide 以勒索軟體即服務模式在東歐運營，並聲稱它與政治及任何民族國家無關。

根據美國司法部副部長麗莎・摩納哥 (Lisa Monaco) 的說法，聯邦調查局從殖民管道營運商(Colonial Pipeline)最初支付的大約 75 個比特幣中追回了 63.7 個。調查人員經由多個比特幣位址跟踪贖金支付，在獲得DarkSide 的一個比特幣錢包的私鑰或密碼後，追回了大部分贖金，儘管沒有具體的策略。恢復行動是拜登政府最近成立的勒索軟體和數位勒索專案小組的第一次。「勒索軟體攻擊是不可接受的，但當它們針對關鍵基礎設施時，我們將不遺餘力地做出回應」摩納哥說。美國司法部還表示，它計劃將反勒索軟體工作與用於恐怖主義的同一組協議進行協調。

據報導，DarkSide 已經收取了超過 9000 萬美元的比特幣贖金。但奇怪的是，該組織在 5 月份無法存取服務器並且其加密貨幣被轉移到一個未知的錢包時，本身就成了受害者。《華盛頓郵報》報導稱，美國政府並不是DarkSide運營中斷的幕後黑手。

> 在一系列新的勒索軟體攻擊中，我們終於聽到了一些好消息：支付給犯罪企業的勒索軟體罕見地追回了。

**知名目標**。殖民管道營運商(Colonial Pipeline) 並不是最新一波勒索軟體攻擊的唯一目標。 主要肉類生產商 JBS 也遭受了勒索軟體攻擊，影響了北美和澳大利亞的 IT 系統，促使其關閉工廠並提醒客戶和供應商注意可能的交易延遲。在一份聲明中，聯邦調查局將 JBS 攻擊歸咎於 REvil 勒索軟體集團（又名 Leafroller 和 Sodinokbi），並「承諾將努力將威脅行為者繩之以法」。它還強調了私營部門夥伴關係在確保對日益增多的網路入侵做出快速反應方面的重要性。

與此同時，JBS 報告稱在解決打擊其北美和澳大利亞業務的攻擊方面取得了「重大進展」。

與俄羅斯有關聯的 REvil 因入侵台灣硬體供應商廣達電腦而受到指責，並在過去發布了廣達電腦所握有的機密蘋果裝置藍圖。現在，該組織似乎正在升級，據稱該勒索軟體集團的代表威脅要加倍關注美國目標。在發佈到俄羅斯 OSINT Telegram 頻道的一次採訪中，自被刪除後，這

位據稱的發言人陳述了這些主張，同時還聲稱該組織並不害怕被視為恐怖組織。針對美國的行動，REvil 發言人表示，「既然不再迴避美國的目標，我們已經取消了所有限制。從現在開始，這個國家的每個實體都可以成為攻擊目標。」

**全球烽火連天**。不僅僅是美國在與不斷上升的勒索軟體威脅搏鬥。日本企業集團富士軟片在 6 月初意識到勒索軟體攻擊後，不得不關閉其部分網路。該公司表示，已與各個全球據點協調，採取權宜措施暫停所有受影響的系統，並正在努力評估問題的程度和規模。富士軟片沒有具體說明攻擊背後的勒索軟體組織，但 BleepingComputer 報導稱，Advanced Intel 執行長 Vitali Kremez 表示，截至 2021 年 5 月 15 日，該公司似乎感染了 Qbot 惡意軟體。 Kremez 稱，Qbot 與 REvil 勒索軟體組織合作。

**其他隨機的勒索軟體新聞還包括**：經營前往馬薩諸塞州瑪莎葡萄園島和楠塔基特島的渡輪的輪船管理局遭到襲擊。該公司表示，該事件影響了其 IT 系統，而不是其雷達或 GPS 功能，因此其車隊的安全並未受到威脅。目前還沒有關於誰對這次攻擊負責的消息，雖然服務沒有中斷，但票務系統受到了影響。

> 不僅僅是美國在與不斷上升的勒索軟體威脅作拚搏。

**網際網路中斷**。當許多大型知名網站本月稍早時，短暫離線時——亞馬遜、Reddit 和紐約時報，僅舉幾例——下意識的反應是另一次網路攻擊，這次是 Fastly，它運營著一個內容交付網路 (CDN) . Fastly 在短時間內恢復了服務，將問題歸因於由有效的客戶配置更改觸發的軟體錯誤。該公司現在正試圖弄清楚為什麼在測試過程中沒有出現這個錯誤。

**網路釣魚已大不如前**。微軟警告稱，俄羅斯所支持的駭客組織 Nobelium 在駭入美國國際開發總署 (USAID) 的電子郵件行銷平台 Constant Contact 並取得使用帳戶的控制權後，能夠發送看上去很正常的網路釣魚電子郵件，正在策劃一場網路釣魚活動。網路釣魚活動的目標是與政府機構、智囊團、顧問和非政府組織相關的大約 3,000 個帳戶，並且大部分出現在美國。後門可能是一系列惡意活動的媒介，從資料竊取到感染網路上的其他電腦。

就跟勒索軟體一樣，網路釣魚也應該採取必要的防禦及示警機制。Barracuda Networks 的一份最新報告發現，躲過防禦機制的網路釣魚電子郵件平均會在員工的收件匣保存三天以上，好消息是：只有 3% 的員工在收到網路釣魚電子郵件時會打開惡意附件或點擊鏈接。

面對網路安全威脅的風暴，很高興知道我們正在取得一些進展。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/feature-stories/symantec-security-summary-june-2021

## 關於作者

**貝絲・斯塔克波爾**
記者

貝絲・斯塔克波爾是一位在商業與技術交叉領域擁有 20 多年經驗的資深記者。她為大多數領先的 IT 行業出版物和網站撰寫文章，並為一系列領先的技術提供商製作定制內容。

**更多資訊 請造訪我們的網站 http://www.SaveTime.com.tw**
**(好記：幫您節省時間.的公司.在台灣)**

**關於保安資訊：**

**從協助顧客簡單使用賽門鐵克方案開始，到滿足顧客需求更超越顧客期望的價值。**

- 保安資訊被業界公認為最專業的賽門鐵克解決方案的專家。
- 保安資訊的團隊自 1995 年起就專注於賽門鐵克資訊安全解決方案的銷售、規劃與整合、技術支援、教育訓練、顧問服務，特別是提供企業 IT 專業人員的技能傳承(Knowledge Transfer)的效益上，以及比原廠更快速的技術支援回應，深獲許多中大型企業與組織的青睞(特別是有 IT Team 的組織)，長期合作的意願與滿意度極高。
- 與許多系統整合或服務公司不同的是，我們不吝惜分享我們的專業技能與經驗給顧客的 IT Team，經由常態性的教育訓練、精簡的快速手冊、標準 SOP 文件的提供，以及基於比原廠更孰悉顧客的使用環境與現況的快速回應的品質，在業界建立扎實的口碑。
- 保安資訊一直專注於賽門鐵克領先業界的資訊系統基礎架構上的安全性與可用性的解決方案。進而累積了許多與基礎架構整合的成功經驗，讓導入 Symantec 解決方方案的成效非常卓越。我們的顧客都能免除Try & Error 的時間浪費及不確定的投入或自行摸索的運作風險。
- 關於我們：

**保安資訊有限公司**
**http://www.savetime.com.tw**
**0800-381500、0936-285588**