近在眼前的威脅

2019 年網路犯罪經濟規模達到 1.28 萬億美元，2020 年全球的網路犯罪激增 400%

■文：徐俊毅

回顧 2020 年的資安威脅記錄就會發現，它的影響範圍絲毫不比 COVID-19 差到哪裡去。而且資安問題帶來的網路犯罪甚至直接利用了人們對新冠疫情焦慮和對自身健康的擔憂，同時針對醫療和健康相關設施的攻擊大幅度激增。

來自世界經濟論壇《2020 全球風險報告》指出，2019 年網路犯罪經濟規模達到 1.28 萬億美元，2020 年全球的網路犯罪激增 400%，經濟規模的資料只會更加驚人。

2020 年重大資安事件

利用 COVID-19 進行釣魚

這可能是是 2020 年最具時間特性的網路釣魚攻擊，比如在美國，駭客們利用人們對新冠病毒的焦慮，冒充 CDC 專家或者病毒學家，誘使用戶下載惡意文件，不僅騙取大量重要個人資料，而且還感染很多其他計算設備。除了計算設備，來自 Palo Alto Networks 公司的報告顯示，全美多達 83% 的醫療成像設備存在安全隱患，可能被網路攻擊者利用。2020 年的醫療系統，不僅要承受新冠病毒帶來的壓力，還要同時應對來自互聯網的各種麻煩。

2020 年屢被“勒索”攻擊的工業和製造業

統計顯示，2020 年前三季度全球勒索軟體攻擊同比激增 40%！作為一種全球性的威脅，勒索軟體已經成為全球第四大犯罪活動，無論是個人還是企業、政府都面臨被勒索的巨大風險。製造業方面，本田、佳能、富士康、研華等大廠先後遭到勒索軟體攻擊，而索要的贖金也一再創下新高。

- 2020 年 2 月，歐洲最大的天然氣和電力公司 EDP 遭遇了軟體攻擊，被勒索 1000 萬歐元。
- 2020 年 4 月，以色列供水部門工控設施遭網路攻擊，事涉危險化學品。
- 2020 年 5 月，臺灣兩大油企。臺灣石油和台塑石化遭到攻擊，造成一些加油站無法正常交易。
- 2020 年 5 月 5 日，委內瑞拉國家電網遭到攻擊，全國 765 條供電骨幹大面積停電，同時發生的還有國外雇傭兵入侵事件。
- 2020 年 5 月，瑞士鐵路機車製造商 Stadler 遭遇勒索。
- 2020 年 6 月，本田汽車收到 EKans 勒索軟體攻擊，一度影響全球運營和生產。
- 2020 年 10 月，澳大利亞航運和物流公司 Toll 第二次遭遇勒索。
- 2020 年 10 月中旬以來，臺灣先後有 10 家上市櫃公司遭遇駭客組織的勒索。富士康美洲廠、研華、仁寶先後遭遇巨額勒索，有些已經支付巨額贖金。

實際上，整個 2020 年，全球各地每個月都有很多關於被攻擊和遭遇勒索的新聞，以至於更大量的被攻擊和勒索事件已經不能成為新聞了。

全球首例勒索軟體致死案

2020 年 9 月 10 日，德國的杜賽爾多付大學醫院遭到勒索軟體攻擊。攻擊者透過醫院商用軟體的漏洞，感染了醫院的 30 台伺服器，結果造成醫院各系統先後癱瘓，醫院無法正常運轉。

此時一名正在等待急救的病人被迫送往 32 公里外的另外一家醫院，但由於錯過了搶救時間，不幸身亡。當地檢查官隨後以過失殺人罪立案調查，目前案件仍然在偵辦當中。

這名不幸的患者成為全球首例，因勒索軟體而死的人。

臺灣 2000 萬人的個人資訊出現在暗網

2020 年 6 月，一家名為 Cyble 的資安機構發文稱，在暗網出售的一份大小為 3.5GB 的資料庫中，發現了全臺灣 2000 多萬人的個人資訊，包括了個人的全名、郵政地址、電話號碼、身份 ID、性別以及出生日期等等。根據分析，資料很可能來自“內政部家庭登記部”或者是“臺灣房屋登記資料庫”。儘管此後不久，暗網商店已經刪除了這項商品，但資料是洩露程度仍然未知。

50 多家科技公司的原始程式碼洩露

包括 Adobe、微軟、AMD、Qualcomm、MTK、GE、賓士、任天堂等 50 多家公司的原始程式碼出現在 gitlab 網站的公開存儲庫中。一些公司發現，可能是開發系統工具錯誤的配置，導致了原始程式碼被暴露在公共網路上，從而造成代碼洩露。

8 月份，外電報導，Intel 公司至少有 20GB 的機密資料被攻擊者獲取。這些資料不僅包括處理器、晶片組、固件的硬體資料，而且還有大量軟體及開發工具的原始程式碼。有業內人士稱，其中一些資料對競爭對手或者其他有志於處理器或相關 IC 的公司來說相當有吸引力。

微軟的 Windows XP 和 Windows Server 2003 原始程式碼，也在 9 月份出現在互聯網上。如此衆多的公司原始程式碼短時間內相繼外泄，也是不多見的事情。

比“永恆之藍”更具破壞性的漏洞

如果對永恆之藍這個名字不熟，那麼他的後代勒索病毒如今已經“名滿天下”，駭客們正是針對微軟系統的這個漏洞加以利用，創造出了一個勒索軟體家族，並於 2017 年 5 月“一戰成名”，全球大量企業、機構被迫支付贖金才能解密被非法加密的重要資料，到今天他們依然十分猖獗。而永恆之藍正是 NSA 發現並加以利用的微軟系統漏洞。2020 年 1 月，NSA 又發現一個可能更為嚴重的漏洞並提交給微軟，微軟已經在第一時間發佈

補丁程式，希望不會成為下一代的勒索病毒的母體。

安全性漏洞數量再創新高 Android 漏洞翻倍

2020 年 NVD 漏洞資料庫總計新增了 19220 個漏洞，連續第四年創新高，由於遠端辦公數量激增，針對遠端辦公協議漏洞的攻擊屢創新高，2020 年前 11 個月的資料就是去年同期的 3 倍之多。手機更加頻繁地出現在工作生活中，因此針對 Android 系統的攻擊也呈現爆發式增長，光漏洞數量就增長了 3 倍。

年終的“大禮”SolarWinds 供應鏈式攻擊

就在剛剛過去的 12 月，一場針對 SolarWinds 的供應鏈攻擊讓包括美國白宮、五角大樓、財政部、美國國家核安全局等重要部門遭到入侵。除了重要的政府部門，包括電力、石油以及製造業、高科技公司也紛紛中招，CISCO、Microsoft、Intel、NVIDIA 也未能倖免，CISA (美國網路安全與基礎設施安全局 2018 年 10 月成立) 宣稱：這一事件是美國關鍵基礎設施迄今為止面對的最為嚴峻的網路安全危機。

攻擊者在 SolarWinds Orion 商務軟體更新包中植入惡意程式碼，進行分發，這一惡意程式碼被植入後，具備包含傳輸檔、執行檔、分析系統、重啓機器和禁用系統服務的能力，從而到達橫向移動和資料盜竊的目的。

不斷演進的攻擊和層出不窮的手段

來自 Microsoft 的安全資訊報告顯示，如今全球每天有超過 8 萬億個與資安相關的信號在互聯網中傳遞。Verizon 的報告顯示，2020 年全球資料洩露事件多達 15.7 萬多起，其中超過 7 成來自外部入侵，而 2018 年和 2019 年的資料加在一起不過 9 萬多起。不僅攻擊頻率大幅度增加，而且攻擊得手的數量也在上升。IBM 的 2020 年度資料洩露成本報告也指出，發生資料洩露的平均成本已經高達 386 萬美元 / 次。

就像其他產業一樣，網路犯罪也在不斷演進並升級，這點很多機構的報告都有提及。他們的工具越來越先進，動作越來越快，攻擊規模越來越大，攻擊頻率越來越高，甚至出現了公司化和品牌化的趨勢。比如 GandCrab 團隊製作的勒索軟體，透過買給勒索者，已經賺得 20 億美元。

除了利用各式漏洞，使用黑市 (主要是暗網) 上出售的各種“品牌”工具，攻擊手段也層出不窮。

透過 Thunderbolt 介面攻擊電腦

2020 年 5 月，荷蘭的一名研究人員發現，經過一些操作，攻擊者可以透過 Thunderbolt 介面，利用 DMA (直接記憶體存取) 的漏洞攻擊電腦。這名研究人員已經在 youtube 發佈了自己的演示視頻。他使用一種專門的軟體和 SPI 編碼器，透過修改固件來騙取系統的信任，從而獲得系統控制權。所幸不是所有筆電設備都有這樣的漏洞，而且完成攻擊需要一定的條件。

利用風扇電腦設備的散熱風扇傳遞資料

同樣是在 2020 年，以色列的一個研究團隊發現並嘗試攻擊那些未暴露在公共網路電腦的一個方法。

他們在電腦中植入軟體控制風扇轉速，產生特定的聲波，然後再用對應頻段的聲音接收裝置讀取到傳遞過來的資料，只是這種方式傳遞資料的速度很慢。但這種方式的厲害之處是，即便那些沒有暴露在公共網路的電腦，也存在了被竊取資料的可能。同樣，這種方式也有很大局限性，比如風扇要支持調速，要安裝一個特定軟體，收發裝置不能距離太遠，資料傳輸速度很慢等等。

威脅行為複雜度更高也更難發現

從時間線來看，進入 2020 年下半年，無論是勒索還是攻擊行為，針對的物件已經擴展至大型企業、科技公司甚至是一些要害部門，攻擊者的能力和效率都在快速提升，Microsoft 發佈的最新版《數字防禦報告》指出：在過去一年裡，威脅行為者的複雜程度迅速提高，使用的技術使他們更難發現，甚至威脅到最精明的目標，重大事件不斷出現就是例證。人們發現原來資安威脅離我們如此之近。CTA