賽門鐵克安全摘要--2021年4月

網路攻擊的複雜性、勒索軟體和隨時保持警惕

貝絲・斯塔克波爾
記者

嚴陣以待。多年來，專家們一直在大聲疾呼，但如果上個月有任何跡象的話，隨著進階網路攻擊和事件的數量、類型和復雜性不斷升級，企業面臨著更加多樣化和持續的威脅格局。

讓我們從韌體方面開始，它已被確定為一個駭客入侵企業日益覬覦的標的。根據 2021 年 3 月的安全信號研究，超過 80% 的企業在過去兩年中至少經歷過一次韌體攻擊。意想不到的：不到三分之一 (29%) 的安全預算用於保護韌體，21% 的受訪者表示他們的韌體不受監控，這讓大多數公司完全暴露在風險之中。這項研究顯示目前企業安全投資重點包括安全升級、弱點掃瞄、進階安全防護（advanced threat protection，ATP）--當然，這些都是關鍵投資。但調查顯示，韌體更新一直被忽視，這可能是由於缺乏安全意識和自動化更新的機制所致。

韌體攻擊很受攻擊者歡迎，因為它們是電腦核心的底層，可以擷取更有價值的敏感資料（包括憑証和加密密鑰）。常見的檢測產品和通用日誌工具也無法窺探韌體，漏洞允許攻擊者即使在計算機被擦除後仍留在計算機上，使其進一步受到關注。

> 韌體攻擊很受攻擊者歡迎，因為它們是電腦核心的底層，可以擷取更有價值的敏感資料（包括憑証和加密密鑰）

接下來，還有勒索軟體的問題 -- 企業安全團隊的另一個持續惡化的問題。網路犯罪分子賺的錢和勒索的錢比以往任何時候都多。**2020 年，勒索軟體的平均支付額飆升了 171%**，飆升至 312,000 美元。但請注意：從 2019 年到 2020 年，組織支付的最高贖金翻了一番，從 500 萬美元躍升至 1000 萬美元。

勒索軟體對 COVID-19 新冠疫情的衝擊，更是不容忽視。勒索軟體運營商正利用疫情爆發所帶來巨大變化來掠奪製造、醫療保健和建築行業，特別是醫療保健業更是他們眼中的大肥羊。

在今年的所有勒索軟體攻擊中，Ryuk 變種脫穎而出。2020 年 10 月，聯邦調查局、美國國土安全部網路安全暨基礎設施安全局(CISA)以及美國衛生與公眾服務部門(HHS)聯合發布了一份網路安全諮詢報告，特別指出 Ryuk 攻擊對醫療保健組織構成威脅。

傳統企業應用程式也不能倖免於步步進的逼網路攻擊活動。一份新的威脅情資報告發現，未安裝修補程式的 SAP 系統中的重大漏洞正在為全球網路攻擊者提供一個「充滿目標對象」的環境。在 2020 年 6 月至 2021 年 3 月期間，至少跟踪了 1,500 次與 SAP 應用程式相關的攻擊嘗試，並且有證據顯示超過 300 次自動化漏洞利用，利用了七個特定於 SAP 的攻擊媒介和來自各種威脅媒介的 100 多次手動鍵盤入侵(hands-on-keyboard)連線。這些攻擊利用了影響 ERP、CRM 和供應鏈系統的安全漏洞，其中最嚴重的漏洞涉及 CVSS 10（稱為 RECON），這是 SAP NetWeaver/

Java 中的一個可遠端利用的漏洞，由身份驗證檢查失敗所引起。

儘管 SAP 有一個每月的程式修補週期，但企業仍處於被鎖定的目標；問題在於，大多數客戶不會馬上進行修補，而是在發布後的幾個月內（在某些情況下，甚至幾年內，甚至從來沒有修補過）才會套用應用已發布的修復程式。因此，攻擊者有足夠的時間利用未修補的漏洞--研究發現，漏洞利用嘗試發生在修補發布後的短短 72 小時內；在雲端服務的 IaaS 環境中配置的未受保護的 SAP 應用程式只需短短三個小時就可能被攻破。

> 一份新的威脅情資報告發現，未安裝修補程式的 SAP 系統中的重大漏洞正在為全球網路攻擊者提供一個「充滿目標對象」的環境。

這種漏洞利用可以導致對不安全的 SAP 應用程式的完全控制，使攻擊者能夠竊取敏感資料、破壞關鍵業務流程、啟動勒索軟體或實施金融欺詐。鑑於 SAP 產品組合用於關鍵任務業務的範圍和滲透率，攻擊還可能危及 SOX、GDPR 和其他法規的遵循性。該威脅足以讓網路安全和基礎設施安全局 (CISA)根據該報告發出警報。

在個別但有些相關的新聞中，聯邦機構敦促使用 Microsoft Exchange Server 電子郵件應用程式的私營公司和政府機構立即修補他們的系統，以防止不法分子利用新發現的漏洞。在微軟宣布 Exchange 被至少一個中國國家資助的駭客組織入侵後不久，這些新漏洞就被發現了，這可能會影響數千個組織。

甚至連技術支援也正在成為網路安全攻擊的媒介。Vade Secure 指的是 3 月份發起的大規模假冒電子郵件活動，該活動試圖用領先的防毒軟體廠商的虛假賬單電子郵件來吸引企業。這些技術支持詐騙者冒充 Microsoft、McAfee 和 Norton，向公司發送虛假的防毒軟體續訂通知，稱收件人將被收取高達 399 美元的三年訂閱費用，除非他們撥打某個電話號碼取消訂閱。一旦他們這樣做，詐騙者就會試圖引誘他們安裝遠端存取軟體，該軟體會成為惡意軟體的載體。Vade Secure 表示，它已經過濾了超過 100 萬封針對其客戶群的電子郵件。

鑑於大多數公司的網路安全態勢，新興的威脅形勢尤其令人擔憂。事實上，根據安侯建業(KPMG)全球總部日前針對全球年收入超過 5 億美元企業的 500 名CEO進行安侯建業 2021 年 CEO 展望脈搏調查，將網路安全風險列為組織未來三年增長的第一大威脅，近五分之一的 CEO 受訪者表示。去年，它在榜單上排名第五，有 10% 的 CEO 表示它對其組織的發展構成威脅。

更深入的研究來自 Varonis 的一份最新報告發現，醫療保健公司嚴重缺乏對資料安全的正確認知與實踐：擁有 500 個或更多帳戶的公司，有高達 77% 的公司沒有實施強制定期變更密碼的政策、用戶數和服務帳戶超過 1,000 個的組織有高達 79% 的公司，有帳號沒有人使用卻還是啟用的狀態。另一份報告發現，即使是接受過網路安全培訓的員工，當被要求進行有關該主題的基本測驗時，也未能通過。根據趨勢科技發布的一份報告，越來越多的製造商（現在是網路犯罪分子和民族國家團體的首要目標）經歷了一次事件 (61%)，其中四分之三的情況下生產線停工。

儘管網路安全意識和準備工作有所提高，但仍有大量工作要做。

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