在勒索軟體開始攻擊之前斷其後路

2024 年 3 月 14 日發布｜產品洞察

Esther Seguin
端點潛在顧客行銷
、賽門鐵克端點安全

賽門鐵克的「調適型防護--Adaptive Protection」防護技術讓攻擊者吃閉門羹

勒索軟體犯罪集團越來越多地使用合法軟體實施攻擊。事實上，賽門鐵克最近對過去三年 (2021-2023年) 勒索軟體攻擊的分析顯示，有證據顯示，近 50% 的勒索軟體攻擊使用「就地取材 (LOTL：Living-off-the-Land)」工具 (即預裝的合法軟體)。隨著越來越多的勒索軟體攻擊成為頭條新聞，傳統的安全方法顯然招架無力，無法有效對抗這些隱匿的攻擊者。

企業戰略集團 (ESG) 首席分析師戴夫--格魯伯 (Dave Gruber) 在一份新的白皮書《端點安全的進展》中寫道：「超過一半的安全領導者 (52%) 向 ESG 報告說，由於攻擊面不斷擴大和變化，加上威脅形勢瞬息萬變，安全運營比兩年前更具挑戰性。這其中包括使用『就地取材 (LOTL)』的情形增加。」

隨著越來越多的攻擊者利用合法軟體在網路中立足和橫向移動，防禦者顯然需要採取不同的安全方法。

為何就地取材 (LOTL) 攻擊是持續且迫切的問題

就地取材 (LOTL) 攻擊與兩用工具型態的攻擊之所以如此／非常成功，一個原因是企業不想禁用合法軟體。由於這些攻擊的性質，調查人員可用於檢測入侵的感染指標 (IOC) 等數位佐證資料也較少。事實上，美國網路安全暨基礎設施安全局 (ybersecurity and Infrastructure Security Agency，以下簡稱 CISA) 在其最近的報告《識別與緩解離就地取材攻擊手段》中也強調要特別注意這一安全挑戰：『目前普遍缺乏與就地取材 (LOTL) 攻擊活動相關的常規入侵指標 (IOCs)，這使得網路防禦者識別、跟蹤和分類惡意行為的工作變得更加複雜。

此外，格魯伯 (Gruber) 在新白皮書：《端點安全的進展--Advances in Endpoint Security》中寫道：「每家企業的情況各不相同，使用就地取材 (LOTL) 工具的方式也不盡相同，不同業務部門使用的就地取材 (LOTL) 工具往往也不一樣，因此，一體適用的安全方法是不夠的」。儘管在過去 10 年中，端點安全解決方案的功能得到大幅擴展，但大多數解決方案仍然依賴於監控攻擊模式和應對這些活動的模式。這種被動應對的方法忽視了受保護設備不斷變化的運行特性和動態變化。

進入賽門鐵克「調適型防護--Adaptive Protection」。賽門鐵克「調適型防護--Adaptive Protection」一大優勢是，您不需要 IOC 就能抵禦就地取材 (LOTL) 和相關攻擊。賽門鐵克會分析這些攻擊中經常使用的工具和應用程式，而自「調適型防護--Adaptive Protection」則會持續分析各個用戶的操作環境。憑藉這些工具在企業中使用一年歷史記錄，自我調整防護功能可以只阻止不合法使用的工具。這就避免誤攔的風險，同時阻止這些工具的惡意使用--切斷了攻擊者目前正在使用的路徑 (斷其後路)。

在撰寫本文時，「調適型防護--Adaptive Protection」系統正在對 54 種就地取材 (LOTL) 工具和應用程式中的 469 種特定行為進行跟蹤。隨著新攻擊方法的出現，賽門鐵克全球情報網路 (GIN) 會向「調適型防護--Adaptive Protection」回饋新資料，以保持與時俱進。

瞭解攻擊者如何發動就地取材 (LOTL) 攻擊

在我們的新報告《2024 年勒索軟體威脅形勢》詳細介紹勒索軟體攻擊者是如何避開採用惡意軟體來實施勒索軟體攻擊，轉而採用就地取材 (LOTL) 工具。雖然 PowerShell、WMI 和 Vssadmin 是最經常被採用的就地取材 (LOTL) 工具，但許多其他預先已經安裝的合法工具也常涉入勒索軟體攻擊。您還可以在 ESG 的新白皮書：《端點安全的進展--Advances in Endpoint Security》中找到這些工具的列表。

隨著威脅環境 (包括勒索軟體攻擊) 的不斷變化，我們會持續創新，致力幫助我們的客戶在資安威脅的競爭中保持領先。請務必記住，勒索軟體攻擊的短期和長期影響遠遠大過贖金損失。現在是採取新方法防範這些狡詐的攻擊的時候了。我們邀請您參加我們即將舉辦的網路研討會，瞭解有關賽門鐵克「調適型防護--Adaptive Protection」的更多資訊，並學習如何顯著降低就地取材 (LOTL) 攻擊的風險。

關於作者

Esther Seguin

端點潛在顧客行銷、賽門鐵克端點安全

Esther 為賽門鐵克端點安全客戶提供有關當今不斷演變的威脅以及透過端點安全解決方案應對這些威脅的方法的見解。20 多年來，她一直致力於幫助企業瞭解和應對組織中的風險。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/product-insights/shut-door-ransomware-it-gets-started
本文件由保安資訊有限公司專業細心整理後提供。如有遺誤、更新或異動均以上Symantec原廠公告為準，請知悉。2024/3

關於賽門鐵克 (Symantec)

賽門鐵克 (Symantec) 已於 2019/11 併入全球網通晶片巨擘--博通 (BroadCom，美國股市代號 AVGO，全世界網際網路流量有 99.9% 經過博通的網通晶片) 軟體事業部的企業安全部門 (SED)，特別是近年以半導體的嚴謹、系統化以及零錯誤思維來改造核心技術、管理框架以及整合最完整的資安生態體系，讓賽門鐵克的解決方案在穩定性、相容性、有效性以及資安生態系整合擴充性，有著脫胎換骨並超越業界的長足進步。博通 (Broadcom) 是務實的完美主義者，致力於追求卓越、關注細節並且有系統和紀律地投入科技創新與嚴謹工藝，同時也大大降低交易複雜性。Symantec 持續創新的技術能為日新月異的資安問題提供更好的解決方案，近三年 Symantec 很少出現在由公關機制產生的頭版文章中，而且在全球前兩千大企業的市佔率及營收成長均遠遠高於併入博通之前，增長幅度也領先其他競爭對手，是科技創新驅動的解決方案非常穩健可靠深受大型企業信賴的實證，也顯示大型企業顧客對轉型中的新賽門鐵克未來充滿信心。(美籍華人王嘉廉創辦的企業軟體公司，組合國際電腦（CA Technologies）以及雲端運算及「硬體虛擬化」的領導廠商--VMware， 也是博通軟體事業部的成員)。2021 年八月，因應國外發動的針對性攻擊日益嚴重，美國網路安全暨基礎架構安全管理署（CISA）宣布聯合民間科技公司，發展全國性聯合防禦計畫 JCDC(Joint Cyber Defense Collaborative)，而博通賽門鐵克是首輪被徵招的一線廠商，如就地緣政治考量，Symantec 也絕對是最安全的資安廠商。擁有更強大資源與技術為後盾的賽門鐵克已更專注於整合各種最新科技於既有領先業界的端點、郵件、網頁以及身分認證等安全解決方案。

關於保安資訊 www.savetime.com.tw

保安資訊團隊是台灣第一家專注在賽門鐵克解決方案的技術型領導廠商，被業界公認為賽門鐵克解決方案專家。自 1995 年起就全心全力於賽門鐵克資訊安全解決方案的技術支援、銷售、規劃與整合、教育訓練、顧問服務，特別是提供企業 IT 專業人員的知識傳承 (Knowledge Transfer)、協助顧客符合邏輯地解決資安問題本質的效益上，以及基於比原廠更孰悉用戶環境的優勢能提供更快速有效的技術支援回應，深獲許多中大型企業與組織的信賴，長期合作的意願與滿意度極高。保安資訊連絡電話：**0800-381-500**。