保安資訊有限公司--賽門鐵克解決方案專家--原廠防護亮點分享

SEP的網路層防護技術--IPS有效防護RDP攻擊

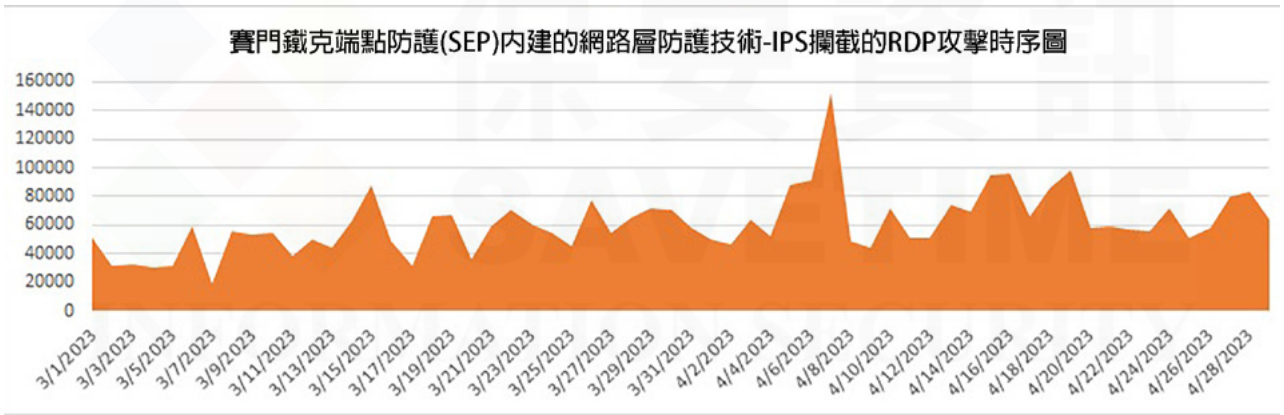
2023 年 5 月 1 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

遠端桌面通訊協定 (Remote Desktop Protocol-RDP) 是 Microsoft Windows 的一項功能，可提供遠端存取。遠端工作人員使用它連接到實際位於其辦公室的電腦，而 IT 專家可以使用它來修復來自世界各地的使用者的電腦。它在 COVID-19 疫情爆發之前就已經很流行，但自從疫情爆發後，大量企業員工突然需要居家辦公，RDP 連線的使用呈指數性成長。不幸的是，它對那些懷有惡意的人來說同樣方便，並且駭客不斷進行 RDP 攻擊以存取和入侵企業網路。

RDP 攻擊是一種網路攻擊，它試圖使用 RDP 協議存取遠端電腦。這些攻擊是駭客利用不安全系統、面向公眾網路的暴險服務和易受攻擊的網路端點一種非常熱門手法。成功的 RDP 攻擊可能允許攻擊者獲取憑證、執行惡意程式碼，甚至讓他們完全控制目標系統。

賽門鐵克每週攔截超過數十萬次 RDP 攻擊。



令人擔憂的是，RDP 攻擊正越來越被網路犯罪分子和國家級駭客用來發動勒索軟體攻擊。透過 RDP 存取受害者的電腦，攻擊者可以安裝勒索軟體來加密受害者的檔案並要求支付解密密鑰的費用。

攻擊者使用多種工具和伎倆來發動 RDP 攻擊：

* 掃描工具：攻擊者可能會使用掃描工具來搜索連接到網際網路且容易受到攻擊的 RDP 伺服器。這些工具可以幫助攻擊者識別 RDP 攻擊的潛在目標。
* 暴力破解工具：暴力破解工具用於透過多種不同的組合來試圖破解密碼，直到找到正確的組合。攻擊者可以使用這些工具來嘗試存取受弱密碼或易猜密碼狀態的 RDP 連接。
* 漏洞利用工具包：這些是用於識別和利用軟體漏洞的工具和漏洞利用的軟體包。一些漏洞利用工具包專門針對 RDP 漏洞而設計。
* 憑證竊取惡意軟體：攻擊者可能會使用目的在從受害者電腦竊取登錄憑證的惡意軟體。這種類型的惡意軟體可用於竊取 RDP 登錄憑證及儲存在受害者電腦上的其他登錄憑證。
* 社交工程：攻擊者可能會使用網路釣魚電子郵件等社交工程伎倆來誘騙受害者洩露其登錄憑證或下載可用於執行 RDP 攻擊的惡意軟體。

RDP 攻擊構成重大威脅，個人和組織都應認真對待。使用強密碼、雙因素身份驗證和其他安全措施確保 RDP 連接得到適當保護非常重要。

賽門鐵克經長時間證實的 RDP 攻擊的**零時差**保護，效益卓越，端點防護內建的網路層防護技術-IPS 可偵測最新攻擊如下：

網路層的攔截定義檔：

我們的 Webpulse (網頁脈衝) 網頁自動回饋框架以及其他先進的網路層防護技術，已將其列為如下分類的網頁型攻擊：

- Attack: NCrack Tool RDP BruteForce Activity
- OS Attack: Microsoft Windows Remote Desktop Services RCE CVE-2019-0708*
- OS Attack: RDP Scan Attempt 2
- Web Attack: Microsoft RDP Exploit Attempt
- Attack: Microsoft RDP CVE-2012-0002 4
- System Infected: GoldBrute RDP BruteForce Attempt

* 這表示同一個名稱涵蓋多個相似的攻擊偵測能力。

欲瞭解更多有關於賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲瞭解更多有關賽門鐵克端點安全安全完整版更多資訊，請點擊此處。

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**。