攻擊者正在如何取得您的網路控制權

2021 年 11 月 4 日發布｜專家觀點

威脅獵手團隊
賽門鐵克

賽門鐵克幫助您為您和您的客戶捍衛網路邊界

阻止攻擊者進入組織總比一旦他們進入組織就被抓住更可取。因為解決問題的成本遠遠高於預防的成本。不用說，防護勝於偵測。有效的防護需要了解攻擊者如何試圖進入內部。但是攻擊媒介受歡迎度忽高忽地。了解當前趨勢至關重要。

攻擊者如何存取組織網路的問題是每個網路攻擊的受害者都希望獲得解答。但是，通常很難確定攻擊者究竟是如何獲得對受感染網路的初始存取權限的。作為博通的企業安全部門，賽門鐵克將繼續積極監控攻擊者用來保護我們客戶組織和網路安全的感染媒介。最近的發現已發表在一份新的白皮書中。

本文的一些主要發現包括：

- 在過去 18 個月中，**利用**公開服務公眾的應用程式中的漏洞是一種熱門的攻擊媒介。雖然零時差漏洞，特別是 Microsoft Exchange Server 的漏洞，仍在被攻擊者利用，但攻擊者試圖利用主要還是已知的漏洞。即使這些漏洞早有可用的修補程式，它們也可能沒有足夠快地修補以避免攻擊。有更多的證據表明，只要漏洞一經公諸於世，攻擊者就會開始利用漏洞。
- **殭屍網路**近來已成為勒索軟體集團的主要威脅傳播網，Trickbot、Dridex 和 IcedID 等主要殭屍網路現在都與勒索軟體行動相關聯。然而，其他殭屍網路也仍在積極傳播加密挖礦惡意軟體，並被用於進行分散式阻斷服務 (DDoS) 攻擊，在最近越來越關注勒索軟體中不應忘記此類殭屍網路帶來的威脅。
- 根據賽門鐵克的資料，網路犯罪分子**對「漏洞刺探攻擊套件：exploit kit」的使用**似乎正在減少，其中一個漏洞刺探攻擊套件：RIG 在過去 18 個月中獨占鰲頭。然而，最近漏洞刺探攻擊套件在網路犯罪分子中的熱門程度似乎有所下降，並不意味著它們不會捲土重來，它們仍然是組織需要注意和防範的媒介。
- **電子郵件**仍然是一個持續流行的攻擊媒介。社交工程是許多利用電子郵件進行騙局的關鍵要素，尤其是商務電子郵件入侵 (business email compromise：BEC) 詐騙，它仍然是網路犯罪領域代價最高的詐騙之一。我們還看到了一些惡意行動者利用社交媒體進行電子郵件詐騙的例子--在 LinkedIn 或 Twitter 等平台上進行初步接觸，最終利用電子郵件向目標發送威脅。有目標式勒索軟體攻擊者也使用電子郵件作為遞送方式。
- **COVID-19** 疫情大爆發在過去18個月內也帶來影響，並被利用作為許多網路釣魚行動的誘餌。

- **展望未來**，一種可能在未來幾年產生影響的新威脅是「企業內部人員」。一些勒索軟體集團鎖定可能願意與他們合作的目標攻擊對象之內部人員做宣傳，一旦讓他們存取他們有權存取的公司網路，這些集團會為那些願意與他們合作的企業內部人員提供豐厚的回報。雖然我們還沒有看到涉及內部人員的針對性勒索軟體目標攻擊，但勒索軟體集團公開採用這種戰術的事實意味著組織和防御者需要意識到這一點。

有關更多資訊，請在此處閱讀新白皮書。

關於作者

威脅獵手團隊
賽門鐵克

威脅獵手 (Threat Hunter) 團隊是賽門鐵克內部的一群安全專家，其任務是調查有針對性的攻擊，推動賽門鐵克產品的增強保護，並提供分析以幫助客戶應對攻擊。

原廠網址：https://symantec-enterprise-blogs.security.com/blogs/expert-perspectives/how-attackers-gain-access-your-networks
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。2021/11

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