Symantec

INTERNET SECURITY THREAT REPORT

執行摘要

2019 年網路安全威脅研究報告

ISTR

第 24 期

執行摘要

表單點擊劫持、目標式攻擊、自給自足攻擊，您的公司正面臨威脅。

如同蒼蠅撲向蜂蜜，不法之徒群起採用最新刺探利用手法，能以極少成本迅速獲利；勒索軟體和挖礦綁架已不再流行，現在是表單點擊劫持的天下。

我們將在第 24 期賽門鐵克網路安全威脅研究報告中，針對全球威脅活動、網路犯罪趨勢和攻擊者動機，分享最新見解。

這份報告使用的分析資料來自賽門鐵克全球智慧型網路 (Global Intelligence Network)，這是全球最大的民間威脅情報網路，記錄來自全球 1.23 億個攻擊偵測器的事件，每日攔截 1.42 億個威脅，並監控超過 157 個國家的威脅活動。

{FORMJACKING}

表單點擊劫持

網路罪犯透過表單點擊劫持快速致富

表單點擊劫持攻擊操作簡單又能帶來獲利：網路罪犯將惡意程式碼置入零售商的網站中，竊取消費者的信用卡詳細資料，平均每個月有 4,800 多個獨立網站遭受入侵。

知名企業 (Ticketmaster 和 British Airways) 與中小型企業均遭受攻擊，去年保守估計為不肖份子帶來數千萬美元的獲利。

每張信用卡在地下交易論壇最高可售得 45 美元，因此只要在每個受入侵的網站竊取 10 張信用卡，即可帶來每月高達 220 萬美元的獲利。單單 British Airways 攻擊事件就有超過 38 萬張信用卡遭竊，歹徒所得淨利可能超過 1,700 萬美元。

RANSOMWARE

勒索軟體

CRYPTOJACKING

挖礦綁架

沉寂，但未消失

勒索軟體和挖礦綁架一度是網路罪犯的必備生財工具，然而 2018 年間獲得的利潤降低，犯罪活動也跟著減少。

自 2013 年以來，勒索軟體犯罪活動首次下降，整體降低 20%，但針對企業的犯罪活動卻上升 12%。

2018 年加密貨幣價值崩跌 90%，挖礦綁架活動也跟著減少 52%；然而，由於入門門檻低且負載最少，挖礦綁架依舊盛行，賽門鐵克在 2018 年成功封鎖的挖礦綁架攻擊是前一年的四倍。

TARGETED ATTACKS

目標式攻擊

目標式攻擊偏好破壞手段

供應鏈攻擊和「自給自足」(LotL) 攻擊現已成為網路犯罪的主要手法：2018 年的供應鏈攻擊激增 78%。

自給自足技巧讓攻擊者可以隱身在合法程序之中，例如，惡意 PowerShell 程序檔的使用率在去年增加 1,000%。

賽門鐵克每個月攔截 115,000 個惡意 PowerShell 程序檔，但這個數字只佔整體 PowerShell 使用量的不到 1%。使用強力手段阻止所有 PowerShell 活動會導致業務中斷，這也是為什麼 LotL 技術會受到眾多目標式攻擊集團青睞，因為這種策略可讓他們躲避偵測。

MORE AMBITIOUS
野心更大

AND STEALTHIER
更為隱匿

攻擊者也越來越常使用魚叉式網路釣魚等經實測證明的可靠方法，來滲透到企業裡。雖然情報收集仍然是攻擊者的主要目的，但有些集團也著眼於製造破壞，現在幾乎每十個目標式攻擊集團中，就有一個使用惡意軟體來破壞或中斷業務營運，活動量自去年以來增加 25%。

Shamoon 便是一個鮮明的例子，在沉寂兩年之後，這種病毒又在中東地區大張旗鼓捲土重來，在目標組織的電腦中部署會清除磁碟的惡意軟體，藉此刪除檔案。

CLOUD
雲端

雲端上的挑戰：雲端資料是否安全，掌握在您手中

只要有一項雲端工作負載或儲存實例設定錯誤，組織可能就須為此付出數百萬元的代價，或是陷入合規問題的夢魘之中。在 2018 年，有超過 7,000 萬筆記錄從設定不當的 S3 儲存貯體中遭竊取或洩漏。網路上的現成工具可讓攻擊者找出設定不當的雲端資源，

入侵者利用 Meltdown、Spectre 和 Foreshadow 等硬體晶片漏洞，侵入託管在同一個實體伺服器上的雲端服務，以存取公司受保護的記憶體空間，成功的攻擊行動讓攻擊者得以進入平常禁止存取的記憶體位置。

對於雲端服務來說這個問題特別嚴重，因為雲端實例雖然有自己的虛擬處理器，卻共享記憶體群組，這表示只要一個實體系統遭成功侵入，就可能導致數個雲端實例的資料外洩。

IoT

您愛用的 IoT 裝置是攻擊者的最佳目標

雖然受感染的裝置中有 90% 為路由器和連網的攝影機，但是包括小型燈泡和語音助理在內，幾乎每項 IoT 裝置都容易遭受攻擊。

目標式攻擊集團越來越常將焦點擺在 IoT，視其為容易攻破的進入點，透過這些進入點，他們可以破壞或清除裝置，竊取憑證和資料，以及攔截 SCADA 通訊。

此外，隨著 Thrip 和 Triton 等威脅集團投入到營運和工業控制系統的滲透攻擊，工業 IT 已然成為網路戰爭的潛在戰場。

ELECTION INTERFERENCE 2018

2018 年選舉干擾

是否有操縱選舉的訊息出現在您的社交媒體上？

2018 年美國期中選舉在眾人的關注下，所幸並未發生重大干擾事件。然而，社交媒體仍然會是極度活躍的戰場。

假冒成合法政治網站的惡意網域遭查獲並關站時，與俄羅斯相關聯的帳號會透過第三方來購買社交媒體廣告，供其所用。

社交媒體公司已採取更積極的態度，打擊干擾選舉的行為，Facebook 成立了戰情室來對抗選舉干擾；Twitter 也移除 10,000 多個 Bot 傀儡程式，這些程式會張貼呼籲大眾不要投票的訊息。

取得詳細資訊。下載賽門鐵克 2019 年網路安全威脅研究報告 (ISTR)
https://symc.ly/APISTR

關於賽門鐵克

賽門鐵克公司 (NASDAQ：SYMC)是世界首屈一指的網路安全公司，無論資料位在何處，賽門鐵克皆可協助企業、政府和個人確保他們最重要資料的安全。全球各地的企業均利用賽門鐵克的策略性整合式解決方案，在端點、雲端和基礎架構中有效地抵禦最複雜的攻擊。同樣地，全球各地超過 5,000 萬的人們和家庭社群，也仰賴賽門鐵克的諾頓產品和 LifeLock 產品套裝軟體來保護自身的居家數位生活及各種裝置。賽門鐵克經營的安全情報網是全球規模最大的民間情報網路之一，因此能成功偵測最進階的威脅，進而提供完善的防護措施。若想瞭解更多資訊，請造訪 www.symantec.com.tw。

台灣賽門鐵克股份有限公司
地址：台北市信義區忠孝東路 5 段 68 號 29 樓

電話：+886 2 8729 9277
傳真：+886 2 8729 9257

如需任何分公司和聯絡電話的相關資訊，請造訪我們的網站。美國地區客戶如需產品資訊，請洽免付費電話 1 (800) 745 6054。

www.symantec.com.tw

ISTR