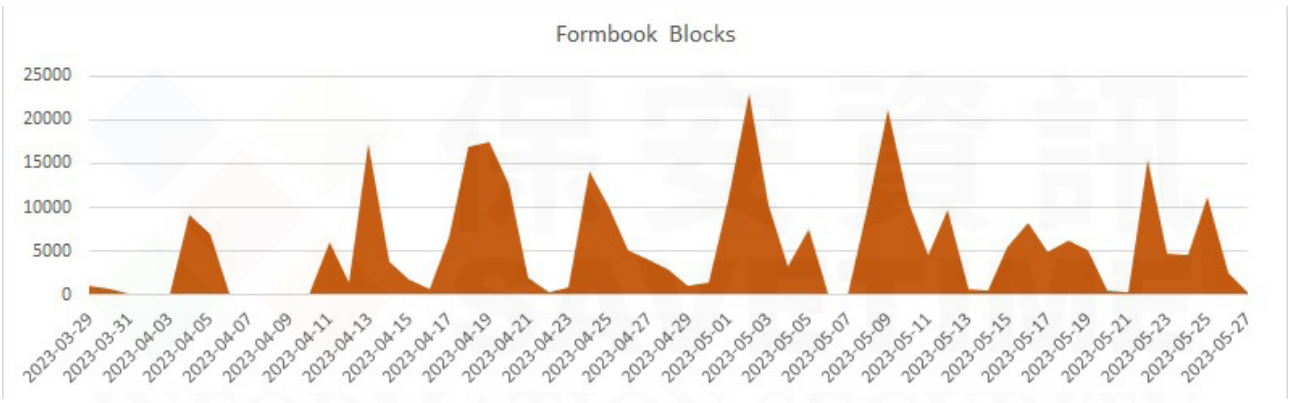
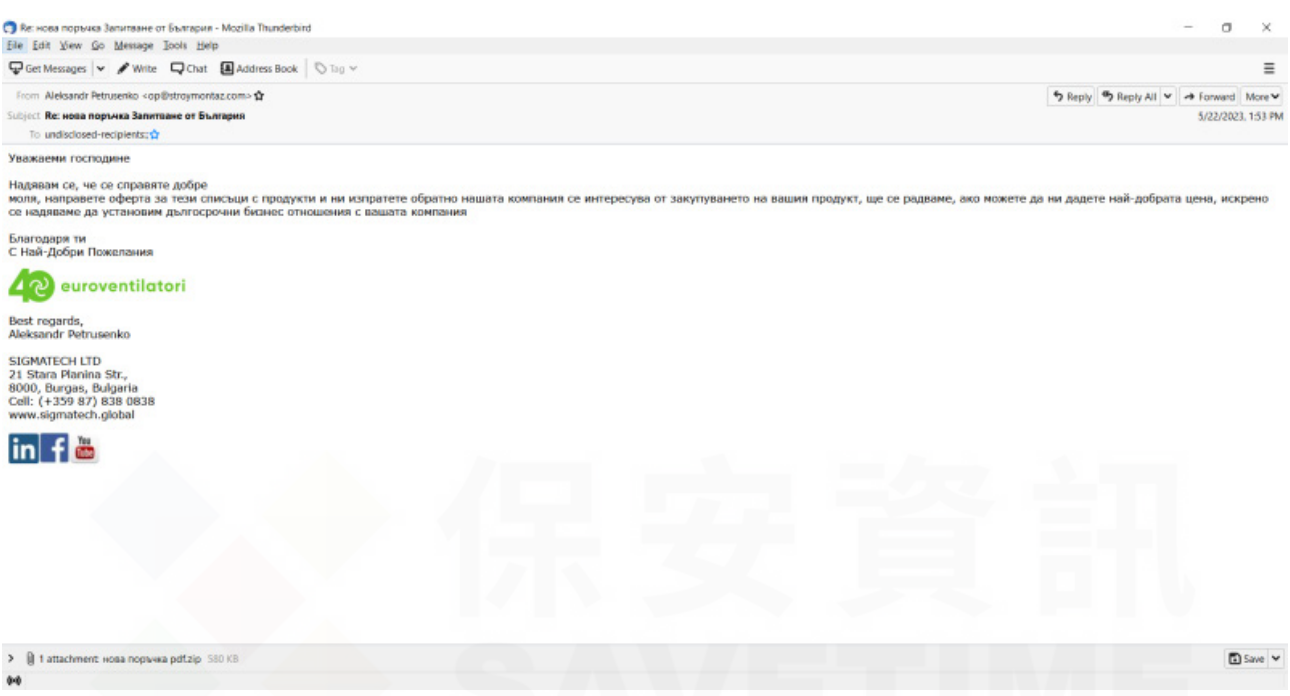
Formbook 被機器學習了

2023 年 5 月 29 日發布

更精準地來談，我們自動化機器學習能力能隨時與時俱進有效遏止 Formbook。我們在 2022 年 12 月 8 日的公告 P9 中詳細討論 Formbook，而現在正是重新來討論並更新資訊的好時機。簡要回顧一下，自 2016 年左右以來，Formbook 一直被用來從遭駭入的電腦中竊取資訊，利用電子郵件作為主要感染媒介，並使用各種主旨，包括常見的假訂單、出貨明細、對帳單與發票和SWIFT外匯轉帳。主要目的是從網頁瀏覽器竊取憑證、收集螢幕截圖和按鍵側錄。以惡意軟體即服務 (MaaS) 的形式出售，針對全球多個國家、地區的各行各業發動目標式和亂槍打鳥式的攻擊行動。很頻繁，至少可以這麼說。真的很頻繁。



這是一封典型 Formbook 電子郵件的範例，這封保加利亞語的郵件包含一個附件，其檔名以狡猾的“pdf.zip”為結尾。寄件人的電子郵件位址與寄件人簽名中的公司名稱和網站完全不同，這顯然就是一個警訊。



在此具體的範例中，zip 壓縮檔包含一個可執行檔，該檔案已使用 .NET 加殼程序進行嚴重混淆。執行後，它將自己複製到“%AppData%\Roaming\fLgUSgFvp.exe”，並將自己排除在 Windows Defender 的掃描中，為自己新增排程，最後解密實際有效籌載，將 Formbook 4.1 版注入以下 Windows 應用程式：“C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe”。

在去年 12 月的防護公告中，報告說明當時 Formbook 攻擊行動，已被我們郵件安全雲端服務 (ESS) 的惡意軟體掃描元件主動攔截，後續發起相關新攻擊行動也是如此，我們客戶完全不受影響。包含機器學習在內的多層次先進防護技術，百分之百有效攔阻 Formbook，但為了證明機器學習的有效性，我們很高興地在本公告中展示，從去年 12 月以來所有攻擊行動，證明無需更新就能完整檢測與攔截 Formbook 的底層邏輯。

賽門鐵克已經於第一時間提供多種有效保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email.Security.cloud**/**DCS**/**EDR**)。以下說明為 Symantec **零時差**防護技術偵測到的惡意程式名稱及有效對應的防護機制：

檔案型(基於回應式樣本的病毒定義檔)防護：

- MSIL.Packed31
- Scr.Malcode!gdn32
- Scr.Malcode!gdn34

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.B!100
- Heur.AdvML.B!200

郵件安全防護機制：

不管是地端自建 (SMG／SMSEX) 的郵件過濾／安全閘道及主機防護、雲端郵件安全服務 (E-mail Security.Cloud) 以及郵件威脅隔離 (ETI)，都能提供終端用戶隔絕或隔離威脅於境外的保護(威脅不落地)。

欲深入瞭解賽門鐵克端點防護 (SEP) 的進階機器學習防護技術，請點擊此處。
欲瞭解更多有關於賽門鐵克郵件安全雲端服務(Email Security.Cloud)的詳細資訊，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**。