保安資訊--本周(台灣時間2025/09/12)
賽門鐵克原廠防護公告重點說明

前 言

賽門鐵克原廠首要任務就是保護我們的顧客，被譽為賽門鐵克解決方案專家的保安資訊更能發揮我們被高度認可的專業知識與技能、豐富經驗以及專為幫助客戶成功的服務熱忱，與顧客共同創造賽門鐵克解決方案的最大效益，並落實最佳實務的安全防護。攻擊者從不休息，我們更不會。一支技術精湛且敬業的團隊不斷創造新的防護措施，以應對每天發布成千上萬的新威脅。儘管不可能詳述我們已經可以防禦的每種新威脅，但該站點至少反映了我們的努力。這些公告分享針對當前熱門新聞話題有關威脅的保護更新，確保您已知道自己受到最佳的保護。點擊此處獲取賽門鐵克原廠防護公告 (Protection Bulletins)。

關於 保安資訊有限公司 | 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。

在端點啟用賽門鐵克入侵預防系統(IPS) 的好處(以下皆為美國時間)

賽門鐵克的入侵預防系統 (IPS) 是業界一流的深層封包檢測技術引擎，可保護包括財富 500 強企業和消費者在內的數億個端點(桌機／筆電／伺服主機)。

過去的 7 天內，SEP 的網路層保護引擎 (IPS) 在受保護端點上總共阻止了 6,700 萬次攻擊。這些攻擊中有 87.2% 在感染階段前就被有效阻止：**(2025/09/03)**

- 在受保護端點上，阻止了**2,940**萬次嘗試掃描**Web**伺服器的漏洞。
- 在受保護端點上，阻止了**510**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**Windows**伺服主機上，阻止了**480**萬次攻擊。
- 在受保護端點上，阻止了**310**萬次嘗試掃描伺服器漏洞。
- 在受保護端點上，阻止了**200**萬次嘗試掃描在**CMS**漏洞。
- 在受保護端點上，阻止了**250**萬次嘗試利用的應用程式漏洞。
- 在受保護端點上，阻止了**97**萬**1,600**次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在受保護端點上，阻止了**56**萬**9,500**次加密貨幣挖礦攻擊。
- 在受保護端點上，阻止了**810**萬台次向惡意軟體**C&C**連線的嘗試。
- 在受保護端點上，阻止了**8**萬**6,400**次加密勒索嘗試。

強烈建議用戶在桌機／筆電／伺服主機上啟用 IPS (不要只把SEP/SES當一般的掃毒工具用，它有多個超強的主被動安全引擎，在安全配置正確下，駭客會知難而退)，以獲得最佳保護。點擊此處獲取有關啟用 IPS 的說明，或與保安資訊聯繫可獲得最快最有效的協助。

有憑有據!SEP的瀏覽器延伸防護功能，在上周所帶來的好處？

賽門鐵克的入侵預防系統 (IPS) 是業界最佳的深度資料包檢測引擎，可保護數億個端點(桌上型電腦和伺服器)，其中包括財富 500 強企業和消費者。

賽門鐵克端點安全 (SES) 或賽門鐵克端點防護 (SEP) 代理透過谷歌 Chrome 瀏覽器和微軟 Edge 瀏覽器的延伸供瀏覽器保護。這些延伸有兩個組成部分：

- 瀏覽器的入侵預防，利用 IPS 引擎保護客戶免受各種威脅的侵害。
- 網頁信譽，可識別可能包含惡意軟體、欺詐、網路釣魚和垃圾郵件等惡意內容的網域和網頁帶來的威脅，並阻止瀏覽這些網頁。

在過去 7 天內，賽門鐵克透過端點防護的瀏覽器延伸防護功能，在受保護端點上阻止了總計 1,330 萬次攻擊。**(2025/09/03)**

- 使用網頁信譽情資，在端點上阻止了 **12M** 次攻擊。
- 在受保護端點上攔截 **1.1M** 次攻擊，這些攻擊試圖將用戶重定向到攻擊者控制的網站上。
- 在受保護端點上攔截 **147.2K** 次瀏覽器通知詐騙攻擊／技術支援詐騙攻擊／加密劫持嘗試。
- 在受保護端點上攔截 **7.7K** 次攻擊，這些攻擊利用被入侵操控網站上的惡意腳本注入。

建議客戶啟用端點防護 (SEP) 的瀏覽器延伸，以獲得最佳防護。按下此處獲取：整合瀏覽器延伸和 Symantec Endpoint Protection (SEP)，防止惡意網站的說明。

2025/09/12

新版ZynorRAT遠端存取木馬(RAT)利用Telegram攻擊Linux與Windows系統

Sysdig 威脅研究團隊 (TRT) 發現一種新型 Go 語言編寫的遠端存取木馬 (RAT) --ZynorRAT，其具備針對 Linux 與 Windows 平台的強大指令與控制 (C&C) 功能。值得注意，ZynorRAT 以 Telegram 作為核心 C&C 基礎架構，簡化殭屍網路管理並增進自動化運作。其 Linux 版本為 64 位元 ELF 可執行檔，提供多種惡意功能。其能力包含竊取檔案、列舉系統細節 (例如：IP 位址、主機名稱及使用者名稱)，並能擷取螢幕截圖。為了在遭入侵的 Linux 系統中持續存活，ZynorRAT 運用 systemd 使用者服務確保自身持久存在。此外，該程式支援執行任意指令，使攻擊者能深度掌控受感染機器。此組合特性使 ZynorRAT 成為重大威脅，具備廣泛入侵與竊取資料的能力。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1;

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

- Trojan.Gen.NPE
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/12

Yurei勒索軟體

Yurei 勒索軟體於九月首度現蹤，此新型勒索軟體集團採用雙重勒索模式，同時實施檔案加密與資料竊取。由程式碼分析顯示，Yurei 勒索軟體是微幅修改的開源勒索軟體 Prince。更多技術細節詳見 Check Point Research 發布的報告。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Net!g1
- ACM.Ps-Wbadmin!g1
- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.Ransom!gen107
- SONAR.RansomPlay!gen1
- SONAR.Ransomware!g1
- SONAR.Ransomware!g7
- SONAR.Ransomware!g12
- SONAR.Ransomware!g16
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!g253
- SONAR.SuspLaunch!g307
- SONAR.SuspLaunch!g507
- SONAR.SuspLaunch!gen4

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen.HC
- Ransom.Zombie
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/09/12

免錢永遠最貴～AMOS惡意竊密軟體持續透過破解版應用程式進行傳播

趨勢科技最新報告揭露一項利用 AMOS 惡意竊密軟體 (亦稱 Atomic macOS Stealer) 的複雜攻擊行動。攻擊者運用社交工程手法，將惡意軟體二進位檔偽裝成破解版軟體，或誘使用戶將惡意指令貼入 macOS 終端機，藉此繞過 Gatekeeper 等內建防護機制。該行動透過輪替網域名稱規避偵測並阻礙封鎖行動，大幅提升防禦難度。針對 macOS 平台的 AMOS 惡意軟體專門竊取各類敏感資訊，包含認證憑證、瀏覽器資料、加密貨幣錢包、鑰匙串 (英語：Keychain) 是蘋果公司 Mac OS 中的密碼管理系統及其他重要數據。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- WS.Malware.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/12

Fireant駭客組織持續在緬甸活動，並利用ToneShell後門程式發動攻擊

ToneShell 是一款由 Fireant(又稱 Mustang Panda) 駭客組織部署的後門程式。Intezer 資安研究人員已公布近期觀察到的變種詳情，相關活動顯示該組織持續對緬甸目標發動攻擊。ToneShell 透過 DLL 側載技術執行，將合法執行檔與惡意軟體共同封裝於 ZIP 壓縮檔中。此惡意軟體整合了反規避機制及多種反分析功能，使安全產品更難偵測與防範。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/11

BlackField(又稱BlackFL)勒索軟體

BlackField (又稱 BlackFL) 是一種採用雙重勒索勒戰術的索軟體攻擊者，首次被觀察到活動時間約為 2025 年 7 月。對其勒索軟體的分析顯示，該組織採用典型的雙重勒索模式，同時運用加密手段與竊取數據來向受害者施壓。

遭入侵後，加密檔案會被冠上 .BlackFL 副檔名，並在多個目錄中放置勒索通知文字檔 (BlackField_ReadMe.txt)。該通知告知受害者資料已被加密並竊取，攻擊者威脅若未付款將出售或洩露敏感資訊 (例如：資料庫、原始碼及商業機密)。受害者被要求透過加密即時通訊軟體：qTox 或 Telegram 聯繫攻擊者，並警告延誤將加劇損害程度。

觀察到的技術、流程與程序 (MITRE ATT&CK 的戰術、技術與子技術)：

- 「執行」戰術階段 (TA0002)--排程任務／工作 (T1053)：以系統權限建立名為「Windows Update BETA」的持久化任務。

- 「持久化」戰術階段 (TA0003)--修改登錄檔 (T1112)：變更登錄檔以實現開機自動執行。
- 「權限提升」戰術階段 (TA0004)--利用SYSTEM 層級進行排程任務。
- 「防禦繞過」戰術階段 (TA0005)--採用 UPX 壓縮的混淆／壓縮檔案 (T1027、T1027.002)；透過偽造 DLL 名稱進行偽裝 (T1036)；間接命令執行 (T1202) 透過 cmd.exe 與 schtasks.exe；隱藏痕跡 (T1564.003) 運用隱藏視窗。
- 「發現」階段 (TA0007)--系統資訊發現 (T1082)；透過 .ini 檔案進行檔案與目錄發現 (T1083)。
- 「收集」戰術階段 (TA0009)--透過操作 C:$Recycle.Bin\ 內的檔案進行資料暫存 (T1074)。
- 「危害」戰術階段 (TA0040)--為造成危害而加密資料 (T1486)：冠上 .BlackFL 副檔名並投放勒索說明文字檔 (BlackField_ReadMe.txt)。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Ps-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

基於端點偵測與回應(EDR)：

- 賽門鐵克 EDR 能夠監控和標記該威脅攻擊者的策略、技術和程序(Tactics、Techniques、Procedures，TTPs)。
- 賽門鐵克新增了特定惡意軟體的威脅搜尋查詢，客戶可以在 iCDM 控制台上觸發這些查詢。有關這些查詢的更多訊息，請參閱此 GitHub 儲存庫：https://github.com/Symantec/threathunters/tree/main/Trojan/Remcos

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/09/11

BlackNevas勒索軟體

BlackNevas 勒索軟體，最初於 2024 年 11 月現身。此加密勒索程式鎖定亞洲、北美及歐洲的企業與關鍵基礎設施，尤其集中攻擊亞太地區。該惡意軟體背後的威脅行為者會加密檔案、竊取敏感資料，並威脅公開發佈竊取的資料。與典型勒索軟體即服務 (RaaS) 營運模式不同，BlackNevas 會與資料外洩網站 (DLS) 合作進行公開披露。據南韓的資安公司安博士 (Ahnlab) 研究

人員報告，此勒索軟體採用 AES 對稱式加密與 RSA 非對稱式加密雙重加密演算法，並在被加密檔名後冠上「.encrypted.」字樣。BlackNevas 透過檢查檔案末尾的特定數據值來判斷檔案是否已被加密，而非依賴副檔名。其勒索通知文字檔「how_to_decrypt.txt」指示受害者透過電子郵件或 Telegram 聯繫攻擊者，並威脅若未滿足贖金要求將公開已竊取的機敏資料。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen14
- SONAR.RansomTrigon!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Proton
- Trojan.Gen.6
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

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: Ransom.Gen Activity 47

2025/09/11

兼具惡意挖礦軟體與DDoS攻擊能力的Linux殭屍網路：Luno

資安監控業者 Cyble 研究人員發現一起名為「Luno」新型複雜 Linux 殭屍網路行動。此惡意軟體框架結合惡意挖礦與模組化 DDoS 攻擊能力，展現進階功能，例如：程序偽裝、二進位檔案替換及自我更新機制，顯示有專業威脅行為者的參與。該殭屍網路支援多種可調整參數的 DDoS 攻擊模式，專門鎖定 Roblox、Minecraft 及 Valve 伺服器等熱門遊戲平台，顯示其採用「殭屍網路代客攻擊」模式。儘管尚不清楚其直接歸屬的駭客集團，但已觀察到該威脅行為者透過 Telegram 頻道販售 DDoS 攻擊服務。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE
- WS.Malware.1

2025/09/11

先進、隱蔽又持久～NightshadeC2殭屍網路浮出水面

NightshadeC2 是由資安代管廠商 eSentire 新發現的殭屍網路，其先進的隱蔽與持久技術尤為突出。該惡意軟體透過摻雜木馬的合法軟體安裝程式 (例如：CCleaner、ExpressVPN 等) 進行傳播，同時利用偽造的 ClickFix 主題登陸頁面實施釣魚攻擊。該惡意軟體運用隱身程式碼注入、沙箱規避及「UAC 提示轟炸 (UAC Prompt Bombing)」技術繞過安全防護，同時在 Windows Defender 中新增排除項目以躲避偵測。一旦啟動，NightshadeC2 將賦予攻擊者廣泛的攻擊力，包含反向 shell (Reverse shell)、遠端系統控制、螢幕截取、鍵盤記錄、剪貼簿監控，以及竊取源於 Chromium 與 Gecko 引擎的瀏覽器的憑證與 Cookie。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!g257
- SONAR.SuspStart!gen2

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/10

Kamasers惡意軟體

Kamasers 是一款具有後門功能的機器人程式，最近在真實網路情境上被發現。一旦部署，它會與其 C&C 伺服器通訊以接收指令，進而下載並執行檔案、執行 HTTP 和DNS 洪水攻擊 (DNS flooding)、存取本機檔案、載入惡意 JavaScript 以及將瀏覽器導向到攻擊者指定的網址。

分析顯示，Kamasers 利用與 Telegram、Dropbox 和 GitHub Gist 的額外離埠連接 (可能作為信標機制或後備回報管道) 利用可信任平台來掩蓋惡意活動。

該惡意軟體的操作員透過一個基於 Web 的專用 C2 面板進行控制，該面板採用身份驗證保護，允許遠端發出命令。Kamasers 的 C&C 登入 UI 採用暗色主題，並帶有霓虹綠色點綴，顯示粗體「C&C 身份驗證」標題、單一密碼輸入框以及一個發光的綠色登入按鈕。

目前，感染媒介尚不清楚，但 Kamasers 最終以 HostService、GoogleHost.exe 和 AdobeSyn.exe 等誤導性名稱出現，模仿受信任的軟體。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan

基於機器學習的防禦技術：

- Heur.AdvML.B

2025/09/10

NFSkate威脅組織的RatOn安卓手機行動裝置銀行木馬

在最近報告中，資安公司 ThreatFabric 的行動威脅情資 (MTI) 分析師發現一種名為「RatOn」的複雜新型安卓手機行動裝置銀行木馬，由 NFSkate 威脅組織精心設計。 RatOn 代表行動網路犯罪的重大進步，它將經典的覆蓋攻擊與強大的自動轉帳系統 (ATS) 功能和近場通信 (NFC) 中繼功能相結合。該惡意軟體的傳播透過多階段感染鏈展開。初始入口點包含一個偽裝成第三

方安裝程式的惡意植入程式應用程式。該植入程式存在於成人主題網站上，其網域中經常帶有“TikTok18+”，主要針對捷克語和斯洛伐克語用戶。重要是，它請求大量權限，包括安裝來自未知來源的應用程序，進而繞過 Android 安全協議並允許濫用「無障礙服務」(Accessibility Services)。取得這些權限後，植入程式會安裝一個輔助有效酬載。此有效酬載會立即取得無障礙服務存取權限和設備管理員權限。它利用 WebView 介面誘騙受害者授予「輔助功能」存取權限，然後利用該權限自動授予進一步的可入侵權限，例如：讀寫聯絡人以及修改系統設定。然而，第二階段的酬載只是個前奏。其主要功能是部署或下載終極威脅：NFSkate 惡意軟體。第三階段最初設計用於近場通信(NFC)中繼攻擊，賦予 RatOn 廣泛的惡意功能。這些攻擊手段包括顯示假冒通知以欺騙用戶、串流螢幕內容以進行間諜活動、鎖定裝置進行勒索受害者、更改系統設定以實現持續控制，以及執行特定應用程式以進一步入侵裝置。 RatOn 的多面向攻擊方式使其成為 Android 惡意軟體領域中令人畏懼的新威脅。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

賽門鐵克的端點防護行動裝置版本(IOS/Android)已將其歸類為以下威脅並提供最完善的保護能力：

賽門鐵克的端點防護行動裝置版本 (IOS/Android) 還能夠分析簡訊內容的鏈接。它利用比對賽門鐵克全球資安情資網路 (GIN) 重要來源之一 Symantec WebPulse 中的威脅情報檢查簡訊內容中的網址，並在該鏈接為可疑時會及時提醒用戶，以保護用戶免受簡訊 (SMS) 網路釣魚攻擊。

- Android.Reputation.2

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/10

全新駭客組織：GhostRedirector，利用搜尋引擎排名優化(SEO)詐騙和後門，針對Windows伺服器發動攻擊

在最近報告中，ESET 研究人員發現一個全新駭客組織：GhostRedirector，該駭客組織已入侵巴西、泰國和越南至少 65 台 Windows 伺服器。該駭客組織涉及保險、醫療保健、零售和教育等多個領域，並使用複雜的自訂工具包。其關鍵武器庫包括 Rungan(可執行遠端命令的被動 C++ 後門)和 Gamshen(一個用於 SEO 詐欺即服務的惡意網路資訊服務 (IIS) 模組)。 Gamshen 專門針對 Googlebot 等搜尋引擎爬蟲，巧妙地修改搜尋結果，人為提升指定網站 (尤其是涉及賭博的網站) 的排名。這種操縱經過精心設計，目的在避免影響常規用戶的瀏覽體驗，進而保持一定的隱蔽性。雖然這種策略不會直接損害瀏覽者，但會將受感染主機伺服器與不道德的 SEO 行為聯繫起來，進而嚴重損害其信譽。GhostRedirector 的初始存取通常利用漏洞，SQL 注入是可能的攻擊手法。一旦入侵系統，他們就會利用 PowerShell 或 CertUtil 從臨時伺服器下載自訂工具。為了提升權限並確保持久存取，威脅行為者會利用 EfsPotato 和 BadPotato 等已知的漏洞，目的在建立特權使用者帳戶。這種多管齊下的攻擊方式使 GhostRedirector 能夠保持控制力和抵禦惡意元件被刪除的韌性，對受感染的組織構成重大威脅。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Malcode!gdn32
- Trojan.Gen.9
- Trojan.Gen.MBT
- Trojan Horse
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

網路層防護：

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：

- Audit: EFSRPC Bind Attempt
- Audit: SpoolSS Bind Request
- Attack: Windows Print Spooler Privilege Escalation

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/10

Gentlemen勒索軟體

根據趨勢科技研究人員報告，Gentlemen 是一個全新出現的勒索軟體威脅組織。據觀察，攻擊者會利用合法驅動程式、濫用群組原則物件 (GPO) 以及投放 KillAV 工具，目的在停用目標環境中已安裝的安全產品。部署的勒索軟體負載會加密使用者資料，並在加密檔案冠上 .7mtzhh 副檔名。勒索通知說明文字檔名為「README-GENTLEMEN.txt」的 .txt 檔案形式發送，攻擊者會要求受害者透過 TOX 加密即時通訊工具聯繫他們。該勒索軟體能夠終止與備份或資料庫操作相關的各種程序和服務，並刪除受感染端點上的陰影副本。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.TCP!gen6

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gentlemen
- Trojan.Gen.MBT
- Trojan.KillAV

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!200
- Heur.AdvML.C

2025/09/10

免費永遠最貴～Tamperedchef惡意軟體潛伏在AppSuite PDF Editor的免費工具中

根據 Truesec 報告，一個偽裝成免費應用程式「AppSuite PDF Editor」複雜惡意軟體行動已被發現，該行動會暗中部署名為「Tamperedchef」的惡意竊密軟體。該攻擊者採用高度混淆的程式碼 (可能是由人工智慧產生)，並利用 Google 廣告大肆進行傳播。行動始於促銷網站提供看似合法的 PDF 編輯器廣告。安裝程式執行後，使用者會看到一份標準最終使用者授權協議 (EULA)。之後，HTTP GET 請求會傳送到 inst[.]productivity-tools[.]ai 以監控安裝進度，而實際的惡意軟體負載則會從 vault[.]appsuites[.]ai 下載。雖然「AppSuite PDF Editor」最初運作正常，但它包含一個隱藏的計畫更新機制，該機制會啟動惡意元件。Tamperedchef 運作方式是針對 Web 瀏覽器資料庫，利用 DPAPI 進行資料解密。它會主動探測系統中是否安裝安全軟體，並強制終止正在執行的瀏覽器，以取得敏感的鎖定資料。該惡意軟體在行動啟動後 56 天才會被啟動，這與 Google 廣告活動的典型持續時間相吻合，進一步凸顯攻擊者的心思細膩。這顯示攻擊者在釋放惡意竊密軟體功能之前，會採取一種刻意的策略，以最大限度地取得用戶數，並明確表明其意圖是盡可能多地收集受害者資訊。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-RgPst!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- PUA.Gen.2
- Trojan.Gen.2
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2
- WS.Reputation.1
- WS.SecurityRisk.3

基於機器學習的防禦技術：

- Heur.AdvML.A
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/09

防護亮點：賽門鐵克檔案信譽(File Reputation)技術，上星期給客戶帶來哪些效益？

賽門鐵克檔案信譽服務是我們領先業界防護系統的基石。它會默默地分析雲端中的檔案和入侵指標 (Indicators-of-Compromise，簡稱 IoC)，並在幾分鐘內發佈這些檔案的信譽評等。File Reputation 維護超過 80 億個檔案的信任與惡意軟體評等。它每天分析約 40 億個 IOC 和超過 2,000 萬項新的信譽變更，讓每天有超過 600 萬個新檔案和簽章新增至檔案信譽資料庫。

作為一項雲端服務，Symantec File Reputation 已整合至所有 Symantec 和 Carbon Black 產品中，讓我們的客戶即時受到保護。具有 File Reputation 防護技術的產品包括

- 端點防護產品：SEP／SESE／SESC 等全系列端點防護解決方案
- 網頁閘道產品：WSS Gateway、Cloud SWG
- 電子郵件閘道產品：郵件安全雲端服務 (Email Security.Cloud)、地端自建郵件安全閘道 (SMG)
- 儲存設備：SPE
- Carbon Black 產品，包括：Endpoint standard、EEDR、AppControl

過去一週，賽門鐵克檔案信譽 (File Reputation) 技術為我們的客戶提供以下保護：

惡意軟體攔截

- 封鎖 360 萬個已知惡意軟體檔案。

賽門鐵克每天都會收到數百萬個新檔案和檔案雜湊值的資訊。當檔案被掃描時，掃描程序會交叉檢查我們的 Reputation 系統，查看它是否是已知的惡意軟體。

機器學習(ML-Machine Learning)攔截

- 透過機器學習演算法阻擋 331,000 項惡意軟體

賽門鐵克檔案信譽支援機器學習演算法，提供信譽給我們領先業界的 ML 分類器，然後將可疑檔案的入侵指標 (Indicators-of-Compromise，簡稱 IoC) 轉換成已確認的惡意軟體。

保護重要系統檔案和裝置驅動程式

- 識別出 20.1 億個關鍵系統檔案，確保客戶免受惡意軟體侵害且運作不中斷

賽門鐵克檔案信譽 (Symantec File Reputation) 可確保賽門鐵克產品不會因誤判而刪除關鍵系統檔案和裝置驅動程式而造成傷害。如今，先進的威脅會利用易受攻擊的裝置驅動程式，因此良好的惡意軟體防護必須能夠分辨遭入侵的和乾淨的系統檔案。Symantec Reputation 包括所有主要作業系統 (Windows、Mac、Linux) 上所有已知作業系統檔案和裝置驅動程式的乾淨檔案信譽和簽章者的信譽。

下載鑑識(Download Insight)

- 依賴此技術攔截到 224 萬次的惡意程式。

下載鑑識 (Download Insight) 是一項積極的安全政策，可防止未知的 PE 和 MSI 檔案在受保護的機器上執行。當下載新檔案、未簽署、非普遍或以其他方式識別為客戶使用的檔案時，下載鑑識 (Download Insight) 即會啟動。。

欲深入了解下載防護：下載鑑識 (Symantec Download Insight) 的詳細資訊，請點擊此處。
欲深入了解 Symantec Endpoint Protection 如何使用 Symantec Insight 進行檔案相關決策，請點擊此處。

2025/09/09

不安全的物聯網成為網路攻擊免費傭兵～RapperBot：快速移動的物聯網殭屍網路利用NVR發動DDoS攻擊

RapperBot 是一個快速發展的物聯網殭屍網路，它正在迅速將受感染 DVR 和 NVR 接管為發動大規模 DDoS 攻擊的節點。根據 Bitsight 報告，攻擊者通常會透過暴力破解憑證或利用韌體漏洞來利用網路上暴露的裝置，然後以韌體更新的形式投放惡意籌載。一旦執行，RapperBot 就會掛載 NFS 共享來獲取並運行於特定架構的二進位檔案，且完全在記憶體中運行，並將其命令和控制基礎設施隱藏在加密的 DNS TXT 記錄中。執法部門已開始拆除其基礎設施並逮捕其營運商，但攻擊活動仍在繼續，凸顯未進行修正更新且不安全物聯網設備所帶來的持續風。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護（**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**），並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Linux.Mirai
- Trojan.Gen.2
- Trojan.Gen.NPE

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/09

憑證竊盜：威脅行為者假冒匈牙利郵政(Magyar Posta Zrt.)名義進行詐騙

賽門鐵克發現新一波假冒匈牙利郵政 (Magyar Posta Zrt.) 名義的網路釣魚攻擊，目的在竊取使用者憑證。Magyar Posta Zrt. 是匈牙利的郵政服務，提供物流、金融和支付服務。在此次攻擊行動中，釣魚郵件偽裝成報關費用通知。這些簡潔的電子郵件會提示收件者點擊釣魚網址，支付所謂的貨件報關費用。點擊連結後，受害者會被引導至專門用於竊取憑證的網頁。

- 電子郵件主旨：包裹通關的付款義務
- 經翻譯後電子郵件主旨：包裹報關的付款義務

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

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)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/08

TinyLoader惡意程式載入器在竊取錢包資訊的同時傳播惡意竊密程式

在最近報告中，研究人員重點關注 TinyLoader，這是一款隱密的惡意程式載入器，用於竊取加密貨幣並部署類似 Redline Stealer 和 DCRat 的額外籌載。根據他們的分析，它透過受感染的 USB 隨身碟、共享網路和欺騙性捷徑方式進行傳播，然後透過隱藏檔案副本和篡改登錄機碼來嘗試持久化。重要是，它會主動監控剪貼簿活動--替換複製的錢包位址以劫持交易。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rgsvr!g1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Gen.MBT
- Trojan.Gen.2

2025/09/08

XWorm採用多階段感染鏈

資安業者 Trellix 已揭露 XWorm 後門攻擊行動有所變化，其攻擊方式已從簡單的採用 .lnk 捷徑檔傳播方式演變為更具欺騙性的多階段感染鏈。初始攻擊啟於一封攜帶惡意 .lnk 捷徑檔的網路釣魚郵件，該檔案執行後會啟動一個隱藏的 PowerShell 腳本。該腳本會植入一個誘餌文字檔，同時下載一個偽裝的二進位檔案，該檔案通常以模仿 Discord 等受信任應用程式的命名方式命名。啟動後，此二進位檔案會安裝其他元件，包括真正的 XWorm 酬載。這種分層的流程，加上使用看似合法的應用程序，使攻擊者能夠潛入並規避某些安全措施。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-Schtsk!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh.C!gen15
- SONAR.SuspBeh!gen93
- SONAR.SuspBeh!gen752
- SONAR.SuspDataRun

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.ASync
- ISB.Downloader!gen589
- MSIL.XWorm!gen2
- Scr.Mallnk!gen1
- Trojan Horse
- Trojan.Emotet
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

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：

- Audit: Bad Reputation Application Activity
- System Infected: Bad Reputation Application Network Activity

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/08

TAG-150惡意軟體即服務(MaaS)駭客組織部署自有的Castle惡意軟體家族

TAG-150 是一個全新駭客組織，其運作模式為惡意軟體即服務 (MaaS)。TAG-150 涉入的相關活動主要特色是部署多個客製化開發的惡意軟體，包括 CastleBot、CastleLoader 和 CastleRAT。觀察結果顯示，這些部署通常作為傳遞次級載荷 (例如：NetSupport RAT、RedLine Stealer、Rhadamanthys Stealer 和 SectopRAT 等) 的初始載體。威脅情資平台 Recorded Future 的專家研究團隊--Insikt Group 發布一份報告提供有關該組織活動的詳細資訊。

根據這份報告，TAG-150 採用強大的多層命令與控制 (C&C) 基礎設施來保持韌性並規避攻擊，利用「固定情報解析器 dead drop resolver」技術結合 Steam 社群設定檔來定位活躍的 C2 伺服器。感染通常透過社交工程方式發起，包括以 Cloudflare 或詐騙性的 GitHub 儲存庫為主題的網路釣魚活動。CastleRAT 還利用一種 UAC 繞過方法，該方法涉及重複使用 PowerShell 命令來建立 Windows Defender 排除項，這可能會干擾沙箱分析。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen804
- SONAR.SuspLaunch!g444
- SONAR.SuspStart!gen2
- SONAR.SuspStart!gen6
- SONAR.SuspStart!gen9
- SONAR.SuspStart!gen18n

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- PUA.Gen.2
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Malware.2

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B
- Heur.AdvML.B!100
- Heur.AdvML.B!200
- Heur.AdvML.C

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/08

詐騙是最便宜有效的駭客工具～GPUGate：惡意軟體行動透過GitHub和Google Ads鎖定IT專業人士為目標

根據 Arctic Wolf 報導，一個名為 GPUGate 的複雜惡意軟體攻擊行動利用 GitHub 的基礎設施和 Google 廣告，向西歐的 IT 專業人士傳遞惡意籌載。作為攻擊媒介的一部分，用戶會被一個欺騙性的 Google 廣告引誘，該廣告會將用戶引導至一個被入侵的 GitHub 程式碼庫，其中的特定提交包含惡意下載連結。 MSI 安裝程式模仿 GitHub Desktop 應用程序，並包含 100 多個虛擬可執行檔以逃避安全沙箱的偵測。執行後，該惡意軟體會採用 GPU-gated 的解密例程，確保負載在沒有 GPU 的系統上保持加密狀態。此攻擊行動的目的在透過誤導 IT 員工在嘗試安裝 GitHub Desktop 時下載惡意軟體，進而取得初始存取權限，以竊取憑證、竊取資訊並可能部署勒索軟體。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- Trojan Horse
- Trojan.Gen.MBT

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/08

Salat Stealer：以Go語言撰寫的惡意竊密程式正透過惡意軟體即服務(Masa-a-Service)模式大肆傳播

Salat Stealer 是一款採用 Go 語言撰寫的惡意竊密程式，正透過惡意軟體即服務 (Masa-a-Service) 模式大肆傳播，已被 Cyfirma 回報。該惡意軟體可能由俄語攻擊者所經營作，採用分層持久化技術，包括登錄檔的 Run 機碼、排程任務、程序偽裝以及修改 Windows Defender 排除項目以逃避檢測。它能夠竊取敏感訊息，例如：瀏覽器憑證、加密貨幣錢包以及 Telegram 和 Steam 等平台的會話。Salat Stealer 使用輕量級信標和加密通道與其命令與控制 (C&C) 基礎設施進行通訊，並由回退機制支援以確保連續性。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.Dropper

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Wannacry
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

網路層防護：

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：

- Audit: Bad Reputation Application Activity
- URL Reputation: Webpulse Bad Reputation Domain Request

2025/09/08

Obscura：採用Go語言撰寫的全新勒索軟體～躍上檯面

一款名為 Obscura 全新勒索軟體已現身，成為 2025 年不斷成長針對企業組織活躍的勒索軟體家族之一。該勒索軟體最初由 Huntress 發現，它的加密副檔名為「.obscura」，並釋放名為 README_Obscura.txt 的勒索通知信。受害者有 10 天的時間做出回應，並警告稱，如果不乖乖配合，被盜資料將被公開洩露。

Obscura 以 Go 二進位檔案形式傳遞，透過名為 SystemUpdate 的排程任務建立持久性。這個二進位檔案從 NETLOGON 共用啟動，這使得它能夠跨網域控制器複製，為攻擊者提供隱密的立足點。它還會刪除影陰副本，使復原變得困難。目前已有七家組織確認為受害者，該勒索軟體顯然正在加強攻擊力度，並向各行業擴展。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Untrst-RunSys!g1
- ACM.Vss-DlShcp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomPlay!gen1
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g250
- SONAR.SuspLaunch!gen4

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen.HC
- Trojan.Gen.MBT

2025/09/07

Stealerium：一個引爆大範圍攻擊的開源惡意竊密軟體

Stealerium 是一款開源惡意竊密軟體，近期到處點火。過去幾個月，多個威脅組織發動的各種攻擊行動中部署該惡意軟體。其最初傳播媒介是帶有附件的惡意垃圾郵件，這些附件負責下載 Stealerium 的有效酬載。攻擊目標是從受感染的設備中收集並竊取資料。

該電子郵件的初始攻擊是透過社交工程手法，目的在向目標受害者操弄緊迫情緒，促使其採取行動。郵件主旨包括財務義務 (例如：發票、付款請求、報價) 以及酒店／旅行 (例如：預訂請求) 等，並以此作為誘餌。惡意電子郵件附件的文件類型多種多樣，包括壓縮檔、IMG、JS 和 VBS 等類型的檔案。

Proofpoint 安全研究人員發布一份報告詳細介紹 Stealerium 惡意軟體的功能。該惡意軟體目的在進行廣泛的資料收集，優先考量獲取各式各樣的使用者資訊，包括：

- 登入憑證、銀行和信用卡資訊、與加密貨幣持有相關的資料。
- 使用者通訊、網路設定、VPN 憑證，甚至系統特定資料 (例如：已安裝的軟體和 Windows 金鑰)。
- 可能包含有價值的個人或專業資料的檔案。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP**/**SESC**/**SMG**/**SMSMEX**/**Email. Security.cloud**/**DCS**/**EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.ProcHijack!g55
- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

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)。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Wannacry
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- ISB.Downloader!gen60
- ISB.Downloader!gen68

- ISB.Dropper!gen1
- MSIL.Downloader!gen8
- MSIL.Packed.19
- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.2
- VBS.Downloader.Trojan
- WS.Malware.2
- WS.SecurityRisk.1
- XSNet.Js!gen2

網路層防護：

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：

- Audit: Bad Reputation Application Activity
- System Infected: PUA.Gen Activity 38
- URL Reputation: Webpulse Bad Reputation Domain Request

2025/09/05

LockBeast 勒索軟體

LockBeast 是一種結合檔案加密與資料竊取功能的勒索軟體，藉此向受害者施壓以迫使其付款。執行後，該程式會使用強效加密演算法加密檔案，在檔案名稱後冠上受害者專屬識別碼及「.lockbeast」副檔名，並放置名為 README.TXT 的勒索贖金說明文字檔。該文字檔告知受害者，其敏感資產--包含文件、資料庫、原始碼、交易紀錄及個人資料--已遭加密並竊取。攻擊者要求受害者透過 Session、Tox 等注重隱私的通訊軟體聯繫，警告勿重新命名檔案或使用第三方解密工具，並設定嚴格的七天期限。若未乖乖配合要求，攻擊者威脅將公開竊取的資料，增強 LockBeast 雙重勒索的運作模式。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 (**SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR**)，並以下述的命名及對應的防護機制來提供具體說明：

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomGen!gen3
- SONAR.Ransomware!g38

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Ransom.Gen.HC
- Trojan.Gen.MBT

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.A!400
- Heur.AdvML.A!500
- Heur.AdvML.B!100
- Heur.AdvML.B!200

2025/09/05

網路釣魚攻擊行動，鎖定GMO Aozora專業網路銀行(Net Bank)的客戶

GMO Aozora 專業網路銀行 (Net Bank)，是由日本青空 (Aozora) 銀行和 GMO Internet 共同出資於 2018 年共同創立的日本純網路銀行，為個人及企業客戶提供客製化金融服務。近期發現有針對該行網路銀行服務的釣魚攻擊活動，攻擊者偽造銀行名義寄發電子郵件，利用虛假的 GMO 點數通知誘騙收件者點擊連結以驗證帳戶資訊。該連結會將用戶導向偽造的登入頁面，藉此竊取憑證，使攻擊者可能未經授權存取受害者帳戶。相關電子郵件使用下列主旨：

- GMOあおぞらネット銀行 マイル加算状況のご案内
- 譯文：GMO Aozora Net Bank 里程累積狀況通知

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

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)。

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

2025/09/05

流行讓人失去警覺成為詐騙的破口～AI Waifu遠端存取木馬(RAT)利用人工智慧熱潮

AI Waifu RAT 是一種新發現的遠端存取木馬程式，透過偽裝成 AI 互動或研究工具在大型語言模型角色扮演社群中傳播。該惡意軟體經由 GitHub、OneDrive 和 Mega.nz 散佈，利用社交工程手法誘使用戶停用防毒軟體，並信任其假冒宣傳的「先進 AI 功能」。一旦安裝，此惡意程式將執行本地代理程式，透過明文 HTTP 進行通訊，進而實現指令執行、檔案竊取及持久化功能。

賽門鐵克解決方案已於第一時間提供此類型威脅的完善保護 **(SEP/SESC/SMG/SMSMEX/Email.Security.cloud/DCS/EDR)**，並以下述的命名及對應的防護機制來提供具體說明：

VMware Carbon Black 產品的防護機制：

Carbon Black 產品中的現有政策會阻止和偵測相關的惡意指標。建議的政策至少是阻止所有

類型的惡意軟體執行 (已知、可疑和 PUP)，並延遲雲端掃描的執行，以便從 Carbon Black Cloud 信譽服務中獲得最大收益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Meterpreter
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於網頁防護(如果您有使用WSS--地端或雲端網頁分類／過濾／安全服務)：

被發現的惡意網域名稱／IP位址已於第一時間收錄於不安全分類列表中。

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 年起就全心全力專注在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使用情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。許多顧客樂意與我們建立起長期的友誼，把我們當成可信任的資安建議者、可以提供良好諮商的資安策略夥伴以及總是第一個被想到的求助暨諮詢對象。

保安資訊連絡電話：**0800-381-500**。