保安資訊--本周(台灣時間2025/05/02)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 33 萬 7,400 台受保護端點上總共阻止了 4,700 萬次攻擊。這些攻擊中有 83.6% 在感染階段前就被有效阻止：**(2025/04/28)**

- 在**7萬1,900**台端點上，阻止了**1,860**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬4,100**台端點上，阻止了**630**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬3,000**台**Windows**伺服主機上，阻止了**620**萬次攻擊。
- 在**4萬5,100**台端點上，阻止了**170**萬次嘗試掃描伺服器漏洞。
- 在**1萬600**台端點上，阻止了**8萬3,300**次嘗試掃描在**CMS**漏洞。
- 在**4萬1,300**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**9萬3,400**台端點上，阻止了**200**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**1,200**台端點上，阻止了**72萬7,400**次加密貨幣挖礦攻擊。
- 在**9萬4,700**台端點上，阻止了**690**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**577**台端點上，阻止了**7萬9,500**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 16 萬 4,700 個受保護端點上阻止了總計 730 萬次攻擊。**(2025/04/28)**

- 使用網頁信譽情資，在 **158K** 個端點上阻止 **690** 萬次攻擊。
- 攔截 **18.6K** 個端點上 **277.9K** 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 **5.2K** 個端點上攔截 **125.7K** 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 **310** 個端點上攔截 **3.5K** 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。

2025/05/02

得力於TAG-124惡流量分配系統(TDS)的威力，MintsLoader惡意程式載入器一躍成為駭客圈的當紅辣子雞

MintsLoader 是 2024 年首次發現到先進惡意程式載入器，在 TAG-124 惡流量分配系統 (TDS) 被廣泛使用，勝於其他威脅份子更常部署惡意有效酬載，例如：GhostWeaver、StealC 和修改過的 BOINC 用戶端。這些攻擊主要針對工業、法律和能源等領域。惡意軟體通常透過釣魚電子郵件並以發票為主題的誘餌進行傳播，並採用混淆 JavaScript 和 PowerShell 腳本的多階段感染鏈。MintsLoader 具備先進的反虛擬機 (AntiVM) 功能，可偵測沙箱或虛擬環境，並利用網域產生演算法 (DGA) 每日建立新的命令與控制 (C&C) 網域，使偵測與緩解工作變得更加複雜。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Base64!g1
- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1
- ACM.Wmip-Ps!g1
- ACM.Wscr-Ps!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政

策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Downloader
- ISB.Suspexec!gen48
- Scr.Heuristic!gen20
- Scr.Malcode!gen105
- Scr.Malcode!gen170
- Scr.Mallnk!gen3
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Web.Reputation.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。

2025/05/01

以南非金融情報中心法案(FICA)為主題的簡訊釣魚詐騙，假冒南非的數位銀行：Discovery Bank

Discovery Bank 是南非知名的數位銀行，在最近網路釣魚攻擊中，其品牌遭到團體或個人濫用，目的在於竊取行動使用者的銀行憑證。此攻擊始於利用南非金融情報中心法案 (Financial Intelligence Centre Act in South Africa -FICA) 法規遵循為誘餌的惡意簡訊。

惡意簡訊 (原樣)：Final notice! Your Discovery Bank account is not FICA compliant. Upload your documents now on hxxps[:]//cutt[.]cx/E1mJg to avoid suspension(*最後通知！您的 Discovery Bank 帳戶不符合 FICA 法規。現在就上傳您的文件到 hxxps[:]//cutt[.]cx/E1mJg 以避免被暫停。)

如果使用者被成功誘騙點擊惡意的短網址，就會會被重導向到一個模仿銀行登入入口網站的釣魚網頁。該頁面託管在 Contabo GmbH (一家德國託管供應商) 的雲端空間。寫死在程式碼的表單動作會將憑證提交至惡意伺服器。。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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。WebPulse 已知道此次活動中使用假冒的域名。

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。

2025/05/01

多個進階持續威脅(APT)駭客集團正在使用ClickFix社交工程伎倆

ClickFix 伎倆深受在來自北韓、伊朗和俄羅斯的多個進階持續威脅 (APT) 駭客集團所青睞。這是一種社交工程手法，惡意網站冒充合法的軟體或文件共享平台。觀察到有目標式攻擊會以網路釣魚或惡意廣告誘餌引爆，顯示聲稱文件或下載失敗的詐騙錯誤訊息。然後會提示受害者按一下「Fix」按鈕，這會反過來指示他們執行 PowerShell 或命令列指令碼。執行此類指令會在不知情情況下建立 SSH 通道，並導致惡意軟體的執行，讓攻擊者可從後門存取受害者的系統。

網路知識：ClickFix 為「複雜的社交工程手法」，偽裝成系統錯誤訊息或文件註冊提示，幾可亂真網頁或文件外觀，誘導使用者執行惡意指令。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Trojan Horse
- Trojan.Gen.NPE
- Trojan.XSense.C
- Web.Reputation.1
- WS.Malware.1
- WS.Malware.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。

2025/05/01

伊朗駭客組織攻擊重要的中東關鍵基礎設施

Fortinet 研究人員最近發表他們針對伊朗駭客組織攻擊中東關鍵基礎設施的調查報告。該報告詳述攻擊者的戰術、技巧和程序 (TTPs)，包括入侵、建立持久性和相關的操作。提供的進一步詳細資訊包含所使用的各種植入程式 (後門、載入器、駭客工具、Web shells) 和 lolbins 來達成目標。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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.SuspReg!gen29

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Hacktool
- Hacktool.Gen
- PasswordRevealer
- PUA.Gen.6
- Remacc.MeshCentral
- Revsocks
- Trojan Horse
- 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!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。

2025/04/30

魚叉式網路釣魚行動鎖定WUC會員，並使用經木馬化的維吾爾語文字編輯器

據報導，一個魚叉式網路釣魚行動鎖定世界維吾爾代表大會 (World Uyghur Congress，WUC) 的高級會員傳遞監控惡意軟體。以一個合法維吾爾語文編輯器的特洛伊木馬版本作為攻擊的一部分，以獲得遠端存取、收集系統訊息，並操縱檔案。該攻擊使用兩種不同的命令和控制 (C&C) 基礎架構，兩者皆利用仿冒該工具原始開發者的偽造網域。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Trojan Horse
- 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: Trojan.Backdoor Activity 568

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。

2025/04/30

Pentagon惡意竊密程式

Pentagon 是最近發現的惡意竊密程式，採用 Python 和 Golang 所設計，目的是滲出各種敏感資訊。它主要針對瀏覽器憑證、cookie、加密貨幣錢包資料以及 Discord 和 Telegram 等應用程式的驗證權杖。該惡意軟體透過拚字錯誤的域名手法 (typosquatting) 進行傳播，並有多個別名，包括 Acab 和 BLX Stealer。該惡意程式使用一般 HTTP 請求與其命令和控制 (C&C) 伺服器通訊，以隱匿方式傳輸竊取的資料。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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.Stealer!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.MBT

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.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。

2025/04/30

Hannibal惡意竊密程式～源於重新包裝兩個惡意竊密程式家族的新版本

Hannibal 惡意竊密程式是一款在真實網路情境上發現到的先進惡意軟體，是重新包裝 Sharp 和 TX 惡意竊密程式家族後的新版本。它以 C# 開發，針對 Chromium 和基於 Gecko 的瀏覽器，在繞過瀏覽器保護的同時擷取敏感資料。它的功能擴展到竊取加密貨幣錢包、FTP 客戶端和 VPN 的憑證，以及收集全面的系統資訊。另一個值得注意的功能是其加密剪輯模組，可劫持剪貼簿內容來重導向加密貨幣交易。

該惡意軟體是透過採用 Django 的 Web 框架設計的命令和控制 (C&C) 伺服器面板來控制，並透過每月訂閱計劃在暗網論壇上大肆宣傳。活躍的 Telegram 頻道和持續妥善維護的控制基礎架構顯示其持續涉入攻擊行動和持續深受威脅者喜愛的優勢。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.MalTraffic!gen1
- SONAR.Stealer!gen1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- WS.Malware.1

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
- Audit: Untrusted Telegram API Connection
- System Infected: Trojan.Backdoor Activity 564
- System Infected: Trojan.Backdoor Activity 568
- System Infected: Trojan.Backdoor Activity 641
- System Infected: Trojan.Backdoor Activity 654

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。

2025/04/30

人性永遠是最不牢靠的資安破口～透過Microsoft Teams的語音和視訊平台劫持TypeLib的社交工程攻擊行動

在最近攻擊事件中發現一起濫用微軟 Teams 語音和視訊平台的網路釣魚行動，該行動傳播一種獨特的 PowerShell 後門。被駭客組織：Storm-1811 透過在微軟 Teams 聊天中對目標員工使用社交工程技巧來發起攻擊，假裝是內部 IT 支持人員。其伎倆是藉由協助受害目標解決技術問題

的幌子下欺騙受害者，以便使用內置的 Windows 快速協助遠端監控和管理工具來部署惡意軟體。攻擊者將使用命令更改 Windows 登錄檔 (Registry)，針對 TypeLib 路徑。透過修改 TypeLib 的呼叫點以包含惡意腳本，駭客組織為確保他們的惡意軟體在每次呼叫該物件時運行，從而在遭入侵的系統中建立持久性／常駐能力。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Rd32!g1
- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- JS.Redirector
- ISB.Cobalt!gen2
- ISB.Downloader!gen*
- Scr.Heuristic!gen8
- Trojan Horse
- Trojan.Gen.NPE
- Trojan.XSense.C
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.4

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.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。

2025/04/29

Gremlin惡意竊密程式

Gremlin 惡意竊密程式是 Palo Alto 研究人員最近發現一款全新採用 C# 語言撰寫的惡意軟體。Gremlin 惡意竊密程式目前透過 Telegram 頻道進行販售。該惡意軟體會從遭入侵的端點收集各

種資料，包括剪貼簿資訊、儲存在系統網頁瀏覽器中的資料、螢幕截圖、cookie、加密貨幣錢包資訊以及憑證和銀行資料等。收集到的資料會壓縮成 .zip 檔案，並透過 Telegram API 洩出給威脅份子。

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 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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.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。

2025/04/29

防護亮點：賽門鐵克重要主機防護系統：DCS～Data Center Security--針對好工具總被來當凶器的就地取材攻擊(LOTL)提供強大防護～以PowerShell攻擊為例

就地取材攻擊 (LOTL-Living Off the Land) 如何運作？

與傳統的惡意軟體攻擊不同，LOTL 會利用系統內建或合法工具軟體來執行攻擊計畫，它是無檔案攻擊的一種--攻擊者不需要在目標系統安裝任何程式碼或腳本。相反地，攻擊者會使用環境中已有的工具，例如：PowerShell、Windows Management Instrumentation (WMI) 或密碼儲存工具 Mimikatz 來執行攻擊。

PowerShell 是常用於執行例行性排程自動化和組態管理的工具。網路威脅份子經常利用就地取材攻擊戰略濫用此公用程式。PowerShell 是用於排程自動化和組態管理的強大工具，建構在 .NET 架構上。它由指令 shell 和腳本語言組成，支援多種平台，包括 Windows 和 Linux。一旦入侵受害者環境，多數的勒索軟體和惡意軟體會使用 PowerShell 執行各種任務。PowerShell 腳本也常用於部署勒索軟體、停止 Windows Defender 等服務、刪除陰影複本、修改本機帳號、廣播 MAC 位址，以及包含修改 README 檔案的關聯以允許雙擊開啟等諸多惡意行為。

LOTL 威脅不是將惡意程式碼引入系統，而是使用系統上的現有工具來規避資安軟體偵測，這使得這些網路攻擊更難被偵測和緩解。這些技術可能發生在多種類型的 IT 環境中，包括本地端、雲端或混合環境。國家級駭客組織經常使用這些技術來逃避偵測。

對組織的資安衝擊

由於成功利用漏洞會導致遠端程式碼執行、竊取敏感資訊及組織網路的進一步橫向移動，因此其影響程度被視為嚴重等級。這些漏洞在網路上會被大肆濫用。更廣泛的安全社群已聯合起來保護 PowerShell，並發表多份相關的詳細刊物，包括賽門鐵克的多份刊物。他們協助全球受影響的使用者，深入分析威脅份子所使用的技術、可用的防護範圍，並提供進一步的指導，讓使用者留意入侵指標與緩解策略。

賽門鐵克重要主機防護系統：DCS～Data Center Security--防禦 LOTL 攻擊的有效零時差解決方案

賽門鐵克重要主機防護系統：DCS～Data Center Security 的入侵防護預設政策能為 Windows 和 Linux 伺服器提供零時差防護。傳統的防毒軟體使用定義檔偵測來識別惡意軟體。然而，過去幾年來，無檔案惡意軟體和 LotL 攻擊的增加，迫使業界重新思考如何偵測惡意軟體，進而需要啟發式演算法。

PowerShell 與其他指令碼語言一樣，可以直接在記憶體中啟用，並執行遠端下載有效酬載的指令，繞過安全防護機制，而且幾乎不會在磁碟上留下任何蛛絲馬跡供防禦人員識別和分析。使用 PowerShell 的惡意軟體可以進行權限提升、混淆和遠端程式碼執行等活動。近年來，有幾種惡意軟體家族將 PowerShell 做為凶器，包括 Netwalker、RogueRobin、PowerWare 和 POWELIK。此外，許多合法的後期攻擊框架 (例如：Metasploit、PowerSploit 和 Mimikatz) 也使用 PowerShell，這些框架也可以兼作 CTA 用來攻擊系統和竊取憑證的武器。說到底，濫用 PowerShell 的攻擊不會在短時間內消失，這也就是為什麼在日常工作中使用 PowerShell 的同時，必須加強防禦以免好工具總被來當凶器的主要原因。

DCS 入侵防護系統

DCS 入侵防護系統提供零時差保護，包括：作業系統鎖定、應用程式控制以及實體和虛擬伺服器工作負載的應用程式隔離。針對作業系統和應用程式 (包括 PowerShell) 的底層沙箱技術和政策強制的行為控制，可針對未知威脅提供主動式防護，而無需一直依賴持續的定義檔更新。DCS 為全球客戶的關鍵基礎架構提供保護，二十多年來，大型企業對 DCS 技術堆棧深信不疑。

預設 DCS 的Windows 強化政策

預設的 DCS Windows 強化政策與其預先定義的沙箱可防止威脅者在攻擊期間和攻擊後使用的多種攻擊技術。縱深防護策略可在攻擊鏈的各個階段提供如下 (不限於) 保護：

- DCS 可防止透過子程序使用就地取材技術的執行。
- 啟用沙箱執行控制，以防止任何程序啟動可疑的子程序。
- 將 *\cmd.exe、*\powershell.exe、*\powershell_ISE.exe、*\rundll32.exe、*\net.exe 加入不應由其他應用程式啟動的程式清單。
- 兩用工具可從預先定義的全域原則服務清單中讓它不應被啟動。如果需要執行特定工具，則可根據部署中的使用情況，新增 cmdline 參數和/或使用者名稱的例外。
- 將*.zip、*.rar、*.7z、*.php、*.asp、*.aspx、*.asmx、*.asax、*.jsp、*.js 新增至「Read only Resource」清單，以防止從 powershell.exe 及其子程序寫入更多任意檔案。在政策沙箱中阻

止修改這些檔案。與眾不同的是 DCS 可非常精細地控制允許例外。

賽門鐵克重要主機防護系統：DCS～Data Center Security 能提供最完整的伺服器防護，可在私有雲／公有雲資料中心實現微分段、限縮管理員權限、緩解進行修補的急迫性，以及防護零時差威脅。

關於賽門鐵克的重要主機防護系統：DCS～Data Center Security 的完整資訊可點擊網頁說明或最新簡報檔。網頁或簡報如有說明不夠清楚的地方，歡迎與保安資訊的業務或技術顧問提供建議。

2025/04/29

CVE-2025-24054--存在NTLM雜湊值洩露漏洞被大肆開採濫用

CVE-2025-24054 是一個最近披露的漏洞，涉及透過欺騙手段洩露 NTLM(New Technology LAN Manager) 身分認證協定的雜湊值。未經授權的攻擊者可利用製作的 .library-ms 檔案，在網路上執行欺騙。利用該漏洞，攻擊者可能獲得 NTLM 雜湊值或使用者密碼。此漏洞最近才被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

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 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan Horse
- Trojan.Gen.NPE

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 預設的 Windows 加強政策可防止在攻擊期間和攻擊後使用的多種攻擊技術。縱深防禦策略可在攻擊鏈的各個階段提供保護。
- 預設強化政策可防止系統連線至網際網路，進而防止下載或資料滲透至 C&C 伺服器的嘗試。
- DCS 可防止從網路下載惡意壓縮檔或 .library.ms 檔儲存至磁碟。
- DCS 防止 .URL 檔案透過 UNC 路徑開啟任何網路連線 (此攻擊中有使用網路共用)。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2025/04/29
CVE-2025-3928--存在老牌備份軟體領導廠商Commvault Web Server漏洞

CVE-2025-3928 是最近揭露一個影響 Commvault Web Server 的不明漏洞。若遭成功開採濫用，此漏洞可讓遠端、經驗證的攻擊者未經授權存取受影響系統，並允許他們部署及執行任意 webshell。此漏洞已在 11.36.46、11.32.89、11.28.141 及 11.20.217 版本的產品中解決。此漏洞最近才被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功利用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中，顯示該漏洞在真實網路情境中已遭大肆開採濫用。

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 偵測到的惡意程式名稱及有效對應的防護機制：

基於安全強化政策(適用於使用DCS)：

賽門鐵克重要主機防護系統：DCS～Data Center Security 的 Windows 強化政策中的 Commvault 自訂沙箱可防止在攻擊期間和攻擊後使用的多種攻擊技術，例如：部署和執行 Web shell。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/04/29
ELENOR-corp--源於Mimic勒索軟體的最新變種

ELENOR-corp 是源於 Mimic 勒索軟體的最新變種，最近才在真實網路情境上被發現，據報以醫療保健行業為目標。攻擊者在部署勒索軟體有效酬載之前的活動中，還利用常駐型的 Clipper 惡意軟體以及基於 Python 的惡意竊密程式。ELENOR-corp 勒索軟體具有多種功能，包括反電腦鑑識 (Anti-Forensic) 機制、系統資訊收集、竄改使用者帳戶控制設定 (UAC)、透過修改 Windows 登錄檔 (Registry) 來設定每次系統啟動時的排程執行以達到常駐的功能、程序列舉、卸載虛擬驅動程式或刪除系統陰影複製和備份等。

網路知識：Clipper 惡意軟體是一種專門針對加密貨幣的惡意軟體，能監控用戶的剪貼簿活動，竊取並替換加密貨幣地址，進而將用戶的數位資產轉移至攻擊者控制的錢包。

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 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Infostealer
- Trojan Horse
- Trojan.Gen.MBT
- Ransom.Mimic

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。

2025/04/29

Konni進階持續威脅(APT)駭客集團涉入鎖定南韓公司行號、組織機構的多階段目標式攻擊

據觀察，一個複雜的多階段惡意軟體攻擊行動與北韓的 Konni 進階持續威脅 (APT) 駭客集團有關，主要針對南韓的公司行號、組織機構等實體。此攻擊始於一個 ZIP 檔案，其中包含一個偽裝的 .lnk 捷徑檔，可執行混淆的 PowerShell 指令碼，進行下載並執行其他惡意有效酬載。最後的有效酬載是遠端存取木馬程式 (RAT)，可建立持續存取、收集系統資訊和目錄清單，並將資料滲出到遭入侵掌控的指揮與控制 (C&C) 伺服器。

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 偵測到的惡意程式名稱及有效對應的防護機制：

基於行為偵測技術(SONAR)的防護：

- SONAR.Powershell!g20
- SONAR.Powershell!g111

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- CL.Downloader!gen11
- Scr.Mallnk!gen4
- Scr.Mallnk!gen13
- Trojan Horse
- Trojan.Gen.NPE
- 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。

2025/04/28

RevolverRAT惡意遠端存取木馬透過惡意電郵進行傳播

RevolverRAT 是剛嶄露頭角的全新遠端存取木馬程式，最初是透過收件者母語撰寫的目標性電子郵件傳播，聲稱有版權問題需要處理。這些電子郵件要求使用者點選一個連結，最終會安裝容易受到 DLL 側載攻擊的軟體。RevolverRAT 包含反分析技術、受害者指紋，並允許攻擊者遠端執行程式碼。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

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

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

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：

- Downloader
- Packed.Generic.758
- Trojan Horse
- WS.SecurityRisk.4

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

2025/04/25

散佈DslogdRAT惡意軟體的網路攻擊行動

根據日本電腦緊急應變團隊暨協調中心 (JPCERT) 報告，最近有一場傳播 DslogdRAT 惡意軟體的攻擊行動以日本的組織為目標。攻擊者利用 Ivanti Connect Secure (CVE-2025-0282) 的漏洞來傳送惡意的有效酬載。DslogdRAT 具有執行從特定 C&C 伺服器 (根據寫在程式中的硬編碼配置資料) 接收的任意指令的功能。所執行的指令可包括上傳或下載檔案、執行 shell 程式碼或代理 (proxying)。惡意軟體還會收集受感染端點的基本資訊，並將這些資料轉發給攻擊者。

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 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Trojan
- Hacktool.Webshell
- Trojan.Gen.NPE

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：

- Web Attack: Ivanti ICS CVE-2025-0282

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克重要主機防護系統：DCS～Data Center Security 強化的防護可防止惡意軟體在系統上被注入或執行。DCS 強化的 Linux 伺服器可防止從暫存或其他可寫位置執行相關的惡意軟體。
- DCS 預設防禦政策也會阻止停用 SELinux、修改 syslog 屬性或掛載／卸載磁碟機，這些都是 CVE-2025-0282 攻擊中採用的伎倆。
- 經 DCS 安全強化過的 Linux 伺服器會鎖定管理員帳號，因此可防止任何權限提升 (提權)。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

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。

2025/04/25

出現假冒的英國「駕照與行照局」(DVLA：Driver and Vehicle Licensing Agency)電子郵件通知的網路地行動

英國「駕照與行照局」(DVLA：Driver and Vehicle Licensing Agency)，負責維護英國境內駕駛者及全英國車輛的記錄。最近，賽門鐵克發現有人假冒 DVLA 名義進行網路釣魚，誘使使用者開啟偽造的通知郵件。該電子郵件提到與帳戶相關的付款方式已過期，使用者需要更新偏好的付款方式。這些詐欺電子郵件目的在誘騙使用者點擊釣魚 URL。當受害者點擊電子郵件內容中的釣魚 URL 後，就會進入憑證擷取網頁。

- 電子郵件主旨：DVLA:Action Needed：Update Your Billing Details(*需要採取行動：更新您的帳單資訊)。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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。

2025/04/25

與中國有關聯的威脅份子利用NFC技術進行詐騙活動

與中國有關的威脅份子正利用 NFC 技術針對全球金融機構進行詐騙活動，造成重大損失。Z-NFC 和 King NFC 等複雜的工具被用來進行非法交易。這些工具利用近場通訊 (NFC) 技術，而該技術對於依靠主機卡類比 (Host Card Emulation，HCE) 的非接觸式支付和應用程式來說是必不可少的。HCE 可讓網路罪犯在行動裝置上模擬實體 NFC 智慧卡，建立裝置農場以進行自動化詐騙。除此之外，攻擊者還會利用啟用 NFC 的 POS 終端機和酬賓計劃。NFC 支付的全球範圍，加上錢騾 (擁有許多人頭帳戶幫忙洗錢的服務) 和加密通訊管道所提供的匿名性，使得這些詐騙行為難以追查和瓦解。

網路知識：NFC 是英文「Near-Field Communication」的縮寫，中文稱為「近場通訊」或是「近距離無線通訊」，是一種能讓裝置在短距離內進行安全且非接觸式通訊的高頻無線通訊技術，可實現快速且有效的資料交換。

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 偵測到的惡意程式名稱及有效對應的防護機制：

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。

- AdLibrary:Generisk
- 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。

2025/04/24

AsyncRAT惡意軟體大量濫用Cloudflare隧道(Tunnel)服務來擴散攻擊

據報導，濫用 Cloudflare 隧道 (Tunnel) 服務部署 AsyncRAT 惡意軟體的攻擊行動正在上演。攻擊媒介從包含惡意 .ms-library 檔案的釣魚電子郵件引爆，當開啟此檔案時，會下載 PDF 捷徑 (LNK 檔案)，以引爆一系列的惡意腳本。這些腳本 (包括 Python、.vbs 和 .bat 檔案) 會將惡意有效酬載注入記事本程序，並下載隱藏在 base64-encoded.jpg 影像中的最終 AsyncRAT 有效酬載。與 C&C 伺服器之間的通訊透過動態 DNS 網域和 Cloudflare 通道進行。

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 偵測到的惡意程式名稱及有效對應的防護機制：

自適應防護技術(包含於SESC)：

- ACM.Ps-Http!g2
- ACM.Ps-Wscr!g1

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Scr.Mallibms!gen1
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Malimg
- 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。

2025/04/24

Ammyy Admin和PetitPotato惡意軟體常被被部署在鎖定MS-SQL Server的目標式攻擊中

鎖定管理不善的 MS-SQL 伺服器之目標式攻擊行動有日益增多的趨勢，目的是部署 Ammyy Admin 和 PetitPotato 惡意軟體，以進行遠端存取和權限升級。攻擊者利用易受攻擊的伺服器，執行指令收集系統資訊，並使用 WGet 安裝惡意軟體。他們還會啟用 RDP 服務，並新增使用者帳號以維持常駐能力及存取權限。

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 偵測到的惡意程式名稱及有效對應的防護機制：

VMware Carbon Black 產品的防護機制：

VMware Carbon Black 產品中既有政策就能阻止並檢測到相關的惡意指標。建議的基本政策是阻止所有類型的惡意軟體執行 (已知、可疑和垃圾程式)，並延遲雲掃描的執行，以便從 VMware Carbon Black Cloud 的信譽服務中獲得最大使用效益。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Hacktool.Gen
- Hacktool.Porttran
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!300
- Heur.AdvML.B
- 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。

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**。