保安資訊--本周(台灣時間2025/03/07)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 39 萬 3,500 台受保護端點上總共阻止了 4,730 萬次攻擊。這些攻擊中有 81.6% 在感染階段前就被有效阻止：**(2025/03/03)**

- 在**8萬2,600**台端點上，阻止了**1,730**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**9萬2,900**台端點上，阻止了**610**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬6,400**台**Windows**伺服主機上，阻止了**700**萬次攻擊。
- 在**5萬3,100**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,400**台端點上，阻止了**80萬6,900**次嘗試掃描在**CMS**漏洞。
- 在**4萬9,800**台端點上，阻止了**230**萬次嘗試利用的應用程式漏洞。
- 在**10萬7,800**台端點上，阻止了**230**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**73萬2,100**次加密貨幣挖礦攻擊。
- 在**11萬5,900**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**540**台端點上，阻止了**7萬6,800**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 15 萬 2,700 個受保護端點上阻止了總計 770 萬次攻擊。**(2025/03/03)**

- 使用網頁信譽情資，在 **145.9K** 個端點上阻止 **720** 萬次攻擊。
- 攔截 **18.8K** 個端點上 **331.7K** 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 **5.7K** 個端點上攔截 **133.3K** 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 **166** 個端點上攔截 **3.6K** 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。

2025/03/06

Desert Dexter網路攻擊行動，中東和北非攻擊事件不斷

Desert Dexter 是最近報告針對中東和北非使用者的網路攻擊行動代號。主使的威脅份子在合法檔案分享入口網站或透過看似無害的 Telegram 頻道散佈惡意之二進位檔案。惡意套件庫的連結則透過各種社交媒體平台進行宣傳。交付給受害者最終有效酬載是 AsyncRAT 惡意軟體的最新變種。植入惡意軟體具有從網頁瀏覽器竊取系統的敏感資訊、鍵盤側錄和加密貨幣錢包竊取等功能。

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
- ACM.Wscr-CNPE!g1
- ACM.Wscr-Ps!g1
- ACM.Wscr-Wscr!g1

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- AGR.Terminate!g5

- SONAR.SuspLaunch!g318
- SONAR.SuspLaunch!g483
- SONAR.SuspStart!gen21

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.ASync!gm
- CL.Downloader!gen96
- ISB.Downloader!gen60
- ISB.Downloader!gen68
- ISB.Downloader!gen173
- ISB.Downloader!gen348
- ISB.Houdini!gen6
- MSIL.Trojan!gen7
- Scr.Malcode!gdn14
- 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!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: Untrusted Telegram API Connection
- Web Attack: Webpulse Bad Reputation Domain Request

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。

2025/03/06

Njrat木馬最新變種涉入的攻擊行動，濫用微軟開發通道(Microsoft Dev Tunnels)充當C&C通訊

據報導，在真實網路情境發現 NjRAT 惡意程式的最新變種。NjRAT(也稱為 Bladabindi 或 Ratenjay) 是一種老當益壯還被廣泛使用的遠端存取木馬程式 (RAT)。此惡意軟體通常用來從已遭入侵的端點擷取資料、透過遠端 shell 傳送指令、竄改登錄檔機碼，以及下載額外的有效酬載。新發現的 NjRAT 最新變種，濫用 Microsoft Dev Tunnels 作為 C&C 通訊用途。Dev tunnels 是一種流行的服務，可讓開發人員透過網際網路安全地與他人分享本機網路服務。

網路上知識：開發通道可讓開發人員安全地跨因特網共用本機 Web 服務。可讓您將本機開發環境與雲端服務連線、與同事共用進行中的工作，或協助建置 Webhook。開發通道適用於臨機操作測試和開發，不適用於生產工作負載。

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-RgPst!g1
- ACM.Untrst-FlPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.SuspBeh!gen6
- SONAR.SuspBeh!gen22
- SONAR.SuspDrop!gen1
- SONAR.TCP!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：

- Backdoor.Ratenjay
- Scr.Malcode!gdn14
- Trojan.Gen.MBT
- 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

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。

2025/03/06

倍數成長～Medusa勒索軟體活動日益猖獗

Medusa 勒索軟體涉入的攻擊在 2023 年到 2024 年間躍升 42%。這種活動的增加持續升級，2025 年 1 月和 2 月觀察到的 Medusa 攻擊幾乎是 2024 年前兩個月的兩倍。據報導，Medusa 勒索軟體是由賽門鐵克威脅獵手團隊 (Threat Hunter Team) 所追蹤的 Spearwing 駭客團體所有，以駭客軟體即服務 (RaaS) 的方式運營。與大多數的勒索軟體操作者一樣，Spearwing 及其附屬組織會進行雙重勒索攻擊，在加密網路之前竊取受害者的資料，以增加受害者支付贖金的壓力。如果受害者拒絕支付贖金，該組織就會威脅要在其資料洩漏網站中公佈竊取的資料。

歡迎在我們的部落格中閱讀更多資訊：Medusa 勒索軟體活動日益猖獗。

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-Net!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-Sc!g1
- ACM.Ps-Wbadmin!g1
- ACM.Rcln-Lnch!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Wbadmin-DlBckp!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.RansomLckbit!g3
- SONAR.SuspDriver!g30
- SONAR.SuspDriver!g39
- SONAR.SuspDriver!g40
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g138
- SONAR.TCP!gen1
- SONAR.TCP!gen6

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：

- Downloader.Trojan
- FastReverseProxy
- Hacktool
- PUA.Gen.2
- Ransom.Medusa
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.9
- Trojan.Gen.MBT
- Trojan.KillAV
- Web.Reputation.1
- WS.Malware.1
- WS.SecurityRisk.3
- 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
- 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: Bad Reputation Application Activity
- System Infected: Trojan.Backdoor Activity 634

2025/03/05

全新駭客行動，正在磨刀霍霍鎖定網際網路服務商(ISP)的基礎架構大肆散播惡意竊密程式和挖礦程式

據報導，有新一波駭客行動，正在磨刀霍霍鎖定網際網路服務商 (ISP) 的基礎架構，散布惡意竊密程式和挖礦程式。在攻擊的初始階段，威脅者利用暴力攻擊來存取易受攻擊的環境。成功入侵後，他們會嘗試部署惡意竊密程式和 XMRig 挖礦程式的二進位檔案到目標。收集到的敏感資訊會在 Telegram API 的協助下外傳滲出。在他們的攻擊中，攻擊者還會利用許多網路掃描工具 (例如：masscan) 以及利用 Windows 遠端管理 (WINRM) 服務來執行 cmd/Powershell 指令碼。

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.Icacls-Lnch!g1
- ACM.Ps-Net!g1
- ACM.Ps-RgPst!g1
- ACM.Ps-SvcReg!g1
- ACM.Untrst-RunSys!g1

基於行為偵測技術(SONAR)的防護：

- SONAR.TCP!gen1
- SONAR.TCP!gen6

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
- PUA.Gen.2
- Trojan Horse
- 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!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。

2025/03/04
防護亮點：好工具總會淪為壞凶器～AutoIt如何遭惡意軟體濫用來發動網路攻擊自動化

AutoIt 是一種用於 Windows 圖形使用者介面和系統任務的自動化多功能腳本語言，在網路安全方面已成為一把雙面刃。雖然它為系統管理員和開發人員提供簡單和靈活的應用，但其功能已遭惡意使用者濫用來製造精密的惡意軟體，足以迴避傳統的安全機制。

AutoIt常遭濫用於惡意軟體攻擊行動

最近攻擊鏈揭露幾個惡名昭彰的惡意軟體家族已將 AutoIt 納入其作業中，包括但不限於：

- Formbook
- DarkGate
- Agent Tesla
- VipKeylogger
- MassLogger
- DarkCloud
- RedLine Stealer

這些威脅濫用 AutoIt 的腳本功能來混淆惡意程式碼，使偵測和分析變得更具挑戰性。

AutoIt作為惡意軟體載入程式

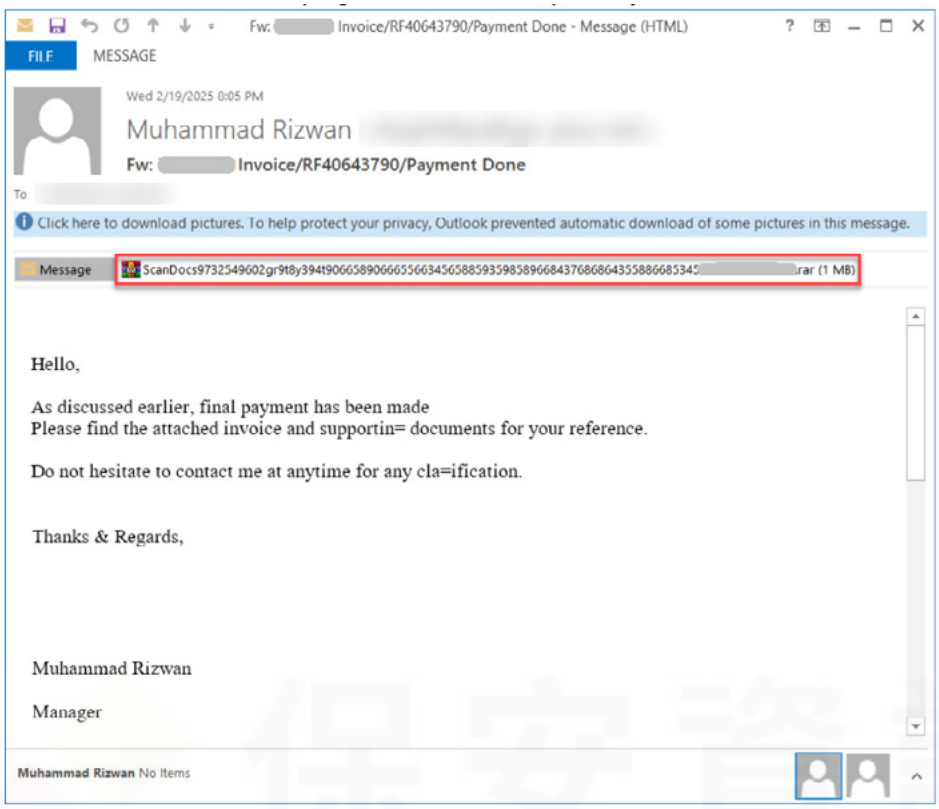
在 AutoIt 涉入的惡意軟體攻擊行動中，常見手法是使用 AutoIt 作為次要有效酬載的載入程式。攻擊者會在 AutoIt 腳本中嵌入加密 shellcode 和最終有效酬載，這些腳本可以是嵌入式字串，也可以從外部檔案載入。

以AutoIt運作載入程式的執行流程

1. 注入有效酬載：執行時，AutoIt 腳本會先將加密的有效酬載注入到系統之 TEMP 資料夾。
2. 執行 shellcode：然後腳本會解密 shellcode 並利用 Windows API 功能傳輸執行，如 ：
   - EnumWindows
   - CallWindowProcA
   - 透過 DllCallAddress 直接濫用 AutoIt API
3. 有效酬載解密與注入：shellcode 會讀取經加密的有效酬載檔案，並將其解密，然後將惡意程式碼注入 suspended 以及 hollowed processes，有效地繞過傳統檔案特徵的偵測機制。

透過利用 AutoIt 腳本的彈性和直接 API 呼叫，這些惡意軟體家族可以避開傳統的安全機制，同時在遭感染的系統中取得常駐／持久性。

DarkCloud 涉入之攻擊行動是濫用包含 AutoIt 可執行「載入程式」的電子郵件傳播



為了對抗這些不斷演進的威脅，我們開發了一系列偵測，專門針對 AutoIt 的惡意使用：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Trojan.Malautoit!g2
- Trojan.Malautoit!g3
- Trojan.Malautoit!g4
- Trojan.Malautoit!g5
- Trojan.Malautoit!g6
- Trojan.Malautoit!g7

基於行為偵測技術(SONAR)的防護：

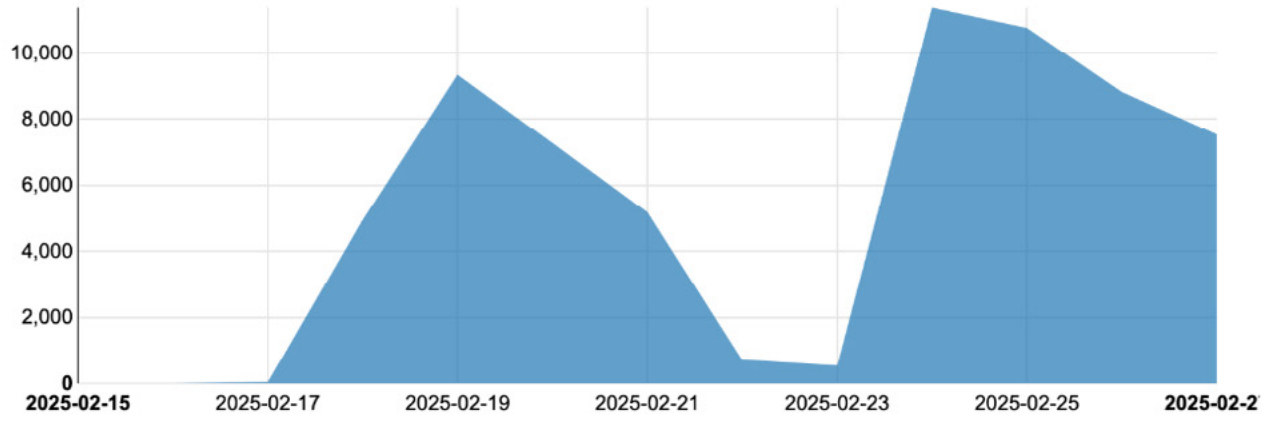
- SONAR.SuspLaunch!g529
- SONAR.SuspLaunch!g532

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：

- [33074] System Infected: Agent Tesla Infostealer Activity
- [33302] System Infected: Trojan Remcos Activity
- [33407] System Infected: Trojan.Formbook Activity 5
- [33471] System Infected: Redline Stealer Activity 2
- [34948] System Infected: Agent Tesla Infostealer Activity 2
- [34260] System Infected: Trojan.Backdoor Activity 757

最近的偵測到的濫用AutoIt 的惡意威脅數量



這些偵測主要在識別並攔截惡意 AutoIt 指令碼，針對利用此指令碼語言的威脅提供強大之防護。透過持續更新偵測功能和監控新出現的攻擊模式，我們可確保客戶免受濫用 AutoIt 的最新惡意軟體變種的攻擊。

儘管 AutoIt 對於合法的自動化任務而言仍是非常有價值的工具，但意識到其可能被濫用是非常重要的。佈署進階的安全措施並持續了解不斷演進的威脅，是保護系統免於惡意軟體濫用 AutoIt 功能的必要步驟。

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。
欲了解更多有關賽門鐵克端點安全入侵防護系統 (IPS) 的更多訊息，請點擊此處。
欲了解賽門鐵克行為安全性技術如何防禦就地取材攻擊的威脅，請點擊此處。

2025/03/03

Havoc惡意軟體透過網路釣魚行動散播

Fortinet 的研究人員在一份新報告中，詳述一起用來傳送 Havoc 惡意軟體的網路釣魚行動。Havoc 是一種惡意框架，類似 Cobalt Strike，被大肆濫用於網路攻擊行動。在這一起攻擊行動中，攻擊者利用多個元件，從一個 html 檔案開始，引誘接收者執行惡意的 PowerShell 指令。攻擊鏈的後續階段會從攻擊者控制的 SharePoint 網站進行多次下載，包括惡意 PowerShell 和 Python 指令碼，最後的 Havoc DLL 有效酬載。

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

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：

- Phish.Html
- 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

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。

2025/03/03

Danger、Loches--真實網路情境最近出現Globeimposter勒索軟體的兩種最新變種

Dange 和 Loches 是 Globeimposter 勒索軟體家族最近被發現的兩種最新變種。惡意軟體會加密使用者檔案，並分別在被加密的檔案冠上 .danger 或 .loches 副檔名。勒索 (贖金支付) 說明會以檔名「how_to_back_files.html」的 HTML 網頁檔形式注入在遭感染的機器上，並要求受害者聯絡攻擊者以取得進一步指示。Globeimposter 是一個問世很久的勒索軟體家族，活躍於威脅領域已有數年，已知會透過各種媒介散佈，包括網路釣魚和漏洞利用等。

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：

- Ransom.GlobeImposter
- 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

2025/03/03

GrassCall惡意軟體攻擊行動鎖定求職者散播惡意竊密程式

GrassCall 是最近被揭露歸屬於威脅組織 Crazy Evil 的網路攻擊行動代號。該攻擊以求職者為目標，利用假冒的面試散佈惡意竊密程式。攻擊者在 LinkedIn 或 CryptoJobsList 等知名網站宣傳假的工作機會。受害者被要求下載假冒的視訊會議軟體 GrassCall。根據受害者電腦的作業系統的不同，受害者會收到 Windows 或 macOS 平台上的 AMOS Stealer 版本。注入的有效籌載會嘗試滲出各種敏感資訊，包括加密貨幣錢包、憑證、驗證 cookies 等。最近報告顯示，攻擊者已進行到此活動新一輪攻擊，現在稱為 VibeCall 攻擊行動，並採用與先前攻擊行動極為相似的戰術、技巧和程序 (TTPs)。

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：

- OSX.Trojan.Gen
- 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。

2025/03/03

CVE-2024-12356--存在BeyondTrust特權遠端存取(Privileged Remote Access，PRA)、遠端支援(Remote Support，RS)系統的嚴重等級的命令注入漏洞

CVE-2024-12356 是存在 BeyondTrust 特權遠端存取 (Privileged Remote Access，PRA)、遠端支援 (Remote Support，RS) 系統的嚴重等級 (CVSS 風險評分：9.8) 的命令注入漏洞。如果遭成功開採濫用，此漏洞可能允許未認證的攻擊者注入以網站使用者身份執行的指令。此漏洞也隨著回報案例的增加，已於2024/12 被美國網路安全暨基礎設施安全局 (CISA) 列入「已遭成功開採濫用的高風險漏洞名單 (the Known Exploited Vulnerabilities Catalog-KEV)」中。

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：

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: BeyondTrust PRA and RS CVE-2024-12356

2025/03/02

散佈AsyncRAT惡意軟體的攻擊行動，利用惡意捷徑檔.LNK 和Null-AMSI工具

有人發現惡意軟體的攻擊行動使用偽裝成桌布的惡意捷徑檔 .LNK 來引誘被害者。作為攻擊媒介的一部分，開放程式碼的 Null-AMSI 工具被用來繞過惡意軟體掃描介面 (AMSI) 和 Windows 事件追蹤 (ETW)。使用經混淆的 PowerShell 腳本連線至遠端伺服器，並下載 gzip 壓縮的有效酬載，以逃避偵測。最終的有效酬載透過 .NET 的反射機制 (reflection載) 入記憶體，使 AsyncRAT 能夠執行遠端控制。

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

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!gen20
- Trojan.Gen.2
- WS.SecurityRisk.4

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: Suspicious Process Accessing Lets Encrypt Certified Site

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。

2025/03/02

攻擊者以查稅為誘餌散佈Winos4.0惡意軟體

威脅組織已利用 Winos4.0 惡意軟體框架對目標受害者發動攻擊。在 Fortinet 最近一份報告中，他們概述針對台灣使用者的攻擊，利用稅務相關的誘餌散佈 Winos4.0 惡意軟體。該攻擊利用 PDF 附件與 zip 檔案，其中包含惡意 DLL 與 shellcode 元件，以及從 C&C 下載其他惡意模組。

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

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：

- Scr.Malcode!gen
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Pidief
- 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!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。

2025/03/02

養成好習慣～下載軟體務必到原廠網站：冒牌的瀏覽器更新程式透過惡意重導來散播

安全研究人員觀察到最近惡意軟體攻擊行動利用網頁型的惡意軟體，透過遭入侵的網站來散佈，而非僅依賴電子郵件類型的攻擊來散佈惡意連結。這些攻擊是透過遭入侵的網站散佈，並注入惡意重導向到冒牌的瀏覽器「更新」頁面。如果使用者點擊更新連結，就會根據使用者的作業系統和位置傳送不同的有效酬載，傳送的惡意軟體包括 Windows 的 Lumma Stealer、Android 的 Marcher 和 Mac 的 FrigidStealer。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- OSX.Trojan.Gen
- OSX.Trojan.Gen.2
- Trojan.Gen.MBT
- 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：

- Malicious Site: Malicious Domain Request 21
- Malicious Site: Malicious Domain Request 22

基於機器學習的防禦技術：

- Heur.AdvML.C

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**。