保安資訊--本周(台灣時間2025/01/10)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 32 萬 3,400 台受保護端點上總共阻止了 4,120 萬次攻擊。這些攻擊中有 78.6% 在感染階段前就被有效阻止：**(2025/01/06)**

- 在**7萬2,900**台端點上，阻止了**1300**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**8萬6,000**台端點上，阻止了**590**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬5,600**台**Windows**伺服主機上，阻止了**6萬1,000**次攻擊。
- 在**4萬6,100**台端點上，阻止了**180**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,400**台端點上，阻止了**83萬800**次嘗試掃描在**CMS**漏洞。
- 在**4萬4,400**台端點上，阻止了**220**萬次嘗試利用的應用程式漏洞。
- 在**7萬2,600**台端點上，阻止了**150**萬次試圖將用戶重定向到攻擊者控制的網站攻擊。
- 在**2,200**台端點上，阻止了**89萬700**次加密貨幣挖礦攻擊。
- 在**8萬5,300**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**448**台端點上，阻止了**7萬6,200**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 10 萬 7,700 個受保護端點上阻止了總計 450 萬次攻擊。**(2025/01/06)**

- 使用網頁信譽情資，在 **102.7K** 個端點上阻止 **400** 萬次攻擊。
- 攔截 **13.4K** 個端點上 **237.6K** 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 **5.1K** 個端點上攔截 **180K** 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 **138** 個端點上攔截 **2.9K** 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。

2025/01/10

LDAP漏洞的概念性驗證(PoC)攻擊程式碼，其實就是惡意竊密程式

CVE-2024-49113 是一個存在 Microsoft Windows 輕量級目錄存取通訊協定 (LDAP) 的漏洞，已於 12 月釋出修補程式。在最近的攻擊行動中，有人觀察到攻擊者散佈偽裝為此漏洞的概念驗證 (PoC) 程式碼的惡意竊密程式。冒名偽造漏洞的概念驗證 (PoC) 程式碼之功用其實惡意程式的注入或下載的腳本，透過 FTP 來竊取系統資訊。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- 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：

- Trojan Horse
- 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。

2025/01/10

CVE-2024-55550--存在加拿大電信業者Mitel的MiCollab整合通訊平臺的路徑穿越漏洞

CVE-2024-55550 是一個新被揭露的路徑遍歷漏洞，會影響加拿大電信業者 Mitel的MiCollab 整合通訊平臺 9.8 SP1 FP2 及更舊的版本。由於輸入識別不足，如果被開採濫用，此漏洞可能會允許已驗證攻擊者在有漏洞的實體上擁有管理權限和本機檔案讀取存取權限。此漏洞也隨著回報案例的增加，已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：

基於安全強化政策(適用於使用DCS)：

賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就內建的系統鎖定政策，可以保護底層的作業系統免受此漏洞的侵擾，包括防止執行任意命令和限制查看關鍵的作業系統檔案。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/01/10

Banshee惡意竊密程式新出現macOS平台的版本

在真實網路情境上新發現 Banshee 惡意竊密程式已出現 macOS 平台的版本。根據 Checkpoint 發表的報告，後繼新增平台上的變種採用與 Apple MacOS XProtect 防毒引擎相同的字串加密演算法。該惡意軟體透過惡意的 Github 頁面散佈，這些頁面也會將 Lumma 惡意竊密程式散佈給 Windows 使用者。Banshee 惡意竊密程式的為害性是從受感染的端點收集和滲出各種機密資料，包括系統資訊、憑證、加密貨幣錢包、雙重認證 (2FA) 擴充套件相關的資訊等。

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：

自適應防護技術(包含於SESC)：

- ACM.Ps-Java!g1

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

基於行為偵測技術(SONAR)的防護：

- 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：

- OSX.Trojan.Gen
- Scr.Malcode!gdn32
- Trojan Horse
- 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。

2025/01/09

雙重勒索的勒索軟體正當紅：Funksec勒索軟體浮出檯面

Funksec (也稱為 Funklocker) 是另一款於 2024 年底出現的雙重勒索的勒索軟體，據稱已有多個組織成為受害者。

當電腦遭成功入侵後，被加密的檔案會被冠上「.funksec」副檔名，並將桌面背景變更為遠端網頁的影像。它透過建立名為「funksec」的排程工作來建立持久性，並嘗試停用 Windows Defender 的即時監控。此威脅會清除事件日誌、偵測虛擬環境以在發現時中止作業，並終止許多程序，包括瀏覽器、生產力工具和媒體應用程式。

其勒索 (贖金支付) 說明檔 (README-[randomcharacters].md) 會被存放在多個目錄中。它會告知受害者他們的組織已被滲透，他們的檔案已被 Funksec 勒索軟體加密。它明確警告不要篡改加密檔案、聯繫執法部門或試圖追蹤攻擊者。攻擊者宣稱他們的勒索軟體非常先進，任何防毒軟體都無法還原檔案，並威脅如果不支付贖金，就會公開洩露竊取的資料。他們要求將 0.1 比特幣 (BTC) 傳送至指定的比特幣錢包，並提供如何購買比特幣的詳細指令、從「getsession.org」安裝會話，以及使用 ID 取得解密程式的詳細說明。該威脅組織自吹自己非常老練，專門取得政府機構的存取權、攻擊資料庫和毀壞裝置。

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.SuspLaunch!gen4
- SONAR.SuspLaunch!g18
- SONAR.SuspLaunch!g253

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.Funk

2025/01/09

借力Skuld惡意竊密程式萃取機敏資料的功能，新版HexaLocker勒索軟體正在發動更精準的雙重勒索攻擊

在真實網路情境上發現改用 Go 語言撰寫 HexaLocker 勒索軟體的後繼新版本。該新變種具有下載 Skuld 惡意竊密程式的新增功能，主要目的是從受感染的端點收集機敏資料。所收集的資訊可能包括儲存在網頁瀏覽器中的資料、cookies、銀行詳細資料、瀏覽歷史、憑證等。該攻擊鏈遵循惡名昭彰的雙重勒索手法，首先收集並萃取敏感資料，然後才進行檔案加密。被加密的檔案會被冠上「.HexaLockerV2」的副檔名，並留下勒索 (贖金支付) 說明檔，要求受害者透過 Telegram 或 Web Chat 與威脅者聯繫。

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
- WS.Malware.1

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。

2025/01/09

CVE-2025-0282--存在Ivanti Connect Secure漏洞被大肆開採濫用於發動零時差攻擊

CVE-2025-0282 是一個新揭露的嚴重等級 (CVSS 風險評分：9.0分) 緩衝區溢位漏洞，會影響 Ivanti Connect Secure。若被成功開採濫用，未經身分驗證之攻擊者可在受影響的機器上執行任意程式碼 (RCE)。原廠已在 Ivanti Connect Secure 韌體版本 22.7R2.5 中解決此漏洞。根據最新報告，此漏洞已在散佈 SPAWN、DRYHOOK 和 PHASEJAM 惡意軟體系列惡意有效酬載的零時差攻擊中被大肆開採濫用。此漏洞也隨著回報案例增加，已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。

網路上的知識：Ivanti Connect Secure 提供高安全性、專門設計為用於遠端辦公或是移動設備 SSL VPN 解決方案，使用者從任何支援網際網路的設備連接到公司資源--隨時隨地。Ivanti Connect Secure 是廣泛佈署於企業組織 SSL VPN，適用各種行業。

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.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 其出廠就內建的強化政策，可防止惡意軟體在系統上植入或執行。DCS 可以保護 Linux 伺服器防止從暫存檔案或其他可寫入位置執行惡意軟體 (如本案例中：DRYHOOK 和 PHASEJAM)，這是惡意軟體中使用的一種技術。
- 預設的防禦政策也會阻止停用 SELinux、修改 syslog 屬性或掛載／卸載磁碟機，這些都是此攻擊中使用的技術。
- 經 DCS 安全強化過的 Linux 伺服器會鎖定管理員帳號，因此可以防止任何權限提升 (提權)。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/01/08

三、四年前已揭露的老舊Oracle WebLogic Deserialization漏洞(CVE-2020-2883)還頻頻傳出該漏洞被開採濫用

CVE-2020-2883 是一個早在 2020 年就被揭露的反序列化漏洞，會影響未修補的 Oracle WebLogic 伺服器。如果被成功開採濫用，則未經認證的攻擊者可透過特訂之 T3 連接埠網路請求，遠端執行程式碼 (RCE)。儘管這個漏洞相對較舊，此漏洞也隨著回報案例的增加，在本周已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: Oracle Weblogic Server RCE CVE-2020-2883

基於安全強化政策(適用於使用DCS)：

- 賽門鐵克的重要主機防護系統：DCS～Data Center Security 其出廠就內建的系統鎖定政策可保護底層作業系統伺服器免受此漏洞攻擊，包括防止執行任意指令，以及限制讀取重要作業系統檔案的存取權限。
- DCS 預設防禦政策透過封鎖所有入埠和離埠連線，防止攻擊者存取有漏洞的系統。

更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/01/07

XWorm惡意程式涉入中東的網路攻擊行動：假冒以色列情報機構Mossad的情報報告作為誘餌

由於中東地區的緊張局勢持續高漲，尤其是最近在敘利亞發生的事件後，威脅份子正利用動盪的局勢，以區域內及全球的組織和個人為目標，利用敏感情報的誘惑來引誘受害者。

最近一個範例涉及威脅份子利用洩露虛構的以色列國家情報機構 Mossad 之情報報告來引誘使用者。該惡意壓縮檔名為 Mossad.rar，內含兩個具傷害性的檔案--JavaScript (JS) 檔案和批次 (BAT) 檔案--將自己偽裝成合法文件。

- قمئاق أسامء تايصخش السوريه - ليبيا.js (敘利亞名人名單--Libya.js)
  ريرقت السرم لا - اسوم لا د.bat (洩密報告--Mossad.bat)

惡意檔案的目的是欺騙使用者，讓他們以為正在存取敏感的情報資訊，並利用以色列國家情報機構 Mossad 的名稱來提高可信度，引誘受害者。

此攻擊展現一個複雜的多階段攻擊鏈。一開始，它會執行擷取惡意 JPG 的檔案，觸發 PowerShell 來啟動進一步的動作。執行後，它會終止數個合法的程序，包括與 CCleanerBrowser.exe、MSBuild.exe 和 aspnet_compiler.exe 等系統公用程式相關的程序，以破壞系統防護。它還會從 C:\ProgramData\WindowsHost 和 C:\Users\Public 等目錄中刪除帶有 .bat、.ps1 和 .vbs 副檔名的文件。惡意程式會在這些位置建立新檔案，包括依序運作的 QIJGHURIURNY.bat、VVHUPYEWODP.vbs 和 ORFWDFDJWS.ps1。

為了維持持久性 (常駐能力)，會修改目前使用者的登錄機碼，將 Windows 啟動資料夾路徑重導向至 C:\ProgramData\WindowsHost。腳本執行流程包括執行新建立的 VBS 檔案，此檔案會觸發批次腳本，並最終執行 PowerShell 腳本。此指令碼會收集系統資訊，例如：裝置 ID、HWID、外部 IP、使用者名稱、防毒軟體的詳細資訊，並擷取螢幕截圖，儲存為 %Temp%\screenshot.png。收集到之資料會使用特定的 BotToken 和 ChatID 傳送至 Telegram 機器人，利用 Telegram 作為外洩途徑。

在後續階段，PowerShell 腳本 ORFWDFDJWS.ps1 會嘗試將遠端存取木馬程式 Xworm 注入 aspnet_compiler.exe 程序。此威脅會與其命令與控制 (C&C) 伺服器建立通訊，以啟用遠端桌面存取、鍵盤側錄、持久化 (常駐能力) 及資料外洩等功能。

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：

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.ASync!gm
- CL.Downloader!gen4
- ISB.Downloader!gen60
- ISB.Downloader!gen173
- Trojan Horse

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

2025/01/07
防護亮點：賽門鐵克雲端沙箱(Synic)讓Carbon Black防護能力如虎添翼

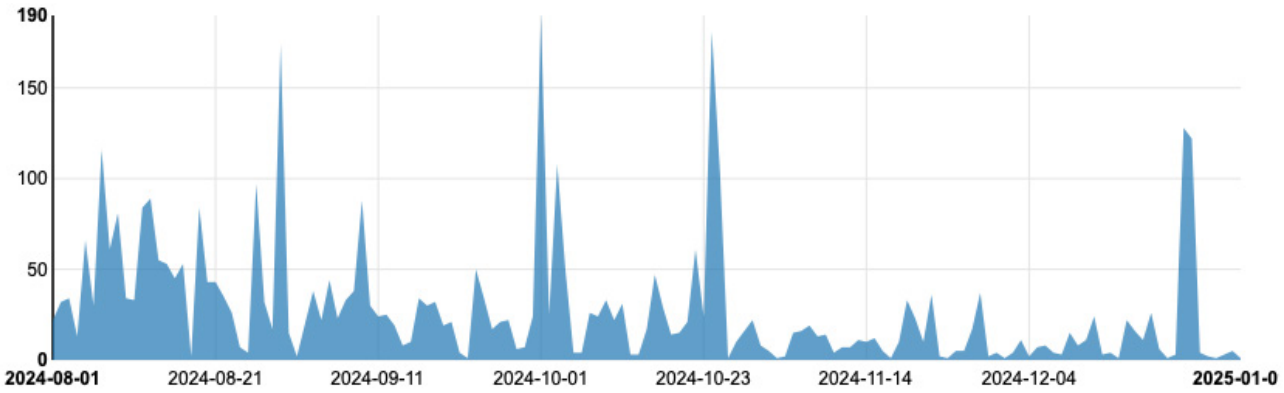
賽門鐵克雲端沙箱讓 Carbon Black如虎添翼

2024 年 7 月，Carbon Black 轉換至 Symantec Cloud Sandbox 服務，以協助識別和封鎖受保護端點上的惡意檔案。在啟用「提交未知二進位檔進行分析」功能的情況下，標示為沙箱分析的檔案會提交到賽門鐵克雲端沙箱 (又稱 Cynic)。

賽門鐵克雲端沙箱會在可被用來攻擊的環境中執行檔案，在此環境中會模仿終端使用者的行為，以觸發可疑惡意軟體的潛在惡意動作或活動。雲端沙箱會匯集整理系統事件資訊、監控網路流量，並利用賽門鐵克全球資安威脅情資網路 (GIN) 和領先業界的賽門鐵克完整防護架構，包括沙箱情境的專用引擎和內容，來判定檔案是否為惡意。

影響

賽門鐵克雲端沙箱(Synic)在 2024 年 8 月至 12 月期間，發現 Carbon Black 端點上傳超過 4000 個獨特的惡意檔案。



賽門鐵克雲端沙箱能偵測並封鎖包括下列各種威脅及其後續變種的零時差封鎖：

- 勒索軟體，例如：Abyss Locker、Lazy Ransomware、fragtor Ransomware
- 惡意竊密程式，包括 RedCap 和 Lumma
- 殭屍網路，例如：Strictor

兩種偵測途徑

賽門鐵克雲端沙箱提供兩種偵測途徑，一種是透過增強型的靜態分析和模擬的快速途徑，另一種是透過檔案執行和行為分析的慢速途徑。

沙箱服務收到所有檔案都會經過這兩個途徑，但是 Carbon Black 客戶可以因此受益，因為如果我們透過快速途徑進行早期處理，他們可以在 <1 秒內獲得處理結果。在此期間，95% 的惡意判決都是透過我們的快速途徑功能提供。這會是一個內嵌區塊。

一旦檔案被賽門鐵克雲端沙箱 (Cynic) 識別為惡意，所有沙箱用戶隨即都會受益於已知的處理方式，而所有賽門鐵克和 Carbon Black 客戶則會在幾分鐘內受益，因為所有產品都會使用我們的全球資安情資網路 (GIN-Global Intelligence Network)。

欲獲得更多、更詳盡的賽門鐵克--雲端沙箱分析引擎 (Cynic)，請點擊此處。
欲了解如何在 Carbon Black Cloud 啟用賽門鐵克雲端沙箱，請點擊此處。

2025/01/06

出現全新的手機／行動裝置的惡意軟體：FireScam

FireScam 是最近在真實網路情境上發現的手機／行動裝置之惡意軟體。該惡意軟體透過釣魚網站並偽裝為 Telegram Premium 手機 APP 散佈。功能方面，FireScam 具備廣泛的資料竊取能力，包括從剪貼簿、自動填入表單、儲存的電話訊息、通知、進行的金融交易等擷取資料。惡意軟體也可能用於在受感染的裝置上下載和執行任意的有效酬載。據觀察，FireScam 會濫用 Firebase 即時資料庫來滲透竊取的資訊。

網路釣客的手法多如牛毛，從雲端服務到社交工程，使其騙術更具說服力。在雲端服務中，谷歌的 Firebase 因其易用性、免費、可擴展性和網域定制功能而被廣泛濫用。這些特性使其成為一個吸引網路釣客的平臺，他們只需花費最少的精力和成本就能上架和傳播詐騙內容。

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。

- 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。

2025/01/05

KGB鍵盤側錄軟體涉入假冒俄羅斯政府電子郵件的企業攻擊行動

在 2024 年 12 月下旬，有攻擊者針對企業發出惡意電子郵件，假冒俄羅斯聯邦工業和貿易部 (Минпромторг России)的社交工程伎倆，以及使用惡意 .scr 檔案 (Письмо в МНТЦ и ЦРП.scr)，誘騙使用者。

當被執行時，惡意 .scr 檔案會模擬合法的 PDF 讀取程式，並顯示一份看起來是俄羅斯政府

官方格式的文件。該文件似乎來自俄羅斯聯邦工業和貿易部 (Минпромторг России)，具有徽章、正式標題和聯絡資訊。它提到 ISTC(國際科學技術中心) 和一家專門從事工業自動化的俄羅斯公司。這份假文件討論的是技術主題，包括專用設備的使用以及與工業組織的合作。

在受害者不知情的情況下，它還會啟動一系列有害的動作，以建立持久性 (常駐能力)、滲出資料並危及系統。一開始，它會在 C:\Intel 下建立一個資料夾，並在其中放置兩個初始檔案：rezet.cmd 和 down.exe，後者的功能類似 curl。使用此檔案，它會繼續從惡意託管網站下載多個附加檔案。這些檔案包括自訂的 7zip 工具 (driver.exe)、一個包含 blat.exe (合法的命令列電子郵件用戶端) 和 wbpv.exe (PasswordRevealer) 的壓縮檔 (pas.rar) 以及另一個包含 go.exe 和 userprofile.exe (KGB 鍵盤側錄軟體) 的壓縮檔 (keys.rar)。其他的下載包括遠端桌面應用程式 AnyDesk(AnyDesk.exe) 的修改版本，以及包含合法公用程式 Tray Minimizer 的壓縮檔 (Trays.rar)。

惡意軟體透過修改 Windows 登錄檔的機碼來建立持久性，在 HKEY_CURRENT_USER\Microsoft\Windows\CurrentVersion\Run 下新增項目。這些項目會確保 userprofile.exe 和 go.exe 在系統啟動時執行。它會進一步從同一惡意網站下載另一個有效酬載 MPK.rar 到 %PROGRAMDATA%，用更新的元件更新惡意軟體。

一旦執行，惡意軟體會掃描系統的 C:、D: 和 E: 磁碟，搜尋與 Telegram Messenger 相關的檔案和資料。收集到的資料會暫存在 C:\Intel 資料夾中，並隨後透過電子郵件發送給外部收件人，進而實現敏感資訊的外洩。與此同時，惡意軟體會執行 KGB 來啟動鍵盤側錄，而被修改過的 AnyDesk 遠端連線程式則被用於遠端存取遭入侵的系統。

為了鞏固其立足點，惡意軟體會更改系統的電源設定，以停用筆電機蓋閉合的電源動作並消除待機和休眠逾時，確保不間斷的運作。它還會建立兩個排程工作：一個是每天凌晨 5:00 關閉電腦，另一個是每天凌晨 1:00 啟動 Microsoft Edge。最後，為了確保所有元件都已正確被設定，惡意軟體會重新啟動系統，完成所有攻擊鏈，讓受害者的裝置毫無招架能力。

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-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Untrst-RLsass!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：

- PasswordRevealer
- Spyware.KGBSpy
- Trojan.Gen.MBT
- Trojan Horse

基於機器學習的防禦技術：

- 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: AnyDesk Remote Desktop Activity
- Audit: Bad Reputation Application 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。

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**。