保安資訊--本周(台灣時間2025/06/13)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 34 萬 4,260 台受保護端點上總共阻止了 5,330 萬次攻擊。這些攻擊中有 83.7% 在感染階段前就被有效阻止：**(2025/06/08)**

- 在**8萬1,600**台端點上，阻止了**2,470**萬次嘗試掃描**Web**伺服器的漏洞。
- 在**7萬5,400**台端點上，阻止了**560**萬次嘗試利用的**Windows**作業系統漏洞的攻擊。
- 在**2萬2,500**台**Windows**伺服主機上，阻止了**590**萬次攻擊。
- 在**4萬9,900**台端點上，阻止了**190**萬次嘗試掃描伺服器漏洞。
- 在**1萬2,600**台端點上，阻止了**84萬7,500**次嘗試掃描在**CMS**漏洞。
- 在**4萬2,800**台端點上，阻止了**180**萬次嘗試利用的應用程式漏洞。
- 在**6萬8,600**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**894**台端點上，阻止了**66萬5,700**次加密貨幣挖礦攻擊。
- 在**12萬4,100**台端點上，阻止了**800**萬台次向惡意軟體**C&C**連線的嘗試。
- 在**457**台端點上，阻止了**6萬1,100**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 900 個受保護端點上阻止了總計 750 萬次攻擊。**(2025/06/09)**

- 使用網頁信譽情資，在 **154.9K** 個端點上阻止 **710** 萬次攻擊。
- 攔截 **17K** 個端點上 **244.3K** 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 **4.4K** 個端點上攔截 **118.7K** 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 **173** 個端點上攔截 **1.8K** 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。

2025/06/13

CVE-2025-4123--存在資料圖形視覺化Grafana系統的跨網站指令碼(XSS)和伺服器偽造請求(SSRF)漏洞

CVE-2025-4123 是最近發現存在資料圖形視覺化 Grafana 系統的一個嚴重等級 (CVSS 風險評分：7.6) 開放重導向漏洞。成功開採濫用此漏洞可讓遠端攻擊者將用戶重導向至託管任意外掛的惡意網址。這些外掛可能反過來導致 JavaScript 執行，造成伺服器端請求偽造 (SSRF) 或透過跨網站指令碼 (XSS) 導致帳戶被接管。原廠已針對此漏洞推出修補軟體版本。

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: Grafana XSS Attempt CVE-2025-4123

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 的 UNIX 版本，預設的強化沙箱和應用程式自訂沙箱，可保護受影響應用程式的底層作業系統資源，並防止威脅者使用多種技術來讀取／寫入任意檔案或執行任意程式碼。更詳細的 DCS 資訊與工作原理，請下載 DCS 解決方案說明。

2025/06/12
CyberEye遠端存取木馬(RAT)

CyberEye 是一款模組化遠端存取木馬程式，其 C&C 通訊依賴 Telegram。使用公開可用的建置程式，可自訂其植入物件，包含反分析、加密貨幣劫持和持久性等功能。建置程式還可針對憑證、信用卡和通訊應用程式，進行廣泛的資料外洩。雖然這些功能都不是獨一無二，但卻讓 CyberEye 成為能達成各種目標的多用途遠端存取木馬 (RAT)。

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.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.Trojan
- Scr.Malcode!gen
- Trojan Horse
- WS.Malware.2
- WS.Reputation.1

基於機器學習的防禦技術：

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

2025/06/12
Spectra勒索軟體

Spectra 是今年才在真實網路情境裡被發現的全新勒索軟體變種。該惡意軟體屬於已知的 Chaos 勒索軟體家族。它會加密用戶資料，並在被加密的檔案冠上隨機副檔名。勒索贖金支付通知是以檔名為「SPECTRARANSOMWARE.txt」的文字檔提出，攻擊者要求以比特幣 (Bitcoin) 支付贖金。他們還威脅受害者，如果不乖乖就範付贖金，就會公開被盜資料，因此採用了雙重勒索策略。Spectra 勒索軟體具有停止各種備份服務、刪除磁碟區陰影複本或停用系統監控工具等功能。該勒索軟體還會變更被攻擊端點的桌面背景。

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.Dropper
- SONAR.SuspBeh.C!gen18
- SONAR.SuspDrop!gen1
- SONAR.SuspLaunch!g22

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.Zombie
- 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

2025/06/12

進階持續威脅(APT)駭客集團：Stealth Falcon利用存在WebDAV資料夾的遠端程式碼執行(RCE)漏洞：CVE-2025-33053

據 Check Point 報導，進階持續威脅 (APT) 駭客集團：Stealth Falcon 在新發動的惡意軟體攻擊行動中被觀察到利用存在 WebDAV 資料夾的遠端程式碼執行 (RCE) 漏洞：CVE-2025-33053。威脅者透過 .url 檔案開採濫用此漏洞，執行其控制下 WebDAV 伺服器上託管的惡意軟體。此漏洞允許透過工作目錄執行遠端程式碼，微軟已修補此漏洞。

Stealth Falcon 主要針對中東和非洲的政府及國防部門，採用魚叉式網路釣魚電子郵件，其中包含惡意連結或附件。這些攻擊行動利用 WebDAV 和內建系統工具來傳送惡意軟體，包括在開放原始碼紅隊框架 Mythic 上建立的客製植入程式。Horus Agent 等植入程式在設計上採用迴避技術來抵抗分析與偵測，它們會先驗證目標環境，然後再部署更先進的有效酬載。

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。

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.Upatre
- Exp.CVE-2025-33053
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1

基於機器學習的防禦技術：

- Heur.AdvML.A!500
- Heur.AdvML.A
- 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。

2025/06/12

不尋常的Fog勒索軟體活動

在最近一份報告中，賽門鐵克與 Carbon Black 的威脅獵手團隊分析針對亞洲一家金融機構的 Fog 勒索軟體攻擊。該攻擊因使用 Syteca 等合法軟體和開放源碼的滲透測試工具而脫穎而出。此外，攻擊者在受害者的環境中建立持久性，這對於以財務為動機、通常不需要長期網路存取的勒索軟體團體而言，是非常不尋常的策略。

請參閱我們的部落格：Fog勒索軟體：近期攻擊中使用的不尋常工具集。

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
- Hacktool.Stowaway

- Ransom.Gen
- 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
- 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。

2025/06/12

駭客組織FIN6假借求職名義濫用網路求職社群入口網站和雲端基礎架構來逃避偵測

有人在真實網路情境裡發現到由駭客組織 FIN6 所發起的惡意軟體攻擊行動，該攻擊行動假裝 LinkedIn 和 Indeed 等平台上的求職者。一旦目標被誘騙，威脅者就會傳送含有無法點選的網頁的網路釣魚電子郵件，這些網頁會指向 AWS 上雲端託管的「履歷」網站。這些網站使用圖靈 (CAPTCHA) 驗證機制來逃避偵測，並最終傳送包含惡意 .LNK 捷徑檔案的 ZIP 壓縮檔。當開啟此捷徑檔案時，會觸發 JavaScript 的惡意程式下載器安裝隱匿的 More_eggs 後門。該後門能夠竊取憑證、執行遠端指令和部署額外的有效酬載。

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
- ACM.Wmip-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：

- Trojan Horse
- Trojan.Gen.NPE
- 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：

- 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。

2025/06/11

中國駭客組織鎖定網路安全供應商為目標

根據 SentinelLabs 最近一份報告，由中國支持的威脅份子在全球攻擊行動中部署 ShadowPad 和 PurpleHaze 惡意軟體。這些攻擊的目標涵蓋各行各業，從金融、政府到製造業，甚至包括試圖攻擊 SentinelOne 本身。

該駭客組織使用 ShadowPad 惡意軟體其特點是 PowerShell 腳本、資料外洩，以及透過遠端存取架構建立指揮與控制 (C&C)。PurpleHaze 惡意軟體具有明顯的跨平台性，可影響 Windows 和 Linux 系統。在 Windows 上，攻擊者使用 DLL 側載來啟動惡意軟體。在這兩種作業系統上，攻擊者都建立 C&C 連線，並部署 GoReShell 變種，以透過反向 shells 取得持續存取權／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.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。

檔案型(基於回應式樣本的病毒定義檔)防護：

- Backdoor.Cobalt
- Linux.Mirai
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.2
- WS.Malware.1

- WS.Malware.2

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
- 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。

2025/06/11

Myth惡竊密軟體

Myth 是最近在真實網路情境裡新發現一種基於 Rust 的全新惡竊密軟體。此惡意軟體前一陣子曾在多個 Telegram 群組中進行廣告，最近則被回報其透過詐騙遊戲網站和提供軟體破解版的線上入口網站等散佈。Myth 惡竊密軟體具有從遭入侵的主機收集各種敏感資訊的功能，包括基於 Gecko 和 Chromium 的瀏覽器資料、cookie、自動填入資訊、憑證、銀行資料、螢幕擷取、剪貼簿內容等。收集到的資訊會壓縮成 .zip 檔案，並轉送到攻擊者控制的 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：

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：

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

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: 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。

2025/06/11

存在開源資安平臺Wazuh的嚴重等級漏洞：CVE-2025-24016遭開採濫用於散佈Mirai殭屍網路

據報導，有全新散佈 Mirai 殭屍網路的網路惡意行動正在真實網路情境裡爆發。攻擊者利用存在開源資安平臺 Wazuh 的嚴重等級漏洞：CVE-2025-24016(CVSS 風險評分：9.9)，可能在有漏洞的裝置上執行遠端程式碼。此漏洞已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。名為「morte」和「resbot」的分散式 Mirai 殭屍網路變種支援不同的架構，包括 Arm、MIPS、i686 及其他。

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：

- Linux.Gafgyt
- Linux.Mirai
- Linux.Mirai!g2
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.NPE
- WS.Malware.1
- WS.SecurityRisk.4

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 ，預設鎖定政策就可保護底層伺服器免受 CVE-2025-24016 漏洞攻擊，包括防止執行任意指令和限制存取關鍵作業系統

檔案的讀取。

- DCS 的網路規則政策可設定為，將應用程式限制為受信任的用戶端。

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。

2025/06/10
防護亮點：無懈可擊的組合～賽門鐵克行為分析--SONAR＋賽門鐵克雲端沙箱--Cynic

行為分析

行為分析是當應用程式在電腦上執行時，偵測潛在惡意行為的即時防護。賽門鐵克的行為分析使用啟發式方法和信譽資料來偵測新興和未知的威脅。它提供「零時差」保護，因為它能在傳統病毒和間諜軟體偵測定義建立之前偵測到惡意行為，以解決威脅。行為分析使用啟發式系統，利用賽門鐵克的線上情報網路與用戶端電腦上的主動本機監控來偵測新興威脅。它也會偵測用戶端電腦上應受監控的變更或行為。

賽門鐵克行為分析-SONAR(Symantec Online Network for Advanced Response)

賽門鐵克的行為分析技術 (簡稱「SONAR」) 會持續監控所有程序，不論是否受信任。它會追蹤檔案、登錄、進程、服務、注入線程、DLL 側載和進程空洞化等複雜的攻擊鏈。它還會追蹤攻擊鏈中合法進程的使用情況。這些包括就地取材 (LOTL) 程序和兩用工具。一旦識別出惡意載體，SONAR 會移除惡意檔案、登錄項目和進程，並終止攻擊中使用的任何 LOTL 和兩用進程，進而解除整個攻擊鏈。

賽門鐵克雲端沙箱-Cynic

我們以雲端為基礎的沙箱分析平台 (稱為「Cynic」非常貼切)，利用 SONAR 行為偵測為賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 提供攔截能力，在目標攻擊進入收件匣之前就被偵測出來。

目標式 (有針對性的) 攻擊通常會從精心製作的釣魚電子郵件開始，誘導使用者開啟附件，而使用者並不知道附件會在背景中隱匿進行的複雜攻擊足以癱瘓整個網路。偵測這些攻擊最可靠的方法之一，就是監控完整的攻擊鏈，並在一連串行為被識別為惡意攻擊時啟動偵測。

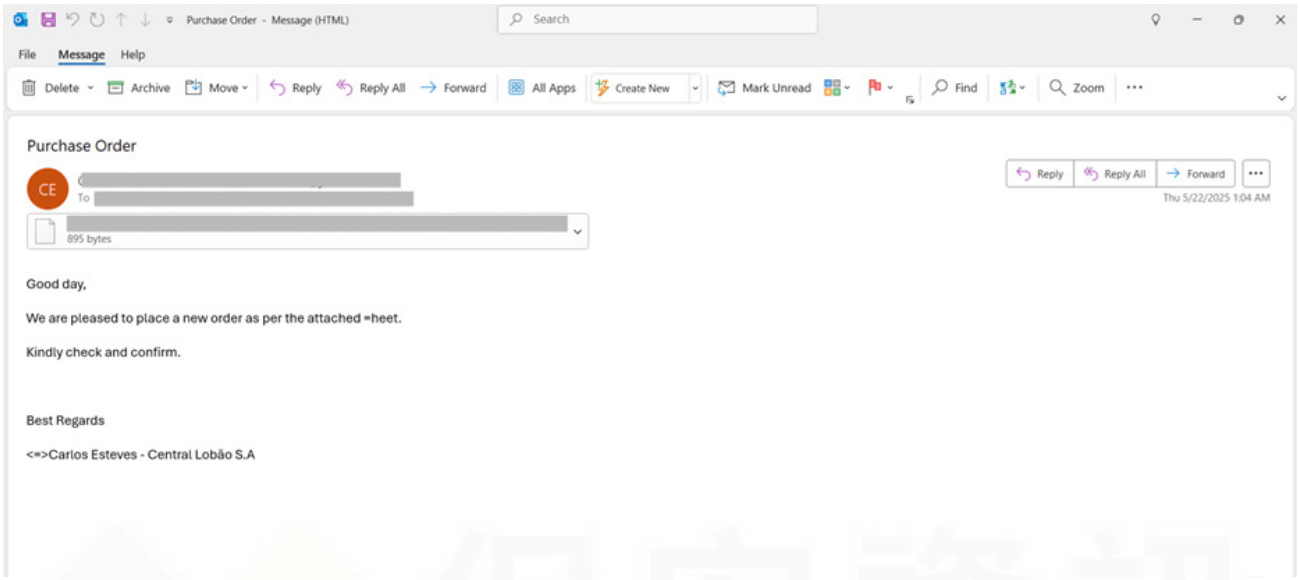
如果我們可以透過觀察其自然行為來偵測攻擊，而不讓網路暴露在任何風險之下，那會如何？甚至在使用者看到釣魚電子郵件之前。

透過在賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 中使用 Cynic，我們就可以做到這一點。來自可疑電子郵件的附件會被轉寄給 Cynic，以便在雲端沙箱中進行分析。Cynic 的一個關鍵元件是來自 SONAR 引擎的沙箱特定行為偵測模型。

舉個最近的例子

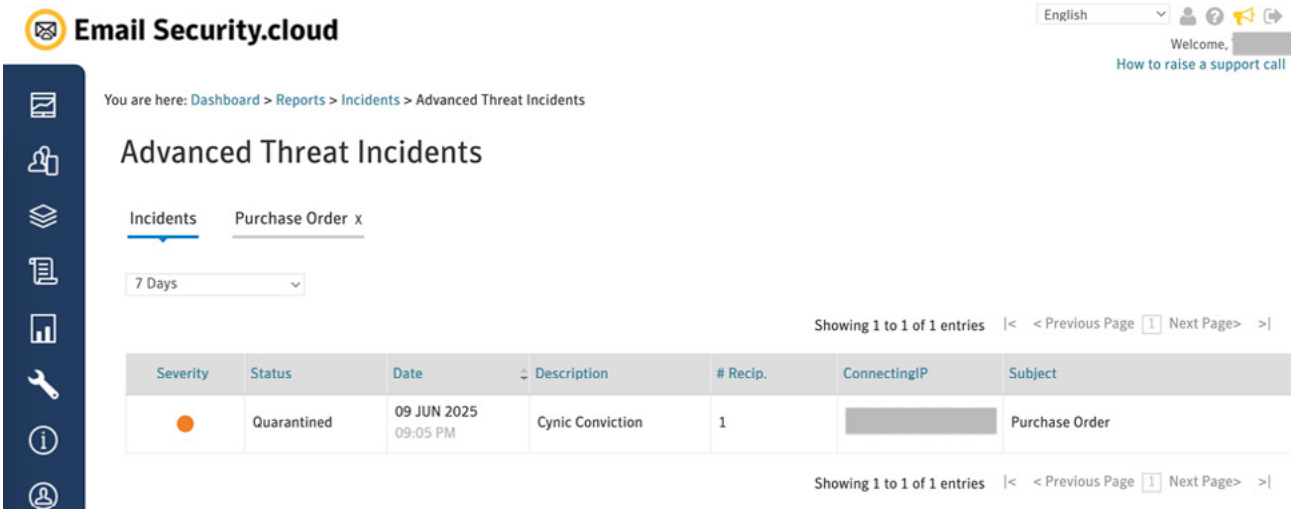
賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 掃描一封包含壓縮檔附件的

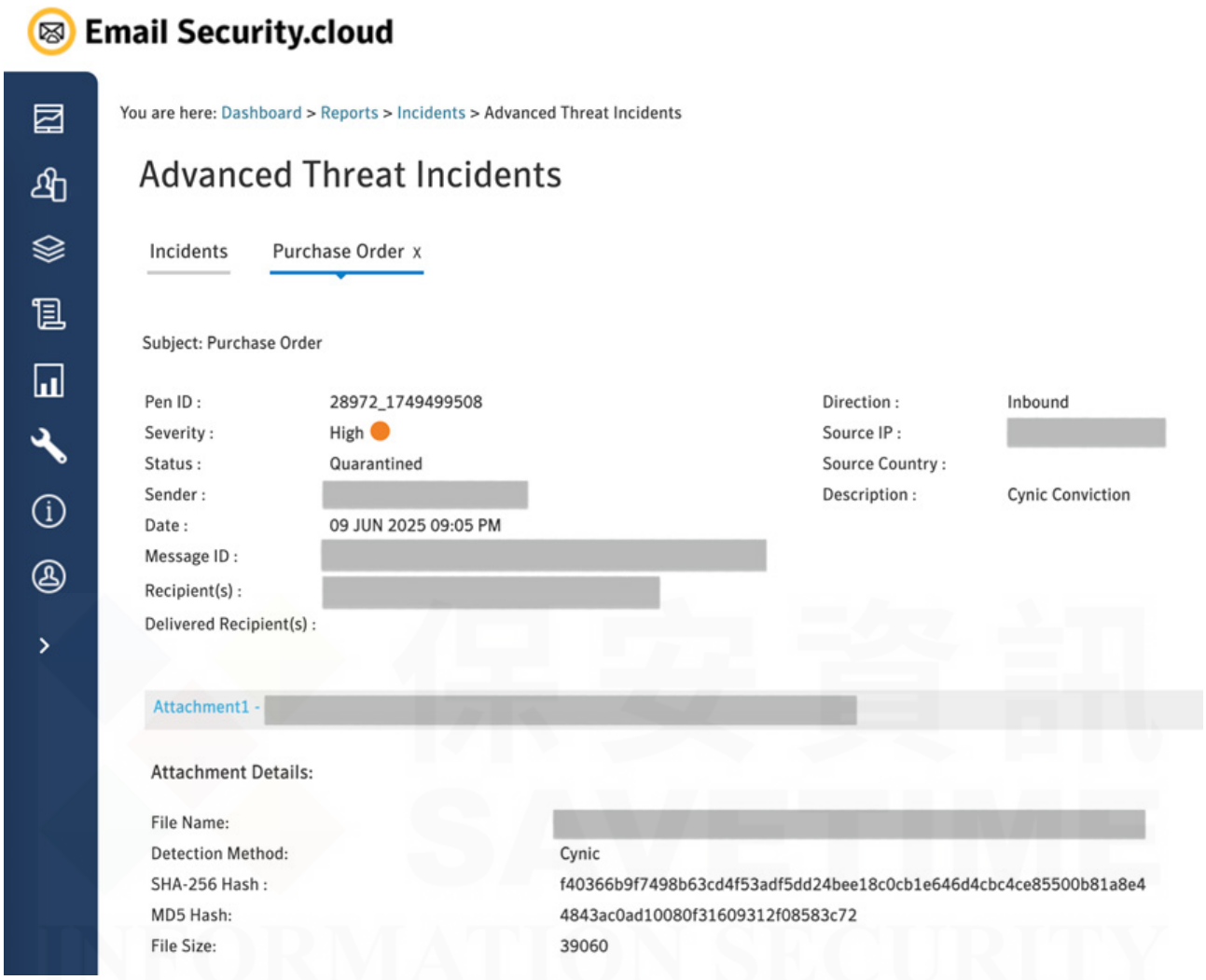
電子郵件。該附件被傳送至 Cynic 進行分析，而壓縮檔內容則會被引爆。在 Cynic 內，我們執行特殊的 SONAR 組態，該組態經過客製調整，可偵測和報告引爆環境中的可疑行為。



從 Cynic 引爆所獲得的大量資料中，我們能夠分析整個攻擊鏈並報告下列行為及偵測結果：

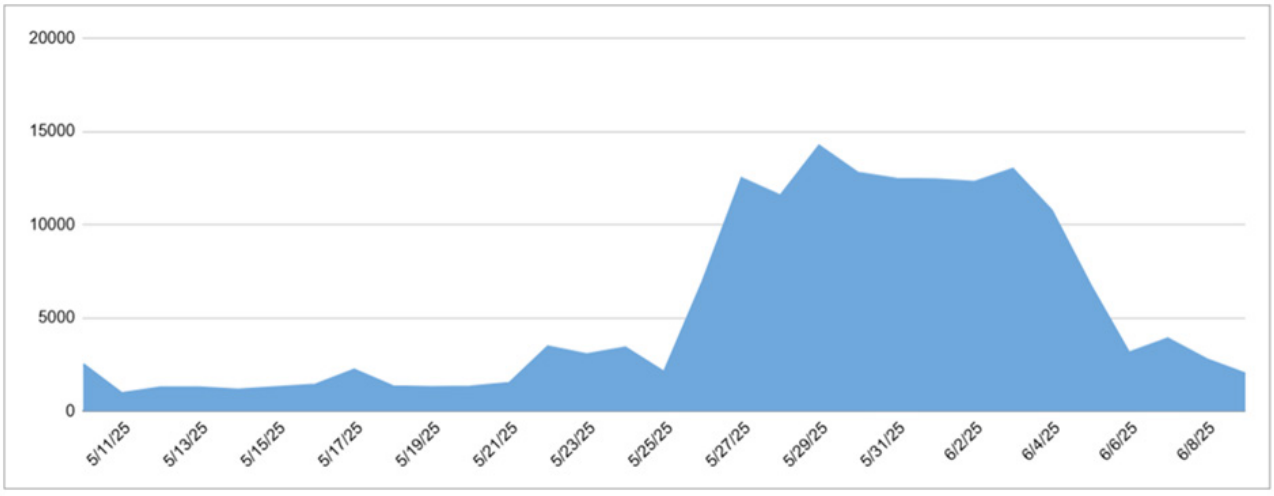
- 削弱防禦能力 (MITRE T1562)：啟動 PowerShell 執行個體時 (instance) 停用 Windows Defender。
- 處理程序挖空 (Process Hollowing) (MITRE T1055)：將 regsvcs.exe 挖空以注入 Snake Keylogger，我們透過深入掃描程序記憶體發現這一個情況。根據這些指標，Cynic 能夠確認電子郵件附件為惡意，讓賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 能夠保護網路免受這次釣魚嘗試的攻擊。





答案都在這裡，你只要登入並瀏覽賽門鐵克郵件安全雲端服務 (ESS：Email Security.cloud Service) 的管理介面。而在 SONAR 寶貴協助下，Cynic 的能力遠超壞人所能想像。

SONAR 攔截的電子郵件



欲了解有關 Symantec Endpoint Protection 的行為分析技術 SONAR 的更多資訊，請點擊此處。
欲了解管理行為分析 (SONAR)，請點擊此處。
欲了解 SONAR 如何與賽門鐵克雲端沙箱 (Symantec Cloud Sandbox) 整合，請點擊此處。
欲了解更多有關賽門鐵克郵件安全雲端服務 (Email Security.Cloud) 的詳細資訊，請點擊此處。

2025/06/10

Datarip--MedusaLocker勒索軟體家族的最新變種

Datarip 是近期在真實網路情境裡發現 MedusaLocker 勒索軟體家族的最新變種。該惡意軟體會加密敏感資料，同時在被加密的檔案中冠上「.datarip」副檔名。勒索贖金支付通知是一個檔名為「RETURN_DATA.html」的文字檔。該勒索軟體採用雙重勒索策略，威脅若不乖乖就範付贖金，就會公開發佈從受害者電腦中擷取的機密資訊。Datarip 具備刪除受感染端點上的磁碟區陰影複本和本機備份的功能。

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：

基於行為偵測技術(SONAR)的防護：

- AGR.Terminate!g2
- SONAR.RansomLckbit!g3
- SONAR.SuspLaunch!g18

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.BlackHeart!gen1
- 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

2025/06/09

發現全新遠端存取木馬(RAT)：DuplexSpy

在真實網路情境裡發現全新遠端存取木馬 (RAT)：DuplexSpy。此惡意軟體以 C# 寫成，具有模組化架構，並使用 DLL 注入技術在記憶體內執行有效籌載。一旦在遭入侵的端點上執行，便可進行鍵盤記錄、遠端 shell 存取、螢幕擷取、電源控制存取、註冊表及程序竄改等。DuplexSpy RAT 在 AES／RSA 加密的協助下，透過安全連線與攻擊者通訊。

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：

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.Malcode!gdn14
- Trojan Horse
- Trojan.Gen.MBT
- WS.Malware.1
- WS.Reputation.1

基於機器學習的防禦技術：

- Heur.AdvML.C

2025/06/09

DragonClone惡意攻擊行動

DragonClone 是在真實網路情境裡發現的全新惡意攻擊行動。攻擊者一直以來就是鎖定中國電信行業為目標，並散佈 Veletrix 和 VShell 惡意軟體植入器作為有效酬載。已報告的行動使用 DLL 側載和 IPFuscation 技術，並顯示與之前 UNC5174 和 Earth Lamia 威脅組織的惡意活動有一定程度之重疊。

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：

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

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。

2025/06/09

Golden Piranha--全新瀏覽器擴充套件的銀行威脅

Golden Piranha 是 SCILabs 研究人員發現的新興銀行木馬程式。該惡意軟體利用 Google Chrome 瀏覽器擴充套件，從各種銀行網站表單中竊取關於銀行的輸入資訊。Golden Piranha 主要針對巴西的銀行機構。此威脅疑似透過釣魚電子郵件散佈，導致受害者下載惡意誘捕程式。利用惡意擴充程式收集的敏感資料會傳回攻擊者控制的 C&C 基礎架構。

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-Net!g1
- ACM.Ps-RgPst!g1
- ACM.Untrst-RgPst!g1
- ACM.Untrst-RunSys!g1
- ACM.Ps-Wscr!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：

- Downloader
- Trojan Horse
- Trojan.Gen.2
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- Trojan.Gen.NPE.C
- Trojan.XSense.C
- WS.Malware.1
- WS.Malware.2
- Web.Reputation.1

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。

2025/06/06

Interlock勒索軟體集團部署全新的遠端存取木馬(RAT)：「NodeSnake」

據觀察，Interlock 勒索軟體集團部署一種名為「NodeSnake」的全新的遠端存取木馬 (RAT)，並以教育機構作為攻擊目標。這些攻擊從含有惡意連結或附件的釣魚電子郵件引爆。一旦使用者與這些郵件互動，NodeSnake 惡意軟體就會執行。該RAT 以 JavaScript 寫成，並以 NodeJS 執行，以達到隱匿和持久性的目的。感染後，它會立即使用 PowerShell 或 CMD 腳本在 Windows 註冊表中建立一個名為「ChromeUpdater」的欺騙性項目。這可讓惡意軟體冒充合法的 Google Chrome 程序，確保它自動重新啟動，並避免最初的懷疑。一旦啟動，NodeSnake 的主要功能是進行偵察。它會收集受感染機器的大量資料，並將收集到的資訊傳送給攻擊者。

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：

基於行為偵測技術(SONAR)的防護：

- SONAR.Ransom!gen112
- SONAR.Ransomware!g7
- SONAR.Ransomware!g16
- 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：

- Ransom.Interlock
- Trojan Horse
- Trojan.Gen.MBT
- Trojan.Gen.NPE
- 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。

2025/06/06

駭客組織：APT41使用自訂惡意軟體「TOUGHPROGRESS」來利用Google行事曆

據觀察，駭客組織：APT41 使用名為 TOUGHPROGRESS 的客製惡意軟體，利用 Google 行事曆事件作為其 C&C 通道，允許其將惡意指令隱藏在看似良善的公共行事曆項目中。此攻擊始於有針對性的魚叉式釣魚電子郵件，引導受害者從受攻擊的網站下載 ZIP 檔案。此檔案包含一個偽裝成 PDF 的惡意 .LNK 捷徑檔，以及數個秘密藏有加密有效酬載及其解密工具的 JPG 影像。執行後，惡意軟體會啟動三階段的記憶體內感染程序，以逃避偵測。初始惡意載入器 PLUSDROP 和 PLUSINJECT 解密並注入最終有效酬載。最後的有效酬載 TOUGHPROGRESS 被嚴重混淆，並透過 Google Calendar API 建立隱蔽的 C&C 通道。

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.Mallnk!gen2
• Scr.Mallnk!gen15
• Trojan Horse

基於機器學習的防禦技術：

• Heur.AdvML.A
• 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。

2025/06/06

遊戲作弊程式暗藏Blitz惡意程式

Blitz 是由惡意程式下載器和殭屍網路元件組成的多階段惡意軟體。Palo Alto Networks 研究人員最近一份報告提供試圖擴散此惡意軟體的活動細節。最初階段是透過隱藏的視訊遊戲作弊應用程式傳送。執行遊戲作弊程式的受害者會在背景下載 Blitz 下載器元件。此元件會負責下載 Blitz 殭屍網路元件。

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

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
- Downloader.Trojan
- Miner.XMRig
- 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
- 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。

2025/06/06

安卓(Android)手機／行動裝置平台上發現偽裝成政府APP的惡意軟體，以印度使用者為目標

在最近觀察到的一些惡意活動中，發現一個偽裝成政府 APP 的惡意軟體，以印度的 Android

使用者為目標。該惡意軟體的目的是竊取個人資訊和簡訊內容 (SMS)。惡意軟體的特徵包括多階段下載、反分析功能，以及使用者互動允許惡意行為的權限。

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：

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
- AppRisk:Generisk